
Public Key Infrastructure Analysis

PKI Certificate Policy Requirements Analysis

Electronic Prescriptions for Controlled Substances

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**

March 13, 2000

**Prepared by
Performance Engineering Corporation**

Table of Contents

	page
Section 1 – Introduction	1–1
1.1 Overview and Background	1–1
1.2 Mission of the Office of Diversion Control	1–1
1.3 Document Organization	1–2
1.4 Description of Task 2.2.1	1–2
1.5 Analysis Methodology	1–4
Section 2 – Data and Findings	2–1
2.1 Controlled Substance Prescription Environment	2–1
2.1.1 Relevant Sections of the Code of Federal Regulation (CFR)	2–2
2.1.2 Registration	2–3
2.1.3 Prescribing and Transmitting	2–3
2.1.4 Prescription Verification and Dispensing	2–4
2.1.5 Record Keeping	2–6
2.1.6 Current Reporting Systems	2–7
2.1.7 Current Use of Electronic Prescriptions	2–8
2.2 Considerations for the adoption of Electronic Prescriptions	2–9
2.2.1 Stakeholder Perceived Benefits	2–9
2.2.2 Existing Security Standards/Environment	2–14
2.2.3 Factors that Influence Adoption of Electronic Prescriptions	2–18
2.3 Regulatory/Legal Environment	2–20
Section 3 – Policy Requirements Foundation	3–1
3.1 Certificate Policy (CP)	3–1
3.2 Levels of Assurance/Security	3–2
3.3 DEA Root Certification Authority Analysis	3–6
3.3.1 Evaluation of Alternatives	3–13

Table of Contents (continued)

	page
Section 4 – PKI Certificate Policy Requirements	4–1
4.1 Electronic Prescription Certificate Policy Analysis.....	4–1
4.1.1 Component #1—Introduction	4–2
4.1.2 Component #2—General Provisions	4–3
4.1.3 Component #3—Identification and Authentication.....	4–5
4.1.4 Component #4—Operational Requirements.....	4–7
4.1.5 Component #6—Technical Security Controls	4–7
4.1.6 Component #7—Certificate and CRL Profiles	4–10
4.2 Summary of Policy Requirements	4–18
Appendix A – Requirements Interviews List	A–1
Appendix B – Documents Reviewed.....	B–1
Appendix C –Relevant Sections of the CFR (Part 1300 to the end)	C–1
Appendix D – Regulatory/Legal Environment	D–1
Appendix E – RFC 2527 Certificate Policy Components.....	E–1
Appendix F – Listing of Acronyms.....	F–1

List of Exhibits

		page
1-1	Registrant categories.....	1-2
2-1	Prescription dispensing environment.....	2-2
2-2	Relevant sections of the CFR.....	2-3
2-3	Prescribing and transmitting.....	2-4
2-4	Pharmacy verification process.....	2-6
2-5	State prescription monitoring programs.....	2-8
2-6	Electronic prescription allowances among states.....	2-9
2-7	Benefits of electronic prescriptions.....	2-10
2-8	Reduced paperwork burden.....	2-11
2-9	Faster filling.....	2-12
2-10	Patient satisfaction.....	2-13
2-11	Patient confidentiality.....	2-15
2-12	Provide tools for authentication.....	2-16
2-13	Reduced forged/stolen scripts.....	2-17
3-1	Federal PKI semantic framework.....	3-3
3-2	Hierarchical trust model.....	3-8
3-3	State of Utah CA licensing requirements.....	3-9
3-4	Hierarchical root CA architecture.....	3-10
3-5	Impact of ARL validity period on frequency of ARL checks.....	3-12
3-6	Evaluation of alternatives.....	3-14
4-1	Advantages and disadvantages of private key storage alternatives.....	4-9
4-2	Advantages and disadvantages of biometric access control to private key.....	4-10
4-3	Single-certificate models.....	4-12
4-4	Multiple-certificate models.....	4-13
4-5	Summary of certificate model analysis.....	4-13
4-6	Candidate data elements for inclusion in certificate.....	4-15
4-7	Advantages and disadvantages of certificate validity period alternatives.....	4-16
4-8	Advantages and disadvantages of CRL validity period alternatives.....	4-17
4-9	Summary of policy requirements.....	4-18

Section 1 — Introduction

1.1 Overview and Background

Under the authority of the Controlled Substances Act of 1970, the Drug Enforcement Administration (DEA), Office of Diversion Control (OD) regulates the manufacture and distribution of controlled substances in the United States. This regulatory control is designed to prevent the diversion of legitimate pharmaceutical drugs into illegal channels and also to ensure that there is a sufficient supply for legitimate medical uses. *Title 21, Code of Federal Regulations, 1300 to the end*, sets forth in detail the authority and responsibilities of DEA in this area. The Government Paperwork Elimination Act of 1999 (Title XXII of Public Law 105-277) mandates that Federal agencies allow for the option of electronic submission of required records and for the use of electronic signatures when practicable.

The DEA plans to modify their regulations to permit the electronic transmission of controlled substance prescriptions between practitioners and pharmacies that employ Public Key Infrastructure (PKI) technology. This technology will bring to this process the following advantages: (1) reduce the amount of paper in the process (2) speed transaction times (3) lower costs per transaction and (4) introduce security services into the process.

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

1.2 Mission of the Office of Diversion Control

Title 21, Code of Federal Regulations, 1300 to the end, defines the registration, record keeping, inventory, order processing, prescribing, and miscellaneous activities as they relate to controlled substances. Persons who wish to participate in a controlled substance business activity, i.e. manufacturing, distributing, dispensing, research, narcotic treatment programs, import, export, are required to register with the DEA unless otherwise exempted from registration described in §1301.22. Registrants fall into two categories, A-Type registrants and B-Type registrants. The two types of registrants are listed in Exhibit 1-1.

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

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

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

Exhibit 1-1. Registrant categories

1.3 Document Organization

The document is organized into the following sections:

Section 1–The introduction provides a description of the task and an overview of the goals and objectives of the task.

Section 2–Section 2 provides definitions and standards that pertain to the classification of Certificate Policies by levels of assurance and security.

Section 3–Section 3 provides detail, summary data, and findings produced by the interviews, meetings, seminars, document reviews and site visits with prescribers, pharmacy representatives, associations, and registrants.

Section 4–Section 4 provides an analysis of the data and findings used to derive the requirements for the electronic transmission of controlled substance prescriptions.

Appendix A–Listing of Interviews, Site Visits, Meetings and Conferences

Appendix B–Listing of Documents Reviewed

Appendix C–Relevant Sections of the CFR

Appendix D–Regulatory/Legal Environment

Appendix E–RFC 2527 Certification Policy Components

Appendix F–Listing of Acronyms

1.4 Description of Task 2.2.1

Certificate Policy Requirements Analysis Task 2.2.1

During this task, PEC Solutions and DEA will define the level of security that the PKI must incorporate in order to support legal and regulatory requirements as well as the

needs of industry. The trust model most appropriate to the organizations and processes involved must also be determined. The analysis will involve making critical risk management decisions and trade-offs in levels of security, cost and resource allocation, time, technical feasibility, and user acceptance. This will be an interactive process between PEC Solutions and DEA.

This analysis will result in a clear, general understanding of certificate policy requirements. During Task 3, a Certificate Policy (CP) and Certification Practices Statement (CPS) will be developed, drawing from the results of this analysis.

The analysis will result in a statement of the obligations and liabilities of the Certification Authority (CA), Registration Authorities (RA), users, and relying parties. It will require an understanding of relevant Federal and State laws, DEA Regulations, and accepted customs and practices of the industry.

The analysis will provide recommendations in the context of the electronic prescription PKI Pilot, regarding the assurances and guarantees that the CA must make to the users and relying parties who accept and use the CA's certificates and the responsibilities and obligations of users and relying parties of the CA's certificates. This will include liability issues, issues of financial responsibility, interpretation and enforcement of the policy or CPS and possible fees associated with the PKI.

PEC Solutions will determine the requirements that participating CAs must adhere to with respect to operational procedures. Some of these requirements may apply to the RAs and directories/repositories. The analysis will also focus on the physical, procedural, and personnel security controls that a participating CA must implement. In the final CP and CPS, the CA will make representations to users and relying parties regarding these matters. A representative list of topics that must be considered includes: site location and construction; power, air conditioning; protection against fire, water, damage; media storage; background checks and clearance procedures for employees; training and certification requirements for employees; role and authority separation for employees; identification and documentation of employees.

Technical security controls—another type of security requirement—will also be analyzed. In this part of the analysis the technical controls needed by the CA to ensure the secure function of key generation, user authentication, certificate management, audit, backup and archiving are determined. Representative areas of this analysis include key pair generation, private key protection, computer security controls, network security controls, and activation data.

A final area that will be considered is the certificate profile. The X.509 standard for PKI certificates is a complex data structure that permits many versions or profiles. During this phase of the analysis PEC Solutions will determine which of the trust models is most appropriate for the PKI. A choice of trust model has implications for decisions on product selection, cost, architecture, policies and procedures, and risk management.

1.5 Analysis Methodology

The methodology used for this analysis included:

- (1) Interviews with selected DEA and industry representatives
- (2) Review of documents recommended by DEA and industry
- (3) Visits to sites recommended by DEA and industry
- (4) Follow-up of leads and sources developed during (1)-(3) above and
- (5) Questionnaires submitted to selected industry representatives.

Appendix A of this document contains the listing of all interviews conducted, site visits made, and conferences and meetings attended in the preparation of this analysis. Appendix B contains a listing of all documents read and reviewed in preparation for this analysis.

1.5.1 Industry Stakeholder Groups Defined

The dispensing activity—as defined in CFR §1300.01 and §1301.13—applies to retail pharmacies, hospital/clinics, practitioners, teaching institutions, and mid-level practitioners. Stakeholders for this project are parties that have an interest or share in the retail pharmacy prescription process. Specifically, this includes; 1) law enforcement/regulatory authorities (DEA and state organizations), and 2) industry, which include practitioners and pharmacists.

Pharmacists

Pharmacy organizations—including chain pharmacies, community/independent pharmacies, pharmacy associations, and integrated health delivery systems—were contacted for interviews. Information collected included: current business policies and practices, information technology (IT) infrastructure, and IT security that are currently in place at pharmacies.

Practitioners

Registered practitioners (including registered mid-level practitioners) have the authority to prescribe controlled substances in the course of their professional practice. Practitioners interviewed included associations, private practitioners, hospital/clinic practitioners, and practitioners associated with integrated health delivery systems. Information collected included: current business policies and practices, IT infrastructure, and IT security.

State Regulatory Organizations

State regulatory organizations such as State Controlled Substance Authorities, diversion control units, and State Boards of Pharmacy play an important role in regulating pharmacy operations. State agencies were interviewed to gather information regarding current laws and regulations, business flow, diversion problems, along with any concerns and ideas regarding an electronic prescription system for controlled substances.

Drug Enforcement Administration (DEA)

The DEA's mission is to enforce the laws and regulations pertaining to controlled substances. The DEA enforces regulations that practitioners and pharmacies must adhere to when prescribing and dispensing controlled substances. DEA has the authority to conduct administrative and criminal investigations. DEA representatives were interviewed to collect information regarding 1) DEA's regulations pertaining to diversion prevention 2) DEA diversion control measures, 3) their investigative practices and 4) the DEA's needs with respect to legal sufficiency.

Section 2 – Data and Findings

The objective of the Electronic Prescription PKI Pilot project is to develop standards and guidelines that will support the electronic transmission of prescriptions for Schedule II-V controlled substances from practitioners to pharmacies. DEA plans to allow this method of transmission as an alternative to the current prescription practice. No change to the currently accepted prescription process will take place. Adoption of this alternative method is not mandatory and is up to the individual stakeholder. Initial acceptance will be based on the benefits such a system will offer stakeholders.

PEC interviewed business process stakeholders and performed research to obtain two distinct sets of information: 1) the current prescription process, and 2) stakeholder opinions on a new method for electronically transmitting controlled substance prescriptions. This section identifies the controlled substance prescription business processes, considerations for electronic prescriptions for controlled substances, and the federal regulatory environment as it pertains to this electronic process.

2.1 Controlled Substance Prescription Environment

This section identifies the major business processes relating to the dispensing and prescribing of controlled substances at the pharmacy and the practitioner settings. Laws, regulations, common industry practices and company policies shape the environment in which pharmacist and practitioners work. This section discusses the current environment.

Exhibit 2–1 is a high level diagram of the prescription dispensing environment.

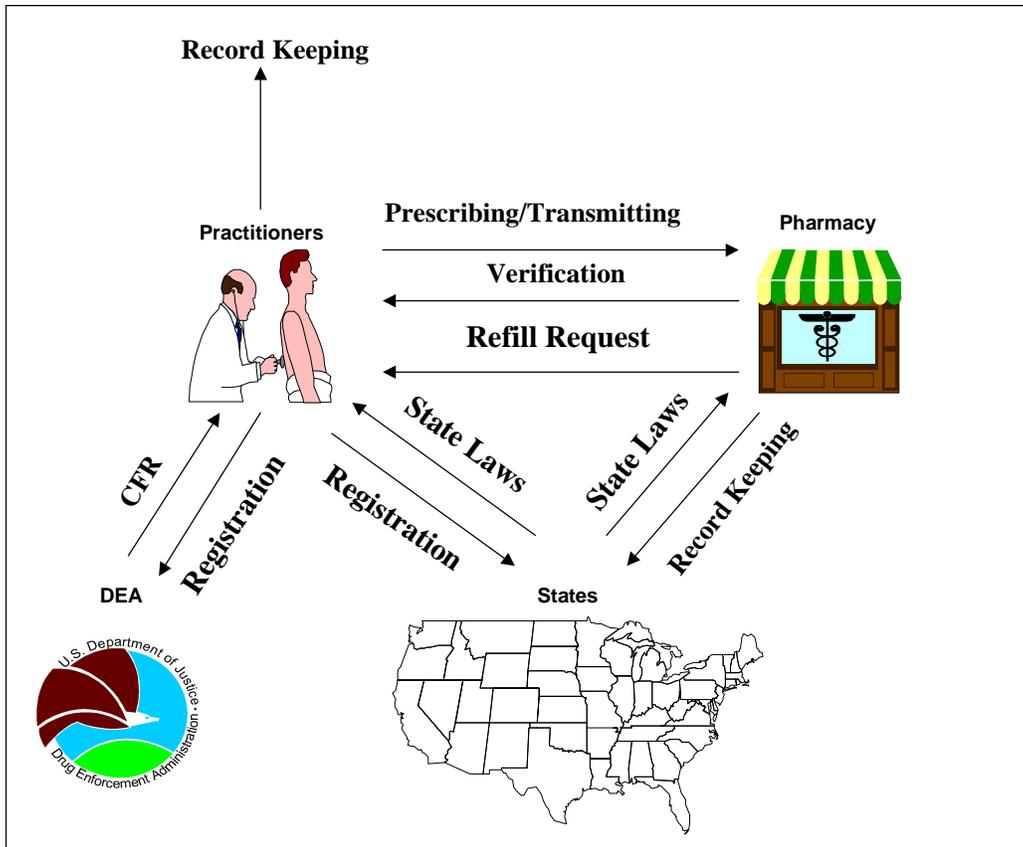


Exhibit 2–1. Prescription dispensing environment

2.1.1 Relevant Sections of the Code of Federal Regulations (CFR)

The DEA is responsible for regulating controlled substances in order to limit their diversion for illicit use. *Title 21 Code of Federal Regulations, 1300 to the end*, describes the various business activities associated with the handling of controlled substances—manufacturing, distributing, dispensing, research, and narcotic treatment programs (NTP)—and provides regulations concerning the security and record keeping that must be followed.

