DEA Diversion Control
E-Commerce System

Controlled Substance Ordering System

Regulatory and Technical Working Group Meeting

January 31, 2001

Arlington, VA

01/31/2001

Table of Contents

Section 1: Opening Remarks

On January 31, 2001, the Drug Enforcement Administration's (DEA) Office of Diversion Control met with representatives from the drug wholesale industry and their major national associations. Ms. Patricia Good welcomed those present to the second regulatory and technical working group meeting on the Controlled Substance Ordering System (CSOS) project. Ms. Good said CSOS is expected to bring numerous benefits to the manufacturing, distribution, and pharmacy communities. These benefits include: reduction in the number of ordering errors; increase in line items on a single order; faster ordering; less consolidating of orders; ability to place more frequent orders for fewer items; less reason to stockpile product; less waiting to fill up an order form; and less need for product to be kept on the shelf. In addition, Ms. Good acknowledged the CSOS project would improve DEA's ability to perform its regulatory responsibilities while at the same time reducing the burden of regulation on industry.

Ms. Good then introduced Ms. Laura Nagel, the new Deputy Assistant Administrator of the Office of Diversion Control, Terrence W. Woodworth, Deputy Director of the Office of Diversion Control, as well as Andrew Sciora and Steven Bruck, both of PEC Solutions. Steven Bruck recently became project manager the CSOS initiative.

Section 2: Overview of CSOS project

2.1 Why PKI

Public Key Infrastructure (PKI) technology was chosen for the CSOS project because it provides many advantages. The following examples point out the benefits of using a PKI for controlled substance orders: reduction in the amount of paper used, increased speed of transaction, lower costs per transaction, and it delivers electronic security services into the process.

The electronic security services include authentication of sending party, integrity of communications and non-repudiation. Authentication of sending party allows the recipient to positively identify the sender of the communication and subsequently to demonstrate to a third party, if required, the sender was properly identified. Integrity of communication permits the recipient of a message to determine if the message content was altered in transit. Non-repudiation ensures the originator of the message can not convincingly deny to a third party that the originator sent it.

2.2 Survey/Interviews with Industry

Early in the project PEC spoke with DEA personnel, as well as industry representatives. PEC interviewed and conducted surveys of the top 30 members of industry representing a wide cross section of the stakeholders in the controlled substance distribution environment. The industry group included manufacturers, distributors, pharmacies, chain pharmacies, and other dispensing registrants. The survey and interviews focused on the handling of DEA Official Order Forms, DEA Form-222 and evaluated industry's preference to use existing systems or develop a new system in the CSOS project. The interviews revealed that industry deals with DEA Form-222's in a consistent manner. Furthermore, industry demonstrated an overwhelming desire to use their existing systems in the CSOS project.

2.3 Policy

PEC developed the CSOS Concept of Operations (CONOPS) document. The CONOPS provides a conceptual overview of how the 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 would be operated from both industry and DEA's perspective. It is available on the DEA Diversion Web Site. The Web site address is www.deadiversion.usdoj.gov.

PEC has delivered the last remaining policy documents, the Certificate Practice Statement and Certificate Policy Statement, to DEA. At this time these policy documents are in draft form.

2.4 Architecture Design

Mr. Sciora of PEC reviewed a flowchart depicting the architectural design of a controlled ordering system. This flowchart outlined the customer's responsibility, the supplier's responsibility, and DEA's responsibility. In addition, Keane Lee, also from PEC, answered questions regarding the CSOS demonstration system. The demonstration system is representative of what a user would experience using a PKI-enabled ordering system.

2.5 Phased Approach

1. PEC and select industry partners (Walgreens and McKesson) are currently in the Proof of Concept phase. At this time, PEC is testing the PKI system they designed and built with these selected industry partners.

2. Pre-production phase (i.e., testing) - this is the next phase, and it can be entered into once the rulemaking process has been finalized (regulations written, comments received, and final rule published). This phase proves the system does what it is intended to do and ensures there are no problems with the system.