This section highlights the pertinent DEA regulations regarding the dispensing processes of pharmacies and practitioners. Exhibit 2–2, details the parts of the CFR that greatly affect the dispensing process that practitioners and pharmacies must follow. For more information, consult Appendix C for a detailed list of the relevant subsections of the CFR.

Part	Title	Summary
1301	Registration of manufacturers, distributors, and dispensers of controlled substances	Defines the registration process for those who wish to participate in the dispensing business activity including details for persons who are exempt from registering with the DEA.
1304	Records and reports of registrants	Outlines the requirements for the storage and maintenance of controlled substance prescription records.
1306	Prescriptions	Defines the requirements for prescribing and the responsibilities of the practitioners and pharmacies involved.

Exhibit 2–2. Relevant sections of the CFR

2.1.2 Registration

Practitioners desiring to prescribe or dispense controlled substances (Schedules II-V) must be registered with the DEA in the applicable dispensing category (practitioner, hospital/clinic, etc). CFR §1301 describes the registration process.

CFR §1301 states that each pharmacy location must be individually registered. The actual location is registered, not the pharmacists at the location.

Practitioners are required to register in each state where they wish to prescribe controlled substances or at any physical site where they intend to store controlled substances. In some instances, a practitioner will practice under multiple DEA registrations. For example, a practitioner might prescribe using different DEA registration numbers if he practices in more than one state. The mid level practitioner (MLP) category includes physician assistants and nurse practitioners that are authorized to prescribe controlled substances by state law or regulation.

2.1.3 Prescribing and Transmitting

Federal Regulations state the following: “All prescriptions for controlled substances shall be dated as of, and signed on, the day when issued and shall bear the full name and address of the patient, the drug name, strength, dosage form, quantity prescribed, directions for use and name, address and registration number of the practitioner.”

A prescription for a Schedule II controlled substance must be written, whereas Schedule III -V prescriptions can either be written, faxed, or called into the pharmacy.

Currently, physician assistants can prescribe medication in forty-six states. Of these forty-six states, thirty-nine states allow physician assistants to prescribe controlled substances - in schedule III-V drugs. Twenty states permit physician assistants to prescribe Schedule

II substances¹.

The dispensing process begins with the practitioner. Practitioners prepare and issue controlled substance prescriptions in accordance with CFR §1306. The prescription is then conveyed to the pharmacy for dispensing. As described in CFR §1306.11, a Schedule II controlled substance prescription must be in written form and bear the manual signature of the prescriber. However, Schedule II prescriptions for a resident of a long-term care facility (LTCF) may be sent to the pharmacy via facsimile and serve as the original prescription—the same is true for prescriptions for narcotic substances for patients in hospital care or for those receiving compounded substances. In an emergency, the pharmacy can accept oral prescriptions for a Schedule II controlled substance, with certain limitations. The process is illustrated in Exhibit 2–3.

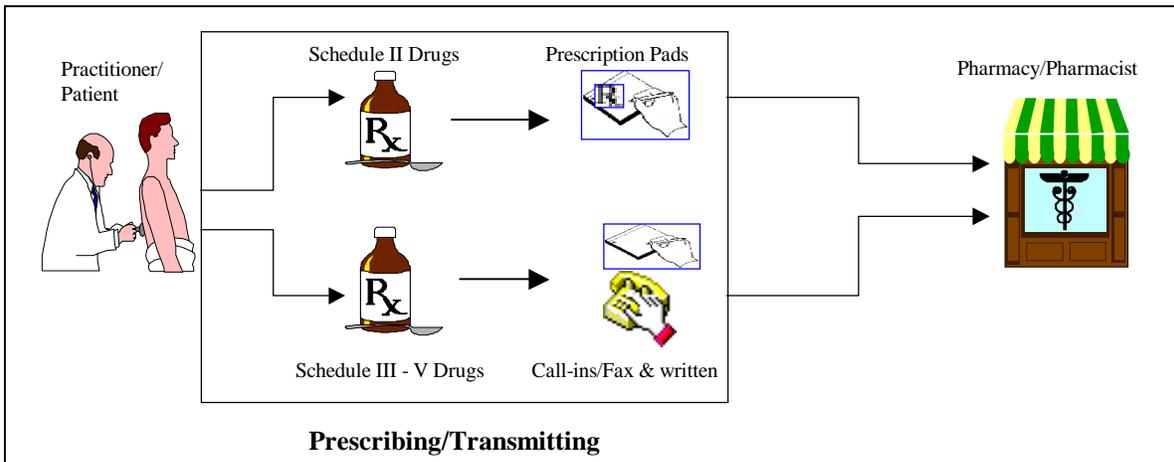


Exhibit 2–3. Prescribing and transmitting

2.1.4 Prescription Verification and Dispensing

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

A pharmacist must make a reasonable effort to determine that the prescription came from a registered practitioner. Pharmacists utilize a number of tools to validate prescriptions for controlled substances. Listed below are some common mechanisms used in the prescription validation process.

¹ American Academy of Physician Assistants

- **Call the Practitioner back**—A tool that is often used by pharmacists is a call back to the practitioner to check a prescription’s validity. Information required on the prescription is confirmed including the DEA number, substance prescribed, and dosage.
- **DEA’s Controlled Substance Act (CSA) database**—The DEA maintains a database of valid DEA registration numbers including the registrant’s name and the schedules they are permitted to prescribe. This information is available through the Department of Commerce in various media formats including CD-ROM and on-line access. Some pharmacies have integrated this database into their computer system to assist in the validation process.
- **DEA number check**—The DEA number is constructed using an algorithm. Many pharmacy systems are programmed to accept the DEA registration number and run the number through the algorithm to see if it matches the format. This verification process only determines if the number follows the DEA format. It does not determine if the practitioner is registered.
- **Familiarity with community practitioner**—Pharmacists often become familiar with the prescribing habits of local community practitioners. If a pharmacist receives a suspicious prescription that is deemed out of the “regular” prescribing habits of a known practitioner, the pharmacist may use other tools to help determine the validity of the prescription.
- **Signature file**—If there is question as to the validity of the Practitioner’s signature on the prescription, signatures on filled prescriptions can be reviewed in an attempt to compare signatures. Some pharmacies maintain a paper file of practitioner signatures to assist in the verification process.
- **Phone trees**—Structured phone trees are a common tool used by pharmacies to notify one another of a “bad” doctor, patient, or other person involved in diversion. In addition, messages are often sent via electronic mail and facsimile to pharmacies warning them of some possible techniques and persons involved in diversion.
- **Miscellaneous**—There are some additional indicators of diversion that a pharmacist must pay particular attention to:
 - Practitioner is writing more controlled substance prescriptions than other practitioners in the same specialty
 - Practitioner writes prescriptions for stimulants and depressants at the same time for the same patient.
 - A patient returns too frequently to the physician or visits a variety of physicians in order to obtain the drugs and quantities desired.

Exhibit 2-4 is a diagram of the verification and dispensing processes at the pharmacy.

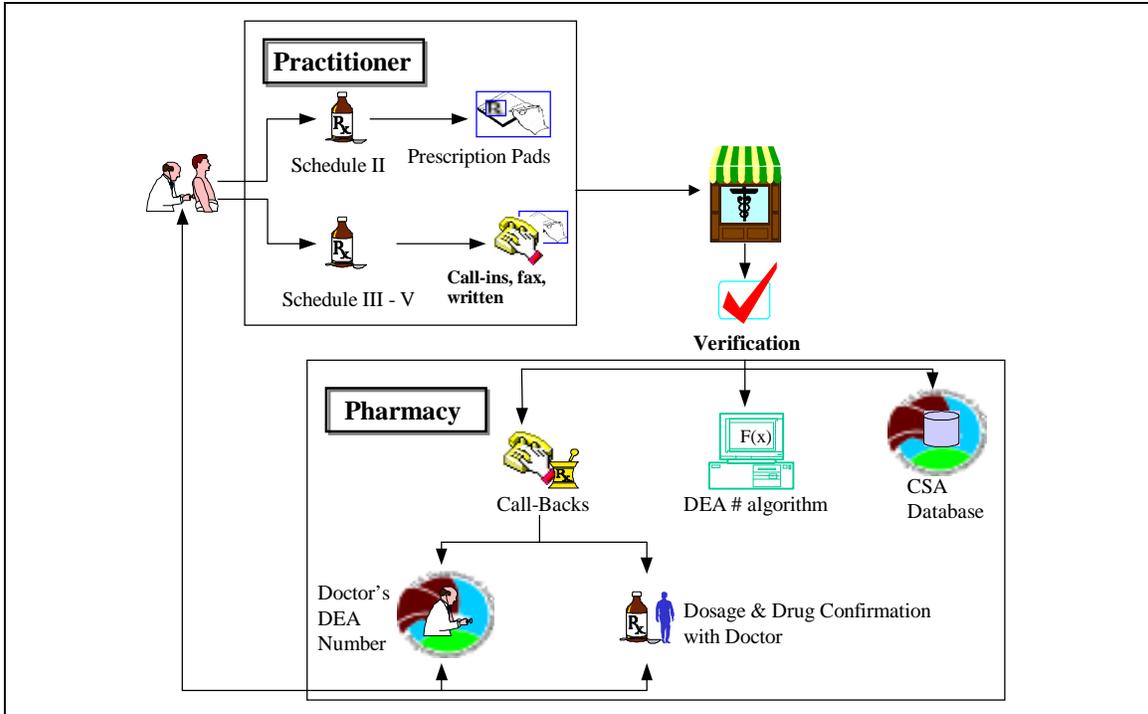


Exhibit 2-4. Pharmacy verification process

2.1.5 Record Keeping

Record keeping is an important requirement of the controlled substance dispensing process. The current record keeping environment is regulated by the DEA and by State Controlled Substance Authorities.

CFR §1304—Records and Reports of Registrants—details the DEA requirements regarding how a pharmacy must maintain controlled substance records. These records must be kept for a period of two years from the date of dispensing and must be available for inspection and copying by an authorized DEA employee. The prescription records must be maintained at the registered location. Schedule II prescription records must be kept separate from all other prescription records. Records of Schedule III-V substances can be kept separately from all other pharmacy records, or they can be maintained with the other records provided they are kept in a “readily retrievable” format—where they can be easily distinguished from all other records (CFR § 1304.04 (h) (2)).

The name or initials of the dispensing pharmacist are required on the prescription after filling. Some states have enacted additional laws and regulations that affect a pharmacy’s record keeping requirements, for example some states require:

- Assignment of a unique serial number to prescriptions prior to record filing
- At the end of his shift, the pharmacist signs a log of prescriptions he dispensed

The DEA requires pharmacies to retain paper prescription records for at least two years. States may require that prescriptions be kept longer.

2.1.6 Current Reporting Systems

The DEA works closely with state law enforcement organizations and health regulatory agencies in their joint mission to prevent the diversion of controlled substances. State laws and regulations vary from state to state. Some states have adopted the Federal laws and regulations, while other states have developed more stringent laws and regulations.

A number of states have adopted prescription monitoring programs—systems for reporting the prescribing and dispensing of specific controlled substances. Changes in prescription transmission methods could affect state monitoring programs. In addition, data collected by state agencies vary from state to state. There are two basic approaches to the reporting of controlled substance prescription data.

- **Multiple Copy Prescription (MCP) Programs**—States that mandate MCP programs preprint prescription pads. Some states have duplicate copy prescription pads, while others use triplicate copies. States with duplicate MCP programs require the pharmacy to maintain one copy and forward the second copy to the state authority. States with triplicate MCP programs require the prescriber, the pharmacy, and the state authority to each have a copy of the prescription.
- **Electronic Data Transmission (EDT)**—Some states have developed EDT prescription monitoring systems as a mechanism for reporting prescribed and dispensed controlled substances. These electronic systems differ from MCP programs in that the prescription information is transmitted electronically by the pharmacy to the state authority. The media on which the data is sent to the state authority can vary. Reports to an EDT prescription monitoring system can be submitted on-line, via a secondary storage device (CD ROM, Tape, etc.), or a Universal Claims Form (UCF)—for those who do not have the resources to electronically submit prescription data.

Additionally, some states issue serialized single, duplicate, or triplicate controlled substance prescription forms to add oversight. Some states have both MCP programs and EDT prescription monitoring systems. Seventeen states currently have prescription monitoring programs. Fourteen other states are planning or developing some type of monitoring program. Exhibit 2–5 illustrates the current status of state prescription monitoring programs.

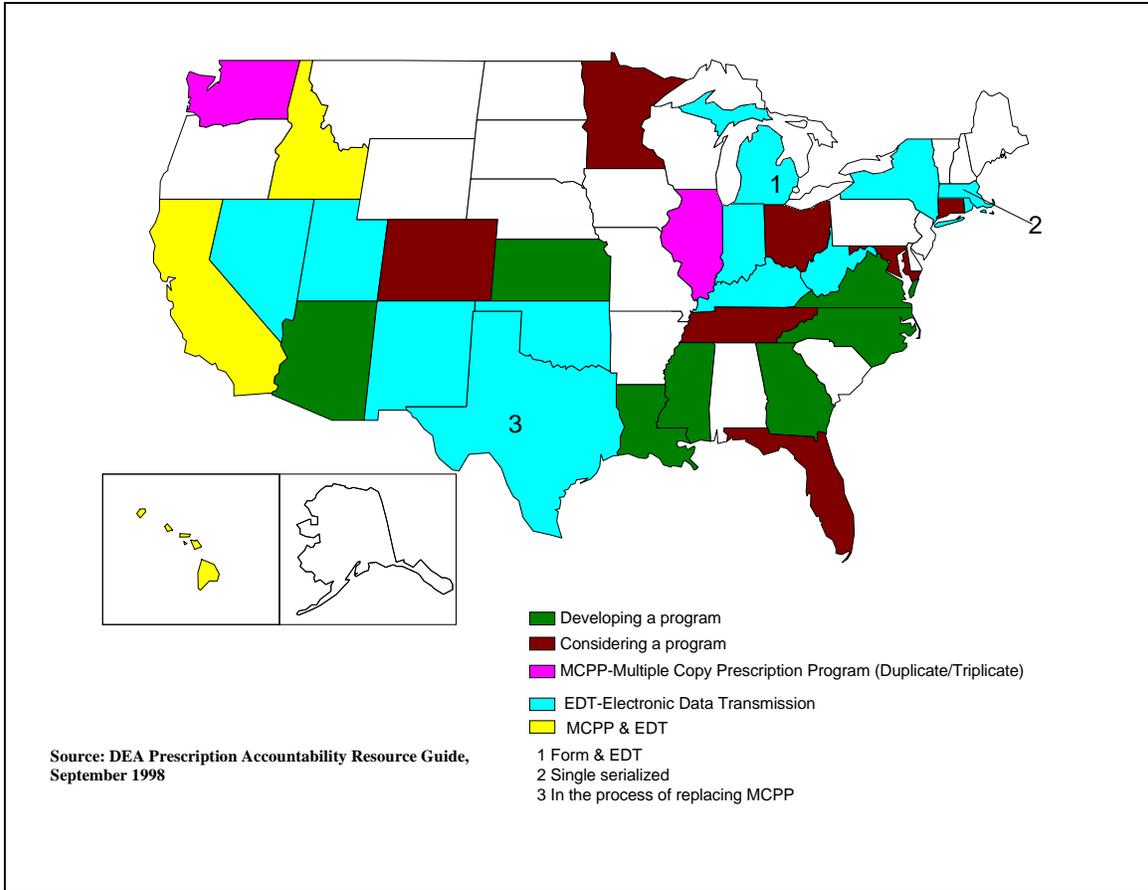


Exhibit 2-5. State prescription monitoring programs

2.1.7 Current Use of Electronic Prescriptions

Currently, thirty-three states permit the electronic transmission of prescriptions between a practitioner and a pharmacy. The transmission of Schedule II prescriptions via electronic transmission is currently prohibited. While a majority of states allow the use of electronic prescriptions, only a small percentage of practitioners and pharmacies are currently using electronic prescription systems. Initial survey results indicate that the majority of all electronic prescriptions occur in three states (Arizona, Texas, and Florida). In these areas, only a very small number of doctors are using these systems. Electronic prescriptions are being used primarily to automate refill requests. That is, pharmacies requesting practitioners to authorize refills for prescriptions. It was estimated that 88% of all electronic prescriptions transmitted today are for refills. Exhibit 2-6 details the current status of state acceptance of electronic prescriptions. As shown, a majority of the states allow electronic transmission of prescriptions. Indiana is currently drafting regulations that would allow this process. States like Montana, Pennsylvania and Alaska have not addressed allowing electronic transmission of prescriptions.

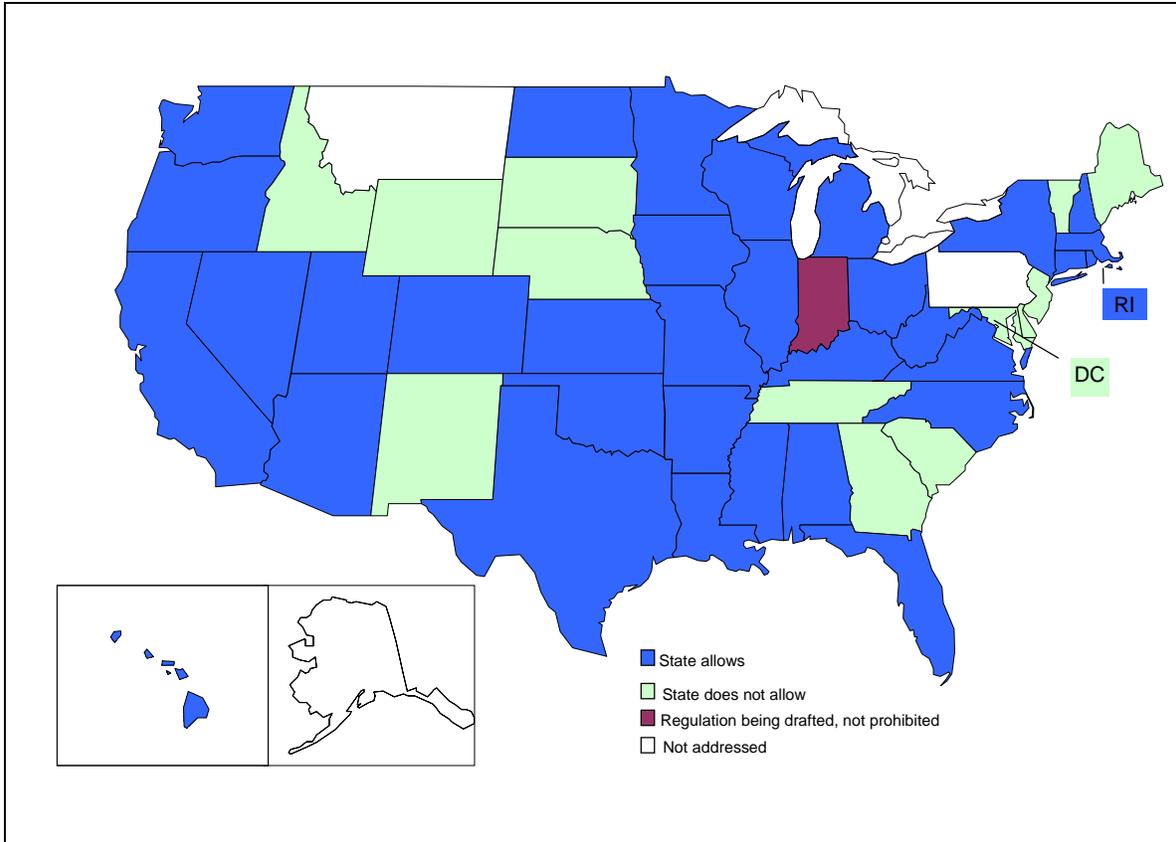


Exhibit 2-6. Electronic prescription allowances among states

2.2 Considerations for the adoption of Electronic Prescriptions

Information collected generally fell under two categories. First—as documented in Section 2.1—the business activities of the stakeholders as related to the prescription process were identified. Second—as provided in this section—the features desired by the stakeholders were determined.

2.2.1 Stakeholder Perceived Benefits

The goal of the Electronic Prescription PKI program is to develop standards and a design concept for the electronic transmission of Schedule II-V controlled substance prescriptions. Adoption of electronic prescriptions for controlled substances will be predicated on a number of factors including; 1) how the technology satisfies legal and regulatory requirements, 2) how it reduces costs and saves time, and 3) the complexity of integrating the technology into current workflow. Specific benefits have to be identified by the stakeholders before they can be expected to support electronic prescriptions.

Exhibit 2-7 illustrates where industry and state representatives see the biggest benefits of electronic prescriptions. All of the stakeholders see the reduction of illegibility as the number one advantage. Practitioners and pharmacists, in particular, see this as a benefit since it will decrease the number of prescriptions that pharmacists cannot read—medical

mistakes can occur when the pharmacist misreads the prescription. Industry indicated that workflow would be enhanced by the reduction of paperwork, providing faster and more accurate service to the patient—thus increasing patient satisfaction. Law enforcement and regulators indicated that the greatest benefits of electronic prescriptions are the reduction of illegibility and the expected reduction of diversion.

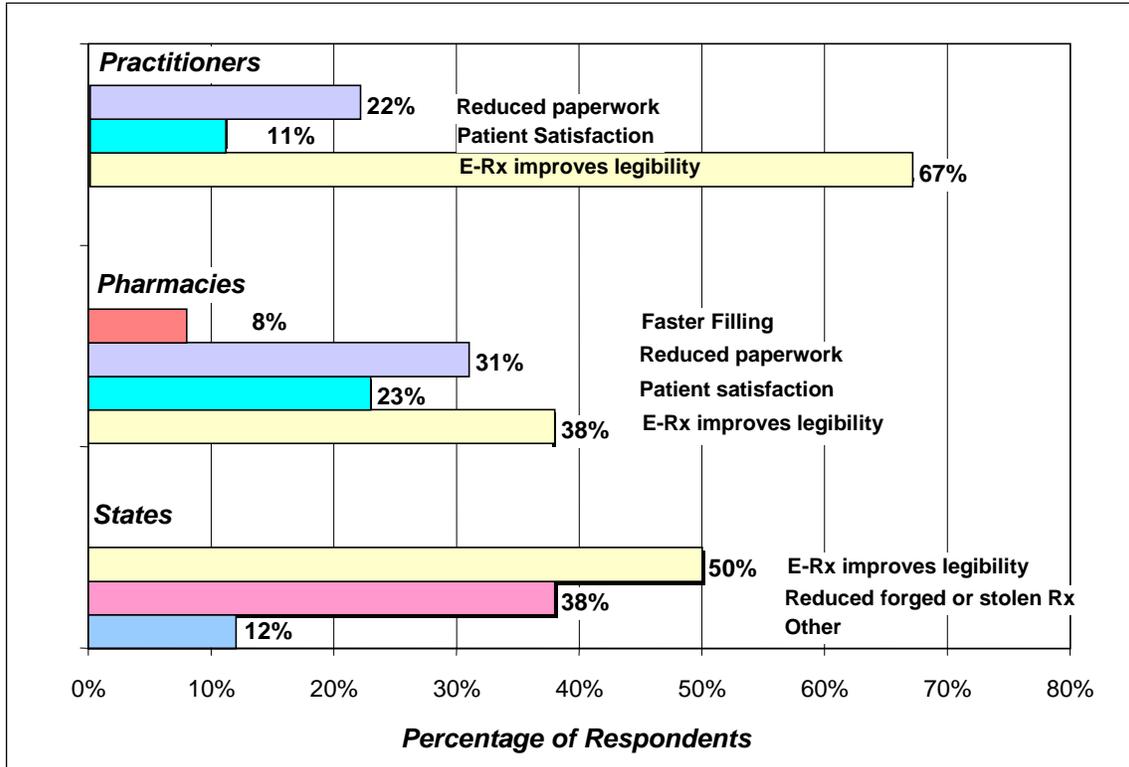


Exhibit 2-7. Benefits of electronic prescriptions

How to read exhibits 2-8 through 2-13

During the interview process, industry and law enforcement/regulatory representatives were asked about the benefits that would be derived from the use of electronic prescriptions. These responses were ranked during the interview process and are illustrated in Exhibits 2-8 through 2-13. As seen in these exhibits, responses from the interviewees were given values between “1” and “8”; where “1” indicates greatest perceived benefit and “8” indicates the least benefit. The columns of the exhibit graphs are the responses obtained during the interviews. If the “1” column for pharmacist indicates 30% for ranking, then thirty percent of the pharmacist/pharmacy representatives thought that the factor/benefit was of greatest value compared to the other factor/benefits.

2.2.1.1 Reduced Paperwork Burden

The benefits of the electronic transmission of prescriptions must be viewed not only in the context of security but also as improving office workflow and productivity. The goal of achieving the “paperless office” has been elusive. PKI provides the tools needed to accomplish it. As seen in Exhibit 2-8, pharmacy representatives and practitioners find that reducing the paperwork burden would be advantageous. Thirty percent of the pharmacist and twenty-three percent of the practitioners rank this as being the greatest benefit of electronic prescriptions. This is due to the enormous volume of paper prescriptions that are filled or refilled, therefore creating a need for a more efficient method. The states on the other hand do not see reducing paperwork as a major benefit—states ranked this benefit near the bottom. Thirty-three of the state representatives ranked this factor the fifth most important out of seven factors.