3. Production phase – when and if this phase is entered is determined by industry. PEC will be available to help industry and offer solutions in the implementation of their CSOS.

Section 3: Project Factors

The PKI enabled software products must be FIPS 140-1 approved. FIPS approval indicates the cryptographic software modules used by the application have met U.S.

government mandated performance guidelines. Industry is not responsible for obtaining government approval; it is the vendor's responsibility to obtain FIPS approval.

The National Institute of Standards and Technology (NIST) Web site should be consulted to learn more about FIPS and FIPS approved products. The Web site address is http://csrc.ncsl.nist.gov/cryptval/140-1/1401val.htm.

Section 4: DEA Criteria

As previously mentioned, the cryptographic modules used in the ordering system must be FIPS approved.

In addition, DEA requires that the users' digital certificate convey basic information including: user name, issuing Certificate Authority, e-mail address of registrant, and validity period. This information will be incorporated into the certificate using X.509 extensions. However, in addition to the basic information, DEA requires certificates to contain additional information such as: the registrants DEA number, registered address, the validity period of the DEA registration, and the drug schedules that the registrant is authorized to handle. The software must extract the information provided by the certificate and ensure that it agrees with the information provided on the order.

Section 5: Industry Criteria

Industry indicated a desire to use their existing systems.

Section 6: Product Evaluation

PEC conducted an extensive evaluation of PKI products and made a selection based on the products ability to best meet both DEA and industry requirements. The products were required to support FIPS, certificate revocation management, and posting of certificate revocation lists.

Section 7: CA/Directory Oversight Structure

The control and management of the CSOS PKI will be the responsibility of the Policy Management Authority, the Operations Management Authority and the PKI Manager.

7.1 Policy Management Authority

The Office of Diversion Control will establish a CSOS PKI Policy Management Authority. The Policy Management Authority will be responsible for setting, implementing, and managing CSOS PKI certificate policy and practices. The Policy Management Authority will be composed of Office of Diversion Control personnel.

The Policy Management Authority will be responsible for certification and accreditation of the overall PKI implementation and has responsibility for oversight of all PKI operations. The PKI Policy Management Authority will also be responsible for the following: approving and revoking certificates of registrants; ensuring appropriate use of PKI facilities throughout the CSOS PKI; and maintaining and publishing the Certificate Policy and Certification Practice Statement. Furthermore, the PKI Policy Management Authority commissions annual audits of PKI operations.

7.2 Operations Management Authority

The Policy Management Authority will establish a 24-hour/day, 7 day/week Operations Management Authority to manage the operation of the CA and to carry out the provisions of the Certificate Policy and Certificate Practices. The Operations Management Authority 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 Operations Management Authority has overall responsibility for proper and reliable operations of the CSOS PKI Certification Authority 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: maintaining the Certificate Practices Statement; oversight of PKI operations; reviewing Certification Authority operations and activity; management of all technical aspects of the PKI; and the review of PKI functional, technical, staffing, and budgetary plans.

7.3 PKI Manager

The PKI Manager will staff and manage the operation of the CSOS PKI Certification Authority and it's associated directories, repositories and communication facilities on a day-to-day basis. The PKI Manager ensures the CSOS PKI 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. The PKI Manager is also responsible for developing and maintaining PKI plans, policies and procedures pertaining to the operation of the Certification Authority and the overall operation of the PKI.

Section 8: Software Auditing

8.1 Criteria

In a PKI controlled substance ordering system a digital signature module will exist on the customer side. A digital signature validation module will exist on the supplier side. These software modules must function in accordance with DEA's CSOS Certificate Policy. This creates a need to audit the software to ensure each company's PKI systems are working properly.

8.2 Private Key Safeguarding-Password Management

A password is used to control access to each user's private signing. System controls that set standards for password selection are critical; security does not exist if there is no ability to safeguard individual private keys. Password management is an essential area to review during the auditing function. The password must contain both alpha and numeric characters, and can not be a word found in the dictionary. The password must meet length requirements, as yet to be determined.