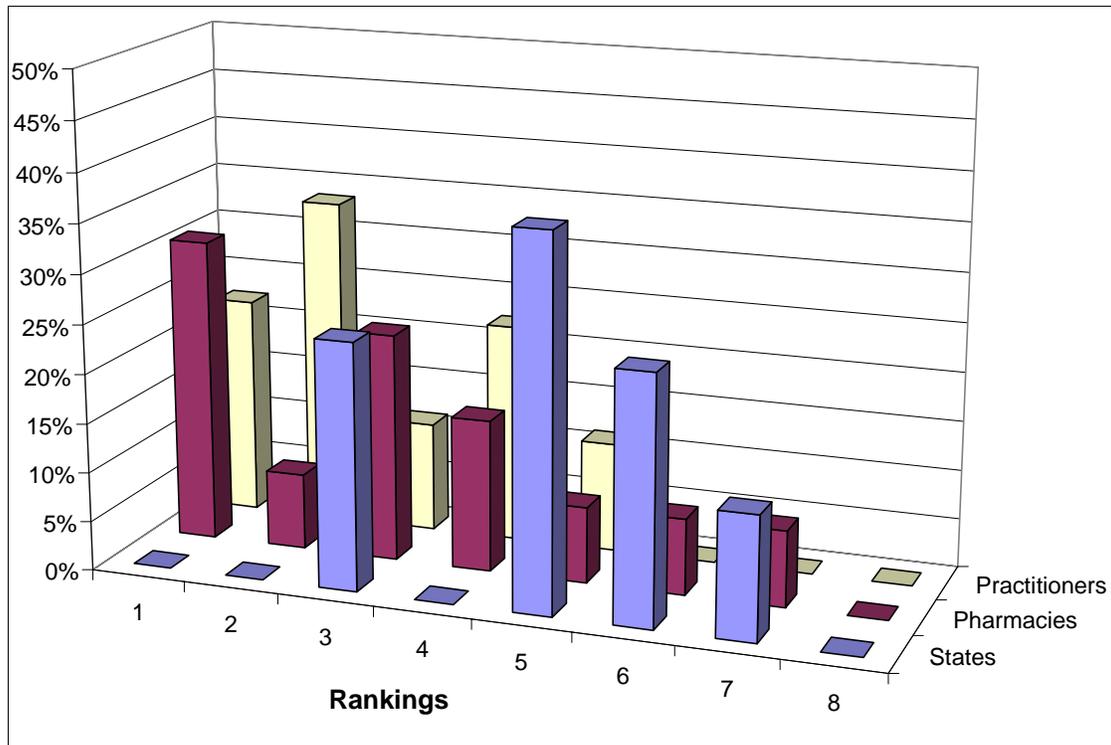


Exhibit 2-8. Reduced paperwork burden

2.2.1.2 Faster Filling

Faster filling allows the patient to receive prescriptions quicker by improving process workflow. Businesses realize improved profit margins by improving workflow efficiency. However, as seen in Exhibit 2-9, faster filling is not a high priority for any of the stakeholders. Surprisingly, they ranked it near the bottom of the list of possible benefits due to the fact that benefits such as illegible prescriptions are more of an issue.

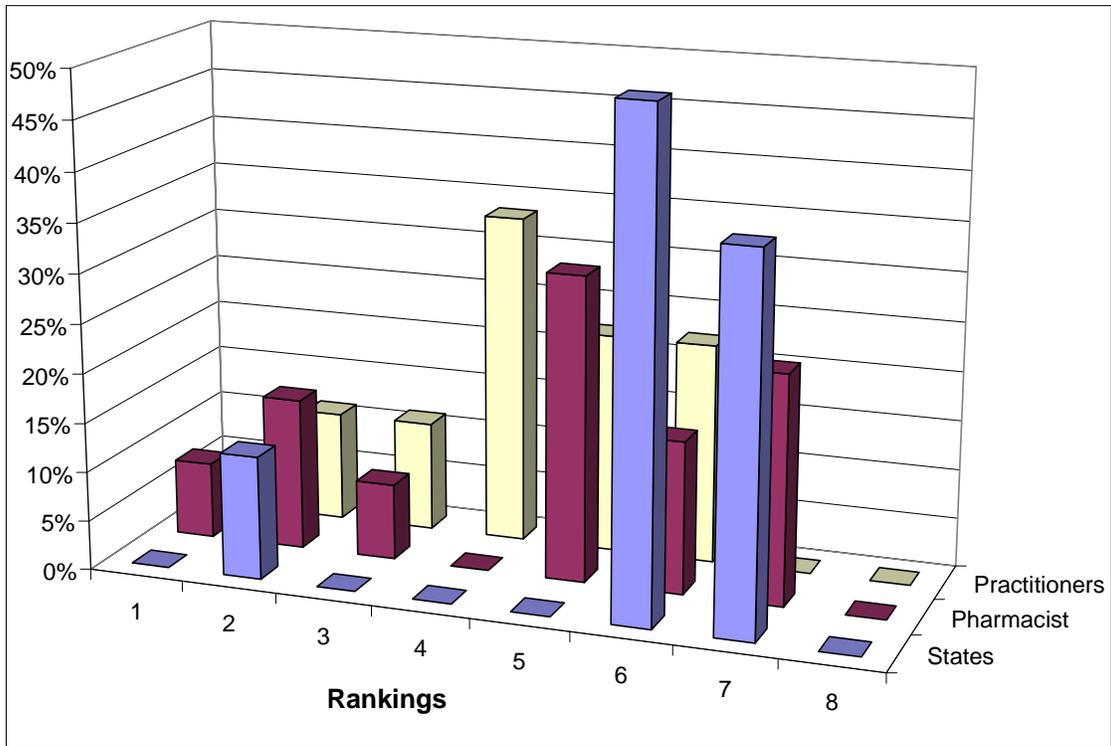


Exhibit 2-9. Faster filling

2.2.1.3 Patient Satisfaction

As shown in Exhibit 2-10, states and practitioners think that overall patient satisfaction is not one of the top benefits of electronic prescriptions, whereas pharmacists are mixed. Some stakeholders see this as being very important—a satisfied customer will most likely revisit the same pharmacy. However, other pharmacists feel that overall patient satisfaction is not as important in relation to the other benefits.

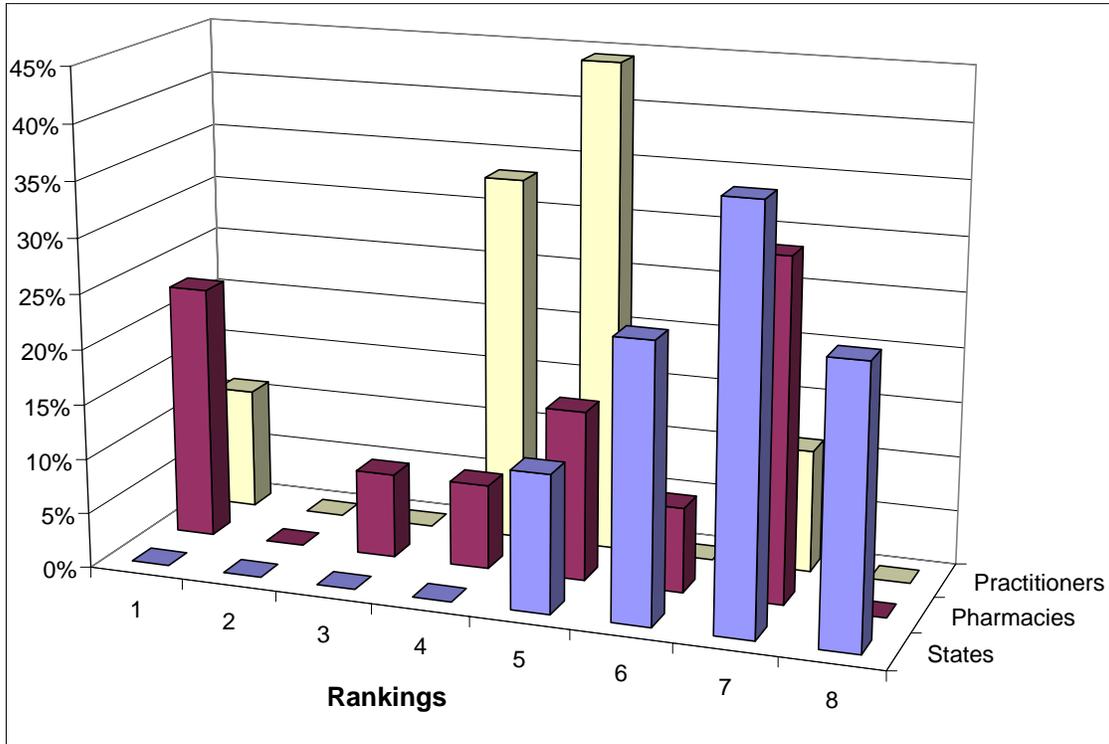


Exhibit 2-10. Patient satisfaction

2.2.2 Existing Security Standards/Environment

The Certificate Policy under which the PKI will operate must reflect the real world security requirements and practices of DEA and the regulated industry. A significant part of the interview process was devoted to determining the actual level of security at which the stakeholders currently operate. This current level of security is, at least, a baseline for determining the security requirements.

Initial project discussions with DEA made it clear that security requirements for electronic transmission would not be less than the current level of security. That is to say that the introduction of this allowance could not bring about a reduction in the security services necessary for DEA and states to perform their regulatory function. The same discussions also included cautions that enhancements to existing security would have to be carefully considered so as not to conflict with other project goals such as industry acceptance.

Another significant driving force is the burden of the “corresponding responsibility” that is placed on pharmacists to ensure that the controlled substance prescription is valid. Currently, pharmacists do not have a good set of tools to certify the authenticity of written prescriptions or the practitioner’s authority to prescribe. At present these tools are weak or non-existent.

Enhancements must be consistent with the realities of the current regulatory and political climate. Public Key Infrastructure technology provides the mechanism for ensuring that electronic prescriptions are more secure than their paper counterparts. A PKI offers the security services of confidentiality, authenticity, integrity, and technical non-repudiation.

- **Confidentiality**—ensures that only authorized parties can read a communication; eavesdroppers cannot.
- **Authenticity**—ensures that the originator of a communication is the person claimed and not an imposter.
- **Integrity**—ensures that the content of a communication has not been altered in transit.
- **Non-Repudiation**—ensures that the sender of a communication cannot convincingly deny that there was a collision between the sender’s unique private key and the data being signed, resulting in a unique signature. The legal and policy environment in which this denial takes place is still evolving.

2.2.2.1 Confidentiality

Confidentiality is a concern to industry—confidentiality exists in the current system. Pharmacies are using closed systems for patient prescription information. The only external interactions occur between pharmacy and the chain headquarters and/or the pharmacy benefits manager (PBM)/switch. Issues arise with the electronic transmission

of patient information that replaces the paper prescription that is hand carried by the patient to the pharmacy.

An open system, one that could be accessed by multiple entities, has the potential of providing patient information to anyone with the tools and determination. As shown in Exhibit 2-11, stakeholders did not rank improved patient confidentiality as a major benefit of PKI-based electronic prescriptions for controlled substances. There were some concerns that electronic prescriptions might put patient information at risk. The concern is that electronic prescriptions might degrade patient confidentiality and that there must be a mechanism to limit access to patient records/information. DEA has no mandate to regulate or enforce patient confidentiality. Any PKI Pilot would of course be required to comply with regulations issued by any other federal authorities—such as the Department of Health and Human Services—which address patient confidentiality.

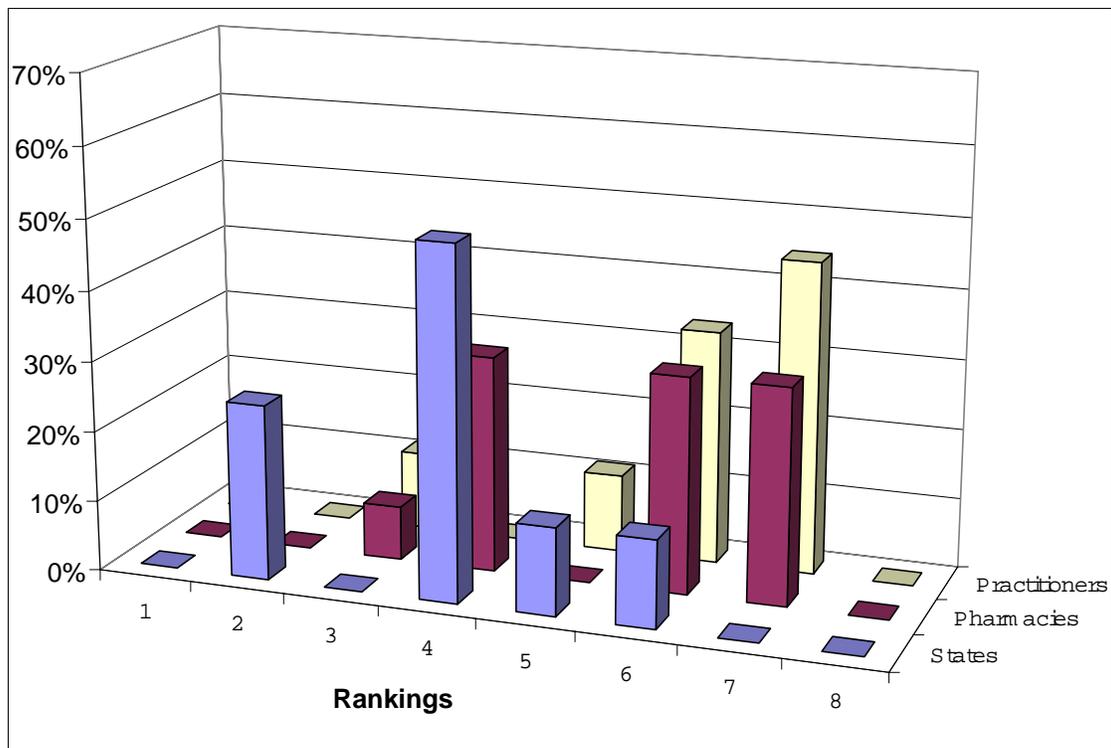


Exhibit 2-11. Patient confidentiality

2.2.2.2 Prescription Authenticity

Authenticity ensures that the originator of a transaction is the person claimed to be and not an imposter. As mentioned earlier, pharmacists have a corresponding responsibility to ensure that a prescription is valid. As found during the interviews, determining the validity of a prescription currently is not an easy process, especially during evenings or weekends when the practitioner’s office is closed. Pharmacists who accept PKI-enabled electronic prescriptions will be able to better authenticate the practitioner; that is, to ensure that the practitioner was the originator of the script and not an imposter/forgery. As can be seen from Exhibit 2-12, pharmacists found this to be a very positive benefit. Responses from practitioners were mixed. Two-thirds of practitioners did not rank this benefit high in terms of importance.

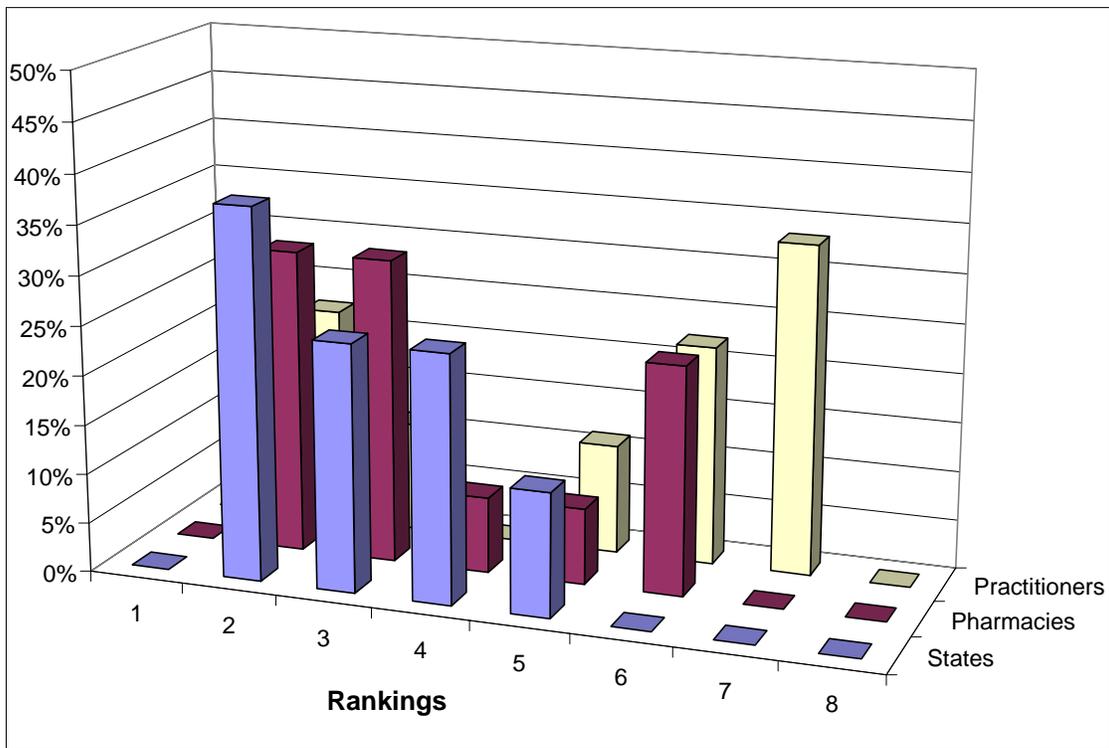


Exhibit 2-12. Provide tools for authentication

2.2.2.3 Prescription Integrity

Integrity ensures that the content of a communication has not been altered in transit. All of the stakeholders interviewed agreed that an electronic prescription secured with PKI would make the diversion of controlled substances by an outside party very difficult. There were some concerns that hackers might eventually find ways to subvert this technology. It was also noted that there is still a corresponding responsibility on the part of the pharmacist, as discussed earlier in this section, and the pharmacist will still be required to ensure that the prescription is appropriate to the condition before filling it.

The results of the interviews yielded common thoughts and comments on the current methods of diversion for controlled substances. An electronic method for transmitting controlled substance prescriptions should preclude these currently used diversion methods. As seen on Exhibit 2-13, law enforcement and regulatory representatives interviewed indicated that the PKI enabled electronic prescriptions would address the problem of forged or stolen prescriptions.

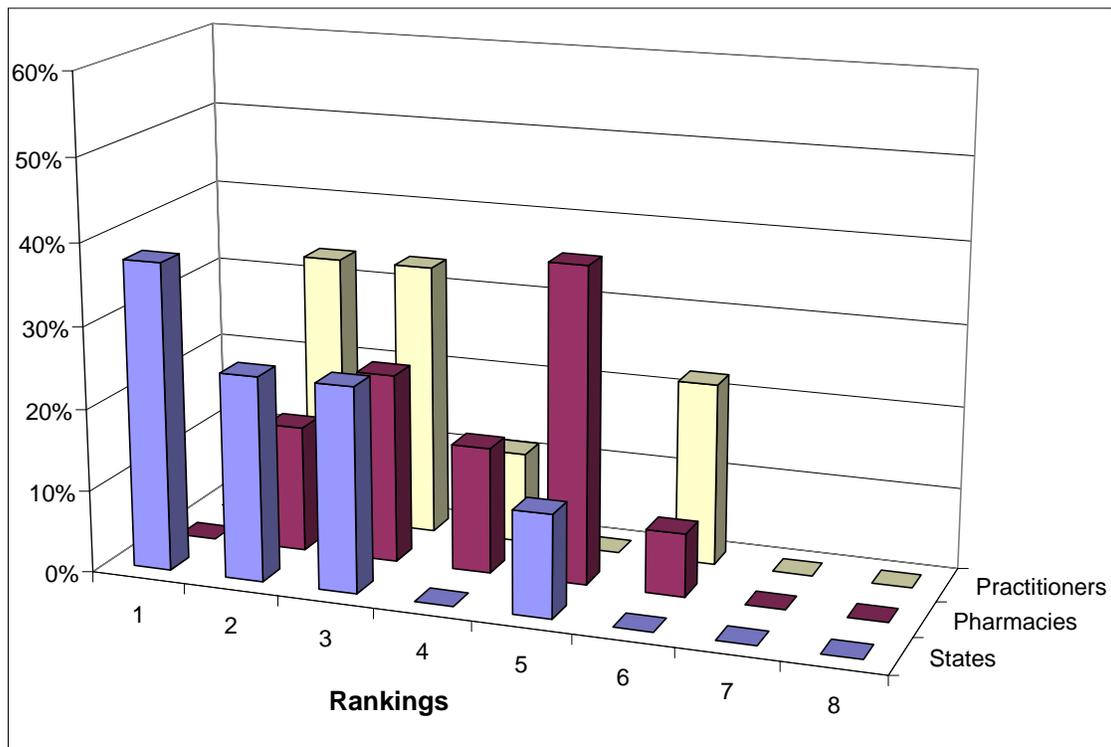


Exhibit 2-13. Reduced forged/stolen scripts

2.2.2.4 Non Repudiation

Repudiation occurs when an individual denies involvement in a transaction. In the paper-world, individuals' written signatures legally bind them to their transactions (for example, credit card charges, business contracts, etc.). The signature prevents repudiation of those transactions. PKI-based digital signature replaces pen-based signature in the electronic world.

State organizations indicated that to ensure authenticity and non-repudiation, a password alone will not be sufficient to ensure that the parties involved in the transmission of an electronic prescription are who they claim to be. Stakeholders suggested the use of tokens or biometrics. Tokens—including smartcards—are portable devices that are used to store the user's profile or certificate information. Requiring the user to authenticate using a biometric technique can further guard access to the information on the card. Biometrics could include thumbprints, iris recognition, or facial scan for example.

2.2.3 Factors that Influence Adoption of Electronic Prescriptions

As previously stated, success of this project hinges on stakeholder acceptance and adoption of PKI-enabled electronic prescriptions to replace or augment current business practices. DEA is not mandating that pharmacies and practitioners use this technology. Therefore, electronic prescriptions must incorporate functionality and have attributes that are important to the users that will eventually adopt this method of transmission. During the interview process, stakeholder comments were solicited regarding what features and functionality are important to them when considering electronic prescriptions.

2.2.3.1 Industry Adoption Factors

Correlations become apparent between the stakeholder groups when analyzing the data. Pharmacies and practitioners—which are considered industry for this project— contend with similar pressures including: aspects that affect business practices, workflow, and profit/loss. Factors that affect industry's adoption of an electronic method include:

- **Affordability/Cost** – Capital expenditures for equipment and software must be reasonable. An electronic method for transmitting prescriptions would need to be affordable to all interested users.
- **Patient Confidentiality** – As seen in Section 2.2.2.1, patient confidentiality is currently not a problem. Current business practices protect patient records and information. Electronic prescriptions will need to protect patient information by limiting access to patient prescription information.
- **Security** – Electronic prescriptions will need to have strong security features built in so that compromise of the system cannot be easily achieved. Participants do not want to have increased liability as a result of using electronic prescriptions.

- **Ease of Use** – An electronic method for transmitting prescriptions must be easy to use and cannot be cumbersome. Operations must be simple and easy to understand for the method to gain widespread adoption.
- **Improved Workflow** – The use of electronic prescriptions must provide the advertised benefits of a ‘paperless office’ environment. Benefits of this improved workflow include faster prescription filling, a reduction in the amount of time spent on the phone for prescription verification, reduced paperwork, and improved patient service

Examination of the factors industry requires for adoption has also yielded unique requirements for both practitioners and pharmacists. Practitioners do not want unrealistic restrictions that would affect business process and would like easy enrollment. Pharmacies, on the other hand, require a system that is reliable, one that provides better tools for verification of prescribers, and one that would be able to be integrated into current information technology architectures.

2.2.3.2 Regulatory/Law Enforcement Adoption Factors

There are also correlations that can be drawn between DEA and state regulatory/enforcement organizations. Factors for law enforcement to adopt an electronic system include:

- **Secure Environment** – An electronic prescription system needs strong, built-in, security features so the system cannot be easily compromised. There was concern that the electronic prescription system may be vulnerable and result in increased diversion if the system was hacked into.
- **Acceptance of Technology by Courts** – As more thoroughly discussed in Section 3.4, the legal basis for the use of electronic prescriptions has not been unequivocally defined by current Federal legislation. Law enforcement is primarily concerned with the ability to enforce the law in situations where diversion occurred.
- **Multi-Factor Authentication** – Law enforcement offered different thoughts about this issue; however, with the common theme that password-based authorization is not enough. One factor authentication requires just a password or perhaps just a biometric. Theft of the password would give unauthorized individuals access to the end entity’s private key. It was suggested that smartcard/tokens and/or biometrics be used in conjunction with a password to authenticate users.
- **Investigative Tools** – With the adoption of electronic prescriptions, the lack of written evidence would result in increased difficulties in tracking the chain of custody of the prescription transaction. An electronic system would need to provide tools that identify chain of custody. Included in this is the availability of audit logs to track computer access.

2.3 Regulatory/Legal Environment

To fully evaluate the impacts of using electronic prescriptions for controlled substances, - government regulations and mandates must be examined. Under the current prescription process, the parties involved (prescriber and pharmacist) assume responsibility and liability based on their role in the process. Mechanisms are in place to bind the identities of both the practitioner and dispenser using wet signature, federal/state registration, and other credentials. The adoption of an electronic prescription system will test the ability to bind the identities of the practitioner and dispenser. The acceptance of electronic prescriptions can be tied to the soundness and acceptance of the enabling technology.

- Digital signature is recognized as the most capable technology to provide an alternative to ink signatures.
- With the increased need for paperless systems, several states have begun to adopt legislation for the acceptance and regulation of digital/electronic signature technology. Some examples are in Texas, Washington, Minnesota, and Utah. All of these states have laws governing the operation of Certification Authorities for PKI. Only CA's that meet those guidelines are recognized to issue digital certificates that will have legal authority.
- The Federal government has begun to define, regulate, and accept digital/electronic signature through the introduction of new bills and the writing of Federal regulations. Two most recent actions in Congress are:
 - The Senate passed the "Millennium Digital Commerce Act" on 11/19/1999.
 - The U.S. House of Representatives passed the "Electronic Signatures in Global and National Commerce Act" on 11/09/1999.
- Federal initiatives are scrutinizing digital signature not only on the cryptography of the technology but also the policies governing the operation and maintenance of the systems that employ such technology.

Appendix D provides a more in-depth discussion of the regulatory/legal environment.

Section 3 – Policy Requirements Foundation

This section provides the foundation of the security policy and discusses the definitions and standards that pertain to the classification of Certificate Policies by levels of assurance and security.

3.1 Certificate Policy (CP)

The X.509 Standard defines a CP as “a named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements.”

Request For Comment (RFC) 2527 is the Internet Engineering Task Force (IETF) standard for the format and content of a CP. It is widely accepted as the US Government and US Industry/Commercial Standard. It is a line-by-line standardization of the “named set of rules.” RFC 2527 also defines the CPS. The CPS is a more detailed description of the practices followed by a Certification Authority (CA) to implement a CP. A CP is a document intended for the public, the users and the relying parties; it is normally published in the same Repository that the CA’s certificates are published. The CPS is generally not a public document, and may contain details of organizational operations that must not be disclosed.

It is explained in the RFC 2527 that when a CA issues a Public Key Certificate to an entity, the CA cryptographically binds a public key value to a set of information that identifies that entity. The entity can be a human user, an organization, or perhaps some item of equipment. The entity is considered the subject of the certificate. The CA certifies that the entity holds the private key value corresponding to the public key value in the Public Key Certificate. A Public Key Certificate is used by a “certificate user” or “relying party” that needs to use, and rely on the accuracy of, the Public Key Certificate. The user wants to verify a digital signature of a certificate subject and/or encrypt information for the certificate subject.

For emphasis, it is re-stated here that the fundamental assumption of PKI is: the subject of a public key does hold the corresponding private key. The CA establishes this through a Proof of Possession Protocol (POP) test/assumption. The proof of possession test/assumption can range from very weak to very strong.

Request For Comment 2527 further explains the degree to which the certificate user can trust the Certification Authority’s binding of the public key. The trust depends on several factors. These factors include: the practices followed by the Certification Authority in authenticating the identity of the subject of the certificate; the Certification Authority’s operating policy, procedures and controls; the subject’s obligations, particularly those in connection with protecting the private keys and reporting them lost or compromised; and the stated undertakings and legal obligations of the Certification Authority such as warranties and limitations on liabilities.

The degree to which a prudent user should trust the Certification Authority's binding of public key and subject of certificate is best measured by the Level of Assurance/Security at which the Certification Authority is operated.

3.2 Levels of Assurance/Security

There is no universally agreed upon standard for the syntax or semantics to be used in describing levels of assurance and security at which a PKI is operated. There exists a Government of Canada (GOC) standard and an evolving U.S. Government standard, based very closely on the Government of Canada standard. The levels in both are: Rudimentary; Basic; Medium; and High.

In the Request For Comment 2527 format for a Certificate Policy there is a large set of items recommended for inclusion. The items each have relevance in determining or describing the level of assurance at which a Certification Authority operates. Each item should be at least considered by the Certificate Policy writer. The items that are relevant should be completed in detail. The items that are not relevant may be noted as "no stipulation." Set forth below is a short list of issues, derived primarily from the items of the standard. Item (13) is not drawn from the standard but is included to provide a simple threat context for the evaluation.

Determining how a Certificate Policy addresses a very similar subset (1) - (13) of these significant issues is a shorthand method under consideration by the Federal PKI (FPKI) Steering Committee for determining the overall level of assurance that a Certificate Policy is written to. For the purposes of this analysis we have adopted this approximation of the Federal PKI semantic framework.