8.3 Physical Access Controls

Physical access control is another auditing function. Each individual must retain possession of their private key. For example, a password may be stored on a smartcard. When the certificate is used, the smartcard is inserted into a machine that reads the card. Use of the smartcard would be coupled with biometrics or be password activated to ensure the card belongs to that individual. Smartcards are just one option, there are other storage mechanisms, such as on the computer's hard drive. However, the company must prove during the audit that its method is secure. Another physical access control criteria is to logout of the system when the transaction has been completed. One more physical access control measure is limiting access to authorized staff.

8.4 Data Access Controls

An additional audit criterion involves data access control. Specifically, inactive accounts must be removed, data access must be restricted to authorized users, and accounts must not be shared.

8.5 Reporting Audit Results

An initial audit conducted by a third party software auditor is required for companies not working with DEA during their development of a PKI-enabled controlled substance ordering system. Annual audits will be required annually thereafter by an independent third party software auditor. Upon successful completion of the audit, the auditor provides the company with an attestation confirming the system complies with DEA standards. The original copy of the certificate will either be sent to DEA or be made available for inspection.

8.6 Failure to Pass Audit

At this point in time, the following options are under consideration. If the company does not pass an annual software audit conducted by an independent third party software auditor, then a warning is submitted by the Policy Management Authority (i.e., DEA) with 60-day correction period. If corrections are not made all registrant and power of attorney digital certificates are suspended, and a request sent to Policy Management Authority for revocation proceedings.

Section 9: Development Initiatives

9.1 Visual Basic – Demo

Keane Lee from PEC exhibited a demonstration PKI electronic controlled substance ordering system using laptop computers. PEC built the demonstration system to simulate the operation of a PKI-enabled ordering system. This demonstration system performs all of the signing and verifications DEA will require and is used as a teaching tool. In developing a controlled substance ordering system, there are basic constraints industry must follow. However, the level of developmental effort in any industry built controlled substance ordering system above and beyond the basic standards is dependent on each company's requirements. PEC and DEA are available to provide assistance as each company implements their system.

9.2 C++-Window Platform

PEC has developed the Dynamic Linked Library (DLL) using C++ for a customer base using the Windows Platform. The DLL supports the full signing and validation of the order form. This module is currently available for any company wishing to implement a controlled substance ordering system.

9.3 Sun Solaris – Unix Platform

A Sun Solaris platform is also available.

9.4 Java – Multi-platform

Industry expressed a need for a signing/verification module for the IBM AS-400 operating environment. In coordination with industry partners, a JAVA-based module was requested to provide cross-platform support and to eliminate the need for a gateway. The JAVA module has the ability to digitally sign and validate the order forms. However, industry will need to conduct additional developmental effort in the areas of smart card technology and extension processing.

Section 10: Project Status

10.1 Industry partners

McKesson and Walgreens are the designated industry partners in the Controlled Substances Ordering System project. However, if others in industry are interested in participating in the project, the point of contact is Mr. Steven Bruck at PEC Solutions, telephone number [redacted].

10.2 Regulations status

A draft of the Notice of Proposed Rulemaking is written and is currently being reviewed and revised. The regulations will be general in order to encompass the entire electronic process, but at the same time they will be specific and detailed in regards to compliance issues and enforceability. The regulations will be in the form of standards to be met, and it is up to industry to meet the requisite standards. The pre-production phase (i.e., testing), will be conducted once the rulemaking process is finalized. DEA anticipates publishing a Notice of Proposed Rulemaking in approximately three (3) months. The NPRM will have a 60-day comment period.

10.3 Standing up CA and Directory

DEA has acquired the necessary equipment for the CSOS CA. Mr. Sciora mentioned PEC is currently integrating the latest versions of the software.

Presently, PEC is waiting for industry partners to complete integration and testing and DEA to publish the regulations.

Section 11: Closing Remarks

Ms. Good thanked the conference participants and DEA staff for attending. She anticipates scheduling the next meeting prior to the publication of the Notice of Proposed Rulemaking.