	Issue	Rudimentary Level	Basic Level	Medium Level	High Level
1	Certification Authority action if private key is lost or compromised	Certification Authority does not bother to revoke end-entity certificates if private key is lost or compromised; no CRL is published	Certification Authority does revoke end entity certificate if private key is lost or compromised, and CRLs are published at least every 24 hours; 6 hours if Certification Authority's private key is compromised	Certification Authority does revoke end entity certificate if private key is lost or compromised, and CRLs are published at least every 12 hours; 2 hours if Certification Authority's private key is compromised	Certification Authority does revoke end entity certificates if private key is lost or compromised, and CRLs are published every 4 hours; ½ hour if Certification Authority's private key is compromised
2	Division of authority/capability among Certification Authority personnel (i.e. N person integrity)	All critical Certification Authority functions can be performed by one person	All critical Certification Authority functions must be performed by at least 2 people	All critical Certification Authority functions must be done by at least 3 people	All critical Certification Authority functions must be accomplished by at least 3 people
3	Certificate validity period	Certificate duration for signature key is up to 6 years if CRLs are published; one year with no CRLs published	Certificate duration for signature key is up to 4 years	Certificate duration for signature key is up to 2 years	Certificate duration for signature key is up to 1 year
4	Backup of Certification Authority and end entity keys	Certification Authority and end-entity private key is not backed up; no requirement for confidentiality private key	Certification Authority and end-entity signature keys must not be backed up; confidentiality private keys are backed up	Certification Authority and end-entity signature private keys must not be backed up; confidentiality private keys are backed up	Certification Authority and end entity signature private keys must not be backed up; confidentiality private keys must be backed up

Exhibit 3–1. Federal PKI semantic framework

	Issue	Rudimentary Level	Basic Level	Medium Level	High Level
5	Interval between request and issuance of certificate	No stipulation	End-entity certificates issued within 5 days of request by Registration Authority	End-entity certificates are issued within two days of request by Registration Authority	End-entity certificates are issued immediately upon request by Registration Authority
6	External auditing	External audit for compliance with Certificate Policy is performed every three years	External audit for compliance with Certificate Policy is performed every 2 years	External audit for compliance with Certificate Policy is performed every year	External audit for compliance with Certificate Policy is performed every year
7	Naming requirements	End entity certificates do not require distinguished names	End entity certificates require distinguished names	End entity certificates require distinguished names	End entity certificates require distinguished names
8	Proof of possession protocols	End-entities do not have to prove possession of private key to obtain certificate	End-entities do have to prove possession of private key to obtain certificate	End entities do have to prove possession of private key to obtain certificate	End entities do have to prove possession of private key to obtain certificate
9	Certification Authority standard for proof of identity from certification applicant	End entity identity proofing is not required; registration can be done in person or on-line	End entity identity proofing is required; it can be done on-line or in person to an Registration Authority, 2 forms of ID required	End entity identity proofing for certificate issuance required; it can be done on-line or in person; it requires two IDs including at least one picture ID issued by a Government entity	End entity identity proofing for certificate issuance required; requires <u>personal appearance</u> with two IDs including at least one a picture ID issued by a government entity

Exhibit 3–1. Federal PKI semantic framework (Continued)

	Issue	Rudimentary Level	Basic Level	Medium Level	High Level
10	Requirements for Certification Authority record maintenance	No requirement as to how long Certification Authority activity records must be maintained	Certification Authority activity records must be maintained for at least 7.5 years	Certification Authority activity records must be maintained for at least 10.5 years	Certification Authority activity record must be maintained for at least 20 ½ years
11	Asymmetric key length modulus	No requirement on asymmetric key modulus	Keys must have the security equivalent of 1024 bit RSA modulus	Keys must have the security equivalent of 1024 bit RSA modulus	Keys must have the security equivalent of RSA 2048 bit modulus
12	Certification Authority signing key and end entities private keys protection requirements	Certification Authority signing key and end entities private keys may be in hardware or software	Certification Authority signing key must be in hardware; end entities private keys may be in hardware or software	Certification Authority signing key must be in hardware; end entities private keys may be in hardware or software	Certification Authority signing key and end entities private keys shall be in hardware
13	Extent of damage if the end entity private key compromised	No injury or loss accrues to enterprise from compromise of end entity private key	Injury accrues to enterprise if the end entity private confidentiality key is compromised; it would cause only minor injury if the end entity private signing key is compromised	Serious injury accrues to enterprise if the end entity private confidentiality key is compromised; it could cause significant financial loss or require legal action for correction if the end entity private signing key is compromised	Extreme injury accrues to the enterprise if the end entity private confidentiality key is compromised; it could cause loss of life, imprisonment, or major financial loss if the end entity private signature key is compromised

Exhibit 3–1. Federal PKI semantic framework (Concluded)

3.3 DEA Root Certification Authority Analysis

Currently, the DEA's involvement with controlled substance prescriptions is limited to registering practitioners and pharmacies and regulating the prescription of these substances by practitioners, and their filling by pharmacists. DEA does not wish to increase its involvement beyond this regulatory role. However, there are advantages to the DEA in operating a root Certification Authority (CA) as will be shown below.

The main issues addressed are presented in question/answer form below. The remainder of Section 3.3 provides additional details in support of the findings.

Question 1—What is a Certificate Policy?

According to X.509, a Certificate Policy (CP) is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." A certificate policy is used by a certificate user to help in deciding whether a certificate and the binding therein, is sufficiently trustworthy for a particular application.

The degree to which a certificate user can trust the binding embodied in a digital certificate depends on several factors. These factors include the practices followed by the CA for subscriber identity proofing; the CA's operating policy, procedures, and security controls; the subscriber's obligations (for example, in protecting the private key); and the CA's obligations (for example, warranties and limitations on liability).

The DEA's CP will define the minimum provisions for CA operation that collectively contribute to the level of assurance that DEA will mandate for electronically transmitting prescriptions for controlled substances.

Question 2—What are the implications of an Industry CA not abiding by the DEA's Certificate Policy?

Regardless of the approach, the DEA will need to establish a list of approved CA's (those that have agreed to operate in accordance with the DEA's CP). If an Industry CA fails to enforce the DEA's Certificate Policy, then there is the potential for the following to occur:

- Inadequate identity proofing by the Industry CA could lead to the issuance of certificates to non-registrants or non-pharmacists.
- Failure of the Industry CA to publish the CRL in a timely manner could provide relying parties with an erroneous picture of a registrant's status.
- Failure of the Industry CA to operate with proper personnel controls could result in a rogue CA administrator issuing bogus certificates.

Question 3—What possible approaches could the DEA take to assure that Industry CAs abide by the DEA’s CP?

The DEA could play a passive role by establishing regulations for Industry CAs and accrediting the CAs to ensure compliance. Under this approach the DEA would make the list of “approved” Industry CAs publicly available. Alternatively, the DEA could take an active role and operate a root CA, thereby empowering the DEA with the ability to revoke subordinate Industry CAs found to be non-compliant with the DEA’s CP.

Question 4—What are the risks of simply regulating Industry CA Certificate Policies?

Risk #1—No Federal Legal Precedent

There is no Federal legal precedent for this approach. Current Federal legislation is focused on approving the use of digital signatures rather than enforcing the CA’s responsibility to abide by the CP. A search of the literature showed no Federal laws that apply any type of penalty to a CA that does not operate in accordance with its CP.

The range of available enforcement methodology is in the formative stages. State laws are somewhat more established. Laws in the states of Utah, Minnesota, Washington, and North Carolina require the CA to license with the state and to periodically submit audit results. In these states, penalties are defined for noncompliance. Exhibit 3.2 summarizes existing state laws that regulate the operation Certification Authorities. Exhibit 3.3 summarizes the steps that are taken to license CAs in the state of Utah.

Details of the law	Washington Ch 19.34	North Carolina Ch 66	Utah Title 46 Ch 03	Minnesota 325 K
Date Law Passed	3/29/1996	8/31/1998	5/1/1995	5/19/1997
Applicability of statute	All Business	Government Business	All Business	All Business
State license is required for CA operation	Y	Y	Y	Y
State enforces requirements for licensed CA	Y	Y (Class I felony)	Y	Y
State has authority to force CA to cease operation	Y	Y	Y	Y
CA is liable for civil actions and punitive damages	Y	Y	Y	Y
CA is liable for all state prosecution/ adjudicating costs during investigation	Y	Y	Y	Y
State can issue a non-compliance warning to a CA	Y	Y	Y	Y
State requires an annual compliance audit and a financial audit	Y	Y	Y	Y
State requires CAs to be bonded (Suitable Guaranty must be demonstrated during license request)	Y (Variable amount)	Y	Y	Y \$100,000 +

Exhibit 3-2. Summary of state digital signature laws

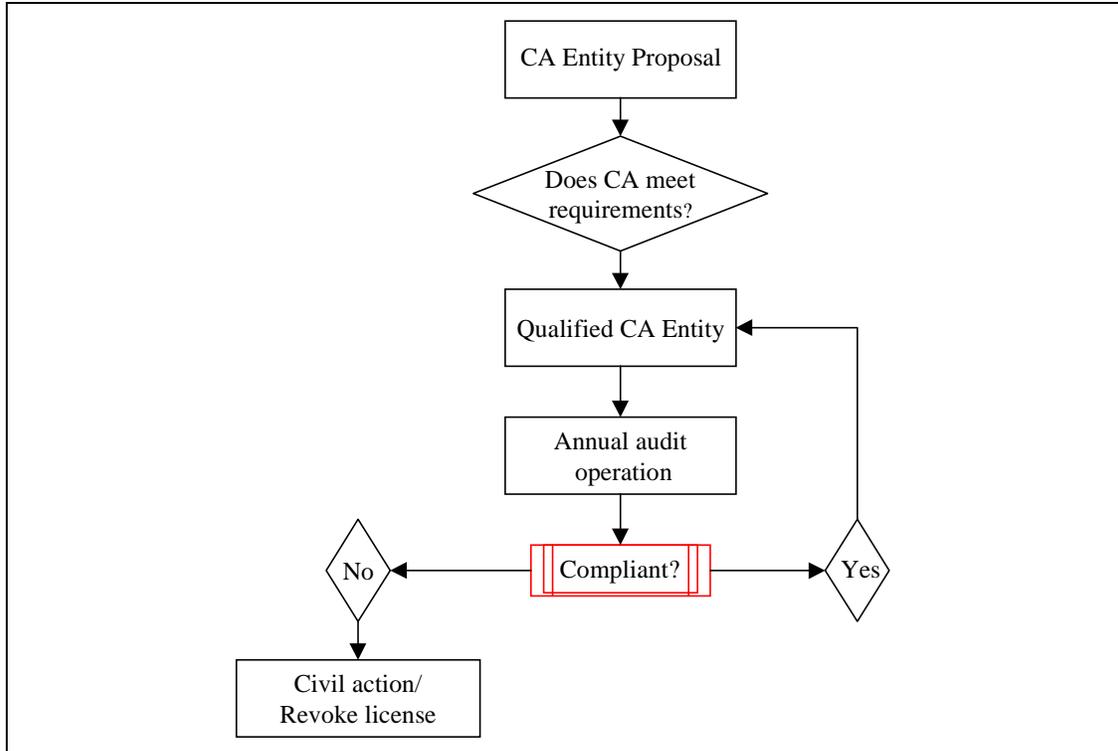


Exhibit 3-3. State of Utah CA licensing process

Risk #2—The practitioner’s choice of Industry CA could restrict the set of pharmacies available to the practitioner for the purpose of transmitting electronic prescriptions.

Left to themselves, DEA approved Industry Certification Authorities could choose to establish trust relationships (cross-certify²) with other CAs for strategic business reasons—not to foster interoperability. Such an environment would not guarantee that all CA’s would “trust” each other and would cause problems should the practitioner’s CA not trust the pharmacy’s CA. This would require practitioners to obtain multiple digital certificates from different CAs to be able to electronically prescribe controlled substances with different pharmacies.

² Cross-certification is a complicated process by which two CAs securely exchange keying information. By doing so, each CA certifies the trustworthiness of the other CA. As a result, users in one CA’s domain trust users in all other CA domains that are cross-certified with their own CA. Cross-certification is much more than a technical exercise. Each CA investigates the other’s security policies, security practices, and learns about the personnel security controls that the other CA employs. Following this period of “due-diligence,” representatives of the CAs will most likely sign a legal agreement before performing cross-certification. This agreement defines the required security policies in both domains and assures both parties that these policies will be followed.

The favored approach should ensure that all CA's are equal, and that "islands of interoperability" do not develop.

Question 5—How can the establishment of a Government root CA help?

The DEA has the authority to take action against registrants. However, it is unclear how DEA regulations would apply to industry operated CAs. Ultimately, the DEA may desire the ability to revoke a CA and all certificates issued by it. By operating a root CA, the DEA would have a mechanism to do this. While such a step would be drastic, it is reasonable to assume that it would only occur after protracted discussions between the DEA and the CA, or after some form of legal action.

The DEA's root CA would issue certificates to approved Industry Certification Authorities. This would result in a single trust domain composed of Industry CAs operating within the DEA's hierarchy. Exhibit 3.4 shows this hierarchy with the DEA CA operating as the root.

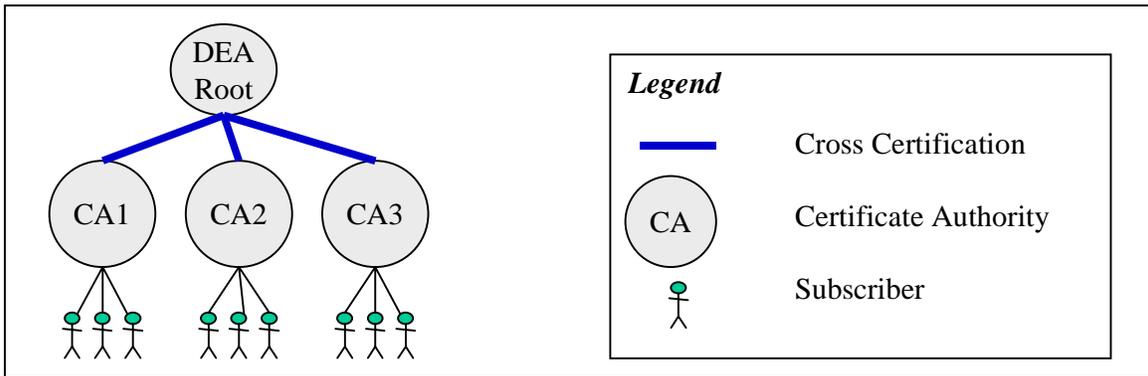


Exhibit 3-4. Hierarchical root CA architecture

Another significant advantage of the Government root CA would be to help ensure interoperability between CAs (as discussed in Question 4).

Question 6—What risks does the root CA approach present to the DEA? How can they be mitigated?

Risk #1—Root key compromise is catastrophic

Since all certificates are based on the root CA's private signing key, its compromise would essentially invalidate all issued certificates. Such an event would require the DEA and all Industry CAs to re-establish the trust hierarchy, and re-issue new certificates to all subscribers. This could result in life threatening situations to patients and, at the very least, would be extremely inconvenient to all parties involved.

The use of strong physical, network, and personnel security safeguards combined with stringent audit requirements would significantly reduce the risk of a compromise.

Industry CAs in operation today mitigate this same risk by employing appropriate safeguards to protect their CA's private signing key.

Risk #2—The root CA must be continuously available to service CA status requests.

Upon receipt of a digitally signed electronic prescription, relying party computer systems will be required to verify the status of the Industry CA that issued the subscriber's digital certificate. This status information is made available to relying parties (upon request) by the root CA in the form of an Authority Revocation List (ARL). The ARL is a signed, time-stamped list of the serial numbers of CA public key certificates (including cross-certificates) that have been revoked.

Based on the large number of prescriptions that are issued every day, it would be unreasonable to require pharmacy computers to perform this check for each and every prescription. Doing so would impose unnecessary workload on the CA and increased response time for relying parties.

An alternative approach would be to allow relying parties to cache the ARL (maintaining a local copy reduces the need to perform a lookup). Such an approach simplifies matters by making the number of ARL status checks a function of the number of pharmacies rather than of the number of prescriptions. This reduces the workload on the CA host system and improves response times for pharmacies and other relying parties. As shown in Exhibit 3–5 by giving the ARL a validity period of one-week (168 hours), the CA would expect to see less than 10 ARL checks per minute. This assumes 51,966³ retail pharmacies nationwide. The chart assumes that all requests fall within a 17-hour period beginning at 8 a.m. Eastern Time and ending at 10 p.m. Pacific Time. The caching period can be increased even more to further reduce this load. If caching were not permitted, the number of requests would be equal to the number of prescriptions—significant planning would be required to build a system capable of handling this workload.

³ NACDS 1999 Industry Profile

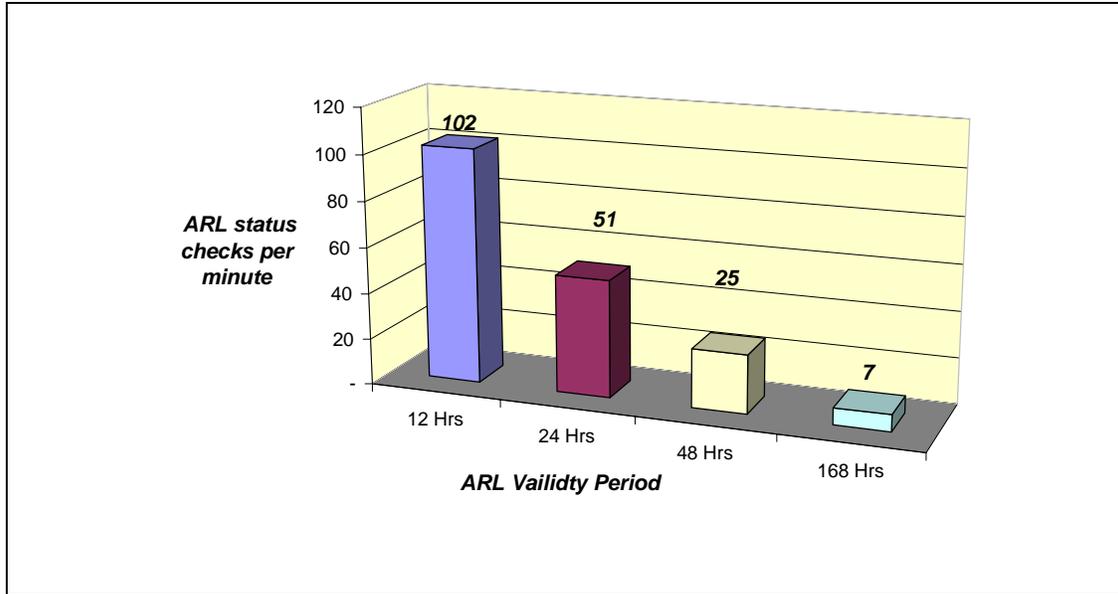


Exhibit 3–5. Impact of ARL validity period on frequency of ARL checks

Question 7—How might Industry react to DEA’s new role?

Surprisingly, industry itself is expected to recommend that the government act as the root of an overarching healthcare PKI to facilitate trust interoperability between CAs. The WEDI/AFEHCT (Workgroup for Electronic Data Interchange/Association for Electronic Health Care Transactions) Internet Encryption Interoperability Pilot—operated during 1999—was conducted to evaluate how digitally encrypted health care data could be transmitted over the Internet. To facilitate trust interoperability between the four participating CAs, a root CA was established. The Pilot report—expected to be released in March 2000—is expected to recommend a government-run healthcare root CA. A DEA root CA would be consistent with this recommendation.

Question 8—How does the root CA alternative compare to others in terms of cost?

All of the alternatives will require the DEA to periodically accredit CAs. DEA could perform the audit itself or accept the results of an out-sourced audit by an accredited accounting firm. Nevertheless, the DEA would need to review the results to ensure compliance.

The recommended root CA alternative will require the DEA to operate and maintain a CA. The root CA will exist for two purposes; 1) to sign Industry CA certificates as these CAs are “approved” and come on-line, and 2) to service infrequent client requests against the ARL—relying parties will need to verify that the CA is still authorized by the DEA on a periodic basis.

Since the operation and maintenance of the root CA does not include subscriber identity proofing or actual certificate issuance to subscribers, the management burden is not expected to be on the same scale as it is for Industry CAs.

3.3.1 Evaluation of Alternatives

Exhibit 3–6 rates the two alternatives against 8 evaluation factors. Each alternative is given a ranking from 1 to 3—with three being the best. Explanations for each rating are also provided.

Evaluation Factor	Regulate only	DEA Root CA
Technical interoperability <i>Will the PKI products used by different CAs interoperate?</i>	+ Technical interoperability between CAs is left to the CAs. No assurance that systems used by the different CAs will interoperate.	++ Technical interoperability with the root improves the chances that an Industry CA will interoperate with other CAs.
Trust interoperability	+ Trust between CAs is left to the CAs. There is no assurance that Certification Authorities will establish trust relationships between each other. Requires cross-certification.	+++ Common root ensures that all participating CAs participate in the same trust domain. Root CA establishes common CP that is adopted by all participating Industry CAs.
Mechanism to approve CAs	++ DEA Certificate Policy would be published in the regulations. DEA would accredit and maintain a list of "approved Industry CAs."	++ DEA Certificate Policy would be published in the regulations. DEA would accredit Industry CAs. These CAs would issue certificates under the DEA root.
Mechanism for relying party to check status of CA	+ Relying party computer system would be required to check the list of approved Industry CAs. DEA would need to publish this information electronically. The details of this process would need to be worked out.	+++ Relying Party computer systems would be required to check the root CA's Authority Revocation List (ARL) at a predetermined frequency as defined by the CP.
Mechanism for the DEA to take action against a CA	+ The Industry CA would be removed from the list of approved CAs.	++ The Industry CA's signing certificate would be revoked. Relying parties will be alerted to this when they routinely check the root CA's Authority ARL.
Consistent with industry recommendations	+	+++ WEDI/AFEHCT Interoperability Pilot will recommend a health care root CA.
Susceptible to root key compromise	Not applicable	- Root Key compromise is catastrophic
Cost to DEA	\$ <ul style="list-style-type: none"> • Accrediting Industry CAs • Making "approved" list publicly available 	\$\$\$ <ul style="list-style-type: none"> • Accrediting Industry CAs • Operating a root CA

Exhibit 3–6. Evaluation of alternatives

Section 4 – PKI Certificate Policy Requirements

This PKI Certificate Policy Requirements section is not a Certificate Policy (CP), rather, it is a statement of the general level of certificate requirements for the PKI. It is based on the analysis of the assurance and security requirements of Industry and law enforcement as determined to date. A CP would contain much more specific detail for those items addressed. It should be noted, further, that not every item recommended in RFC 2527 is addressed. As expressed in RFC 2527, the provisions (or items in this document) of a CP are divided into eight primary components, then further divided into sub-components, and finally divided into elements.

There are no items, or provisions, in a CP that can be dismissed as “boilerplate.” Having established this, some items are more useful and informative to the reader in understanding the general framework of the policy under which certificates are to be issued. All of the data collected in the interviews with Industry and DEA, and the guidance given by DEA personnel was evaluated.

This section has two elements. Section 4.1 identifies and evaluates the relevant security provisions as they apply to an electronic prescription system for controlled substances. This section provides analysis and recommendations for all of the provisions that were considered. Based on the analysis performed in Section 4.1, Section 4.2 lists the complete set of Security Policy recommendations.

4.1 Electronic Prescription Certificate Policy Analysis

The following discussion analyzes the selected Certificate Policy provisions. The analysis summarizes the issues that were uncovered during the interviews and documents the content of discussions between PEC and DEA. While there are similarities in the responses from the industry stakeholders (practitioners and pharmacists), differences are apparent between industry and law enforcement. The discussion is intended to solicit feedback as much as it is aimed at helping decision makers converge to a set of policy requirements for the Pilot. The lessons learned from the Pilot will be used to evaluate the suitability of the Policy recommendations to a real-world environment. The Pilot phase will provide the DEA with a chance to observe the impact of policy decisions on system operation.

This subsection takes its form from RFC 2527—Section 3 discusses the RFC in detail, and Appendix E identifies all of the components that make up the RFC—which identifies the relevant provisions contained within a standard Certificate Policy. Provisions and components that must be addressed now—in order to identify the projected user base (end-entities), the enrollment process, or the system architecture—were selected for analysis in this document. The remaining provisions will be considered in the Final Certificate Policy to be delivered in Task 3.

4.1.1 Component #1—Introduction

This component—as defined by the RFC 2527—“identifies and introduces the set of provisions, and indicates the types of entities and applications for which the specification is targeted.” The following subsections address the set of relying parties for which the system will be designed, and the applications that will be approved for its use.

4.1.1.1 Community and Applicability

For liability purposes, a Certificate Policy is only meaningful for a specific user community and for specific applications. The following sections define these.

4.1.1.1.1 Subscribers

This sub-component identifies those individuals (subscribers) who would be authorized to transmit or receive electronic prescriptions for controlled substances.

- **Registered Practitioners**—Practitioners will receive certificates for the purpose of prescribing controlled substances. These certificates will be granted on the basis of a valid DEA registration. A prescription—digitally signed using this digital certificate—will indicate to any relying party, upon successful certificate validation, that the sender is authorized by the DEA to prescribe controlled substances.
- **Agents or Employees of Registrants**—CFR §1301.22 provides guidelines for exemption of registration for agents or employees of DEA registered institutional practitioners (hospitals, and other such institutions). These exempt agents and employees may prescribe, dispense, or administer under the hospital’s or institution’s DEA number—provided that they are permitted to prescribe, dispense, or administer in the jurisdiction of their practice. These exempt practitioners must have an internal authorization code assigned to them by the hospital or institution. This internal code - takes the form of a suffix to the hospital’s DEA number, —the hospital must keep a record of these internal codes. An electronic prescription system cannot impact agents’ ability to continue to operate in this capacity. Adequate safeguards will be required for the enrollment process to ensure that the Certification Authority requires sufficient identification and employment/role information to bind the digital certificate to the agent.
- **Pharmacists**—Under the Controlled Substance Act and the CFR, pharmacists are not required to obtain a DEA registration for the purpose of dispensing controlled substances—pharmacy locations are registered. However, there are record keeping requirements placed on the pharmacy and pharmacist for the various classes of controlled substances. CFR §1304.22 defines the information that must be recorded by the pharmacist.

4.1.1.1.2 Approved Applications

Based on the current environment discussed in Section 3, the following bullets identify the key processes that will benefit from digital signature and for which the DEA's regulations are applicable.

- **Electronic prescribing of controlled substances**—This activity can only be performed by practitioners who are registered with the DEA or those who are exempt from registering with the DEA (such as agents). The types of controlled substances that the practitioner can prescribe are defined by the practitioner's registration and might not include the entire range of schedules of substances.
- **Electronic refill requests for substances in Schedules III-V**—This transaction would be submitted to the practitioner by a pharmacist in response to the patient's request for a prescription. This application is included since it is reasonable to expect that some level of assurance be provided such that the practitioner can trust that the sender is in fact a pharmacist.
- **Electronic prescription record keeping**—The CFR details the requirements for pharmacist record keeping. Pharmacists have record keeping responsibilities that relate to controlled substances prescribed and dispensed. Since the transaction is entirely electronic, a mechanism must be provided to ensure the identity of the person whom either prescribed or filled the medication. Once the prescription has been filled, the pharmacist must either digitally sign the electronic record (the electronic record will now be the only record maintained) or manually sign a printout of the electronic prescription.

4.1.2 Component #2—General Provisions

This component as defined by the RFC 2527 “specifies any applicable presumptions on a range of legal and general practices topics.” The following subsections address the set of relying parties for which the system is designed, and the applications that are approved for its use.

4.1.2.1 Subscriber Obligations

Subscriber obligations comprise the list of actions an end-entity must take in accordance with the security policy to ensure that the level of assurance for which the system is design is maintained. The following paragraphs identify the recommended subscriber obligations for the Pilot.

- **Protections of the entity's private key**— Requirements for safeguarding the private key are discussed in Section 4.1.5.2.
- **Restrictions on private key and certificate use**—Restrictions on the use of the certificate are discussed in Section 4.1.1.1.2.

- **Notification upon private key compromise**—Possession of a practitioner’s private key along with the corresponding pin code would allow a sophisticated hacker to assume the identity of the practitioner for the purpose of generating fraudulent prescriptions. As a rule, end-entities (practitioners and pharmacists) would be required to report the theft or loss of their key within a prescribed time period.
- **Relying party’s digital signature verification responsibilities**—To ensure that the prescription or refill request had not been altered in transit, the relying party’s (practitioner or pharmacist) computer system will be required to check the digital signature to verify that the signed hash is the same as the hash computed independently by the other relying party’s computer system. This check will be inherent in all PKI enabled systems and will be automatic and transparent to the end user.
- **Relying party’s certificate status checking responsibilities for new prescriptions**—For prescription verification purposes it will be required that the pharmacist’s computer system perform a certificate status check to ensure that the certificate used to sign the transaction is indeed a valid one. Status checking must be performed using a recent copy of the Certificate Revocation List (CRL). This obligation will require that the DEA provide CSA registrant information to the CA on a near real-time basis. Once synchronized, the DEA will share information concerning new and revoked registrations. The CA might report to the DEA information concerning agents who have requested digital certificates. This check will be inherent in all PKI enabled systems and will be automatic and transparent to the pharmacist.
- **Relying Party’s ability to cache CRLs**—As mentioned in the previous paragraph, relying parties will check to make sure the subscriber’s certificate is not listed on the CRL before they accept an electronically transmitted prescription for a controlled substance. This action could result in a lookup across a network. Caching the CRL locally speeds the certificate status checking process by allowing relying parties to check a local copy of the CRL. This eliminates the need for the relying party to transmit a certificate status request to the CA, conserves network bandwidth, and improves performance. Based on the large number of prescriptions that are issued, significant network traffic would result if each prescription required a new CRL check. Relying parties will be permitted to cache CRLs for a period equal to the life of the CRL. This check will be inherent in all PKI enabled systems and will be automatic and transparent to the pharmacist.
- **Relying party’s certificate status checking responsibilities for refill prescriptions (Schedules III-V)**—Status checking will not be required on refills since the DEA bases the validity of the refill on the validity of the original prescription (for Schedules III-V only). This solves the problem that occurs if the practitioner’s certificate is revoked after the original prescription is filled, but before any of the refills are presented to the pharmacist.

- **Relying party’s responsibility to verify the prescriber’s ability to prescribe substances within a particular DEA schedule**—Some DEA registrants are not authorized to prescribe all schedules of controlled substances. Relying parties who receive an electronically transmitted prescription will be required to check the accompanying certificate to ensure that the prescriber is authorized by the DEA to prescribe on the appropriate schedule for the drug prescribed. This check will be inherent in all PKI enabled systems and will be automatic and transparent to the end user.

4.1.2.2 Certification Authority Obligations

The following paragraphs identify the recommended Certification Authority obligations for the Pilot.

- **Proper Identity Proofing**— Before granting a digital certificate, the CA must perform identity and credential checking in accordance with the Policy—see Section 4.1.3.1.
- **Revocation of subscriber digital certificates by the Certification Authority**— The CA must perform revocations in a timely manner to ensure that practitioners cannot continue to electronically prescribe controlled substances after their DEA registration is revoked. Since pharmacies are often open 24 hours, the requirement for near-real time revocation seems reasonable. Also, the large number of practitioners will inevitably generate a moderate number of revocations due to forgotten passwords and/or lost tokens. Therefore, upon receipt of a revocation request, the CA will be required to revoke certificates within 4 hours and place the revoked certificate’s serial number on the CRL.

4.1.3 Component #3—Identification and Authentication

Digital certificates have finite lifetimes. Periodic re-keying is necessary so that a new private key can be generated and a new certificate issued to the entity. For each of the three years of the registrant’s DEA registration period, he or she will be required to obtain a new certificate (see *Certificate Validity Period*, section 4.1.6.1.3). The following section details the requirement for initial enrollment in the first year. For years two and three, an end-entity (practitioner or pharmacist) will be required to obtain a new private signing key and therefore a new certificate. This process could happen in the following ways.

4.1.3.1 Obtaining a Digital Certificate

DEA registered Doctors and licensed pharmacists will be required to obtain a digital certificate before they can issue or accept electronic prescriptions for controlled substances. The first step in this process is called certificate application—the applicant submits the proper identity proofing documents that convince the PKI’s Registration Authority (RA) that a digital certificate should be issued. Once the credentials have been verified and the application has been approved, the applicant must generate a key pair and submit the public key to the Certification Authority for digital certificate generation.

The above process can be performed either in person or remotely (using the Internet or the US Postal Service for example). Each alternative has advantages and disadvantages in terms of the strength of identity proofing, cost, and convenience to the applicant.

The following bullets identify three potential methods for performing registration.

- **In-Person application and registration**—This method provides the strongest level of assurance for applicant identity proofing. Identity proofing documentation could include the following: 1) DEA Registration, 2) Photo ID such as a driver's license or hospital ID, and 3) State licensing information. This method is attractive since the RA staff could help the pharmacist or practitioner through the entire process of generating the key pair and receiving a digital certificate. This method also provides a good way of distributing smart cards and readers to these subscribers. One disadvantage of the in-person method is that it would require CAs to establish local registration centers around the country to minimize travel distances for applicants.
- **Remote Application (Credit Card Model)**—This remote application method is convenient for doctors and pharmacists since it does not require them to travel to a registration location. Doctors or pharmacists would submit copies of their credentials to the CA along with a written application for a digital certificate. CA personnel would then verify the credentials of the applicant and determine if a digital certificate should be granted. If approved, the subscriber would receive a token containing the subscriber's key pair and a token reader for their computer.
- **Remote Application (Web Model)**—This alternative provides the greatest convenience but the least amount of assurance. In the absence of in-person application or a hard copy of the applicant's DEA registration, it would be difficult to verify the applicant's identity and credentials with absolute certainty. This alternative is not recommended due to the lack of assurance it provides.

4.1.3.2 Routine Re-key

Based on a digital certificate validity period of one year—see Section 4.1.6.2.3—the requirement for in-person re-application for a digital certificate may not be required in year 2 and year 3 of a registrant's DEA registration period. Routine re-key could be performed electronically to reduce the burden on the certificate holder. Re-key would be performed prior to the expiration of the current certificate.

4.1.3.3 Digital Certificate Revocation Requests

To reduce the threat of unauthorized prescribing using stolen digital certificates, end-entities who lose access to their private keys due to theft or loss must report the event to an authorized Revocation Authority.

4.1.4 Component #4—Operational Requirements

4.1.4.1 Digital Certificate Application

The methods of certificate application are discussed in section 4.1.3.1.

4.1.4.2 Digital Certificate Suspension and Revocation

The digital certificate represents the authority of the subscriber to either issue or dispense controlled substances. While the revocation of the registrant's DEA registration would obviously result in the revocation of his digital certificate, the opposite is NOT true. Digital certificate may be revoked or invalidated by the CA for a number of circumstances unrelated to any punitive action. The two "revocations" are not synonymous. The following bullets identify possible circumstances for revocation of an end-entity's digital certificate:

- **Loss of DEA Registration**—Since a registrant's DEA registration serves as the basis for the digital certificate, loss of DEA registration—either voluntarily or through administrative action—would remove the basis and therefore require that the certificate be revoked.
- **Change of DEA registration information (Registrants only)**—This could occur due to change of location, name change, etc. The old digital certificate would be revoked and a new one issued that would include the updated registrant information.
- **Change of affiliation (Agents only)**—Since agents are permitted to prescribe under the registration of the employer, this authorization should not "follow" the agent who changes jobs. Institutions will be required to notify the CA when such agents terminate their employment.
- **Forgotten digital certificate access control password**—Access to the private key is guarded by a password. Forgetting this password effectively prevents the end-entity from using the key. The only remedy to this situation is to revoke the old digital certificate and issue a new one.
- **Lost or stolen token**—The digital certificate can be stored on a token—such as a smartcard. A lost or stolen private key could be used for unauthorized purposes if the access control password could be obtained.

4.1.5 Component #6—Technical Security Controls

This component identifies the measures used by the CA and the end-entity to protect the private signing key.

4.1.5.1 CA Private Key Protection

Compromise of the CA's root private signing key has a catastrophic effect on the operation of a PKI. Since all certificates are signed with this key, anyone possessing it could theoretically generate fraudulent certificates. Securing the CA's private key is therefore extremely important. In addition to sufficient physical access controls around the CA, the CA's private key must be stored on a US Government Federal Information Processing Standard (FIPS) approved physical device. The FIPS 140-1 Level 2 standard states that the device used to hold the keys must be tamper evident, and must erase the key if tampering is detected.

4.1.5.2 Methods for storing End-Entity Private Keys

The use of hardware tokens as key storage mechanisms effectively increases the level of assurance for end-entities and relying parties. Exhibit 4–1 identifies the advantages and disadvantages of using a token for end-entity private key storage.

Method of storing private key	Advantages	Disadvantages
Disk-based	<ul style="list-style-type: none"> ● No additional cost ● Storage capacity is not an issue ● Access control can be supplemented with a password. 	<ul style="list-style-type: none"> ● Theft or loss (unauthorized file copy) of a the key is not obvious
Token (Smartcard)	<ul style="list-style-type: none"> ● States prefer two-factor authentication, “Passwords are not enough”– Some states have indicated a preference for two factor authentication systems consisting of “something you have” and “something you know.” Tokens fulfill this requirement. ● Tokens provide roaming capability ● Theft or loss of a token is obvious ● Sharing the token requires holder’s conscious decision. ● Smartcard technology is enjoying more widespread use- Smartcards are finding uses in mainstream applications such as credit cards and stored value systems. ● Access control can be supplemented with a password 	<ul style="list-style-type: none"> ● Tokens increase system cost–Requiring a token for key storage would result in a hardware cost of approximately \$150 per workstation for a token reader and \$20 per token. ● Ensuring end-user compliance with key storage requirements–To guarantee that end-entities are storing private key on a token, the CA would either provide the key on a token - or- would supervise the registration process using a token. ● Smartcards can be lost ● Practitioner acceptance- It was not clear from the interviews whether practitioners would be resistant to this technology. ● Smartcards have limited memory–Typical smartcards provide 32K of memory. This limits the number of private decryption keys it can store.

Exhibit 4–1. Advantages and disadvantages of private key storage alternatives

4.1.5.3 Methods for Controlling Access to End-Entity Private Keys

Biometrics provide a reliable means of identifying humans—either by their fingerprint, voice, or their retina. As noted earlier, some states expressed a strong desire to require the use of a biometric for restricting access to the private signing key. This technology can be used to “lock up” a private key so that only the person supplying the correct biometric can access and use it. Exhibit 4–2 identifies the advantages and disadvantages of the methods for controlling access to a user’s private keys.

Access Control Method	Advantages	Disadvantages
<p>Password</p>	<ul style="list-style-type: none"> ● No added cost 	<ul style="list-style-type: none"> ● Are often easily guessed ● Can be shared with others ● Passwords can be forgotten
<p>Biometric</p>	<ul style="list-style-type: none"> ● States prefer two-factor authentication, “Passwords are not enough”– Some states have indicated a preference for strong authentication. A system using both smartcards and biometric access controls provides 3-factor authentication: (1) “something you know”, (2) “something you have” and (3) “something you are.” ● Biometrics cannot be lost or forgotten ● It is impossible for the key holder to share his/her fingerprint ● Costs are going down 	<ul style="list-style-type: none"> ● Biometrics increase system cost–Requiring a biometric for access control would result in a hardware cost of approximately \$150 per workstation for a biometric reader. ● Ensuring end-user compliance–The CA would have no way of knowing if the subscriber is controlling access to his keys with a biometric. ● Practitioner acceptance–It was not clear from the interviews whether practitioners would be resistant to this technology.

Exhibit 4–2. Advantages and disadvantages of biometric access control to private key

4.1.6 Component #7—Certificate and CRL Profiles

This section analyzes the data elements that could be included in a digital certificate for the electronic transmission of controlled substance prescriptions. The section also

identifies and evaluates a number of issues concerning the validity period of certificates and Certificate Revocation Lists (CRLs).

4.1.6.1 Certificate Models

While a number of certificate models could provide sufficient assurance for electronic prescriptions for controlled substances, a standard model will be required to ensure interoperability of practitioner certificates with different pharmacy computer systems.

The models generally fall into two classes: those that employ a single certificate, and those that employ one or more certificates. This is especially important considering that practitioners can hold multiple DEA registrations in different states and that these registrations are not synchronized to expire at the same time. Thus, the issue arises whether these multiple credentials should be included in one certificate or in multiple certificates. The following sections discuss the advantages and disadvantages of these alternative models.

4.1.6.1.1 Single-Certificate Models

Exhibit 4–3 illustrates two methods of using a single certificate for the subscriber. The following bullets summarize the two models.

- **Single identity-Only Certificate**—This model—shown in Exhibit 4–3 as Method A—would simplify the certificate so that it would only represent the subscriber’s identity. No DEA credential information would be included. As shown, relying parties would be required to submit two transactions to verify the prescription or refill request. The first transaction would verify the certificate’s status. The second transaction would perform a credential check against a DEA database. This method has a number of drawbacks. In addition to the increased number of transactions, this alternative does not provide a mechanism for relying parties to cache subscriber credential information. The DEA would be required to make this information available on a real-time basis to all of the practitioners and pharmacies throughout the country. Lastly, the system would be intolerant of any database downtime that could effectively halt the flow of electronic prescriptions unless the database was sufficiently redundant.
- **Single certificate with credentials included as proprietary certificate extensions**—This model—shown in Exhibit 4–3 as Method B—would require the DEA to develop certificate extensions to convey information about each DEA registration or State Pharmacy license that a subscriber might hold. This method would require that the client software be customized to interpret these extensions such that relying party obligations are met. A significant drawback of this model is its susceptibility to certificate thrashing. This term refers to the continued need for a new digital certificate every time the subscriber either loses or gains a credential that is represented within the digital certificate.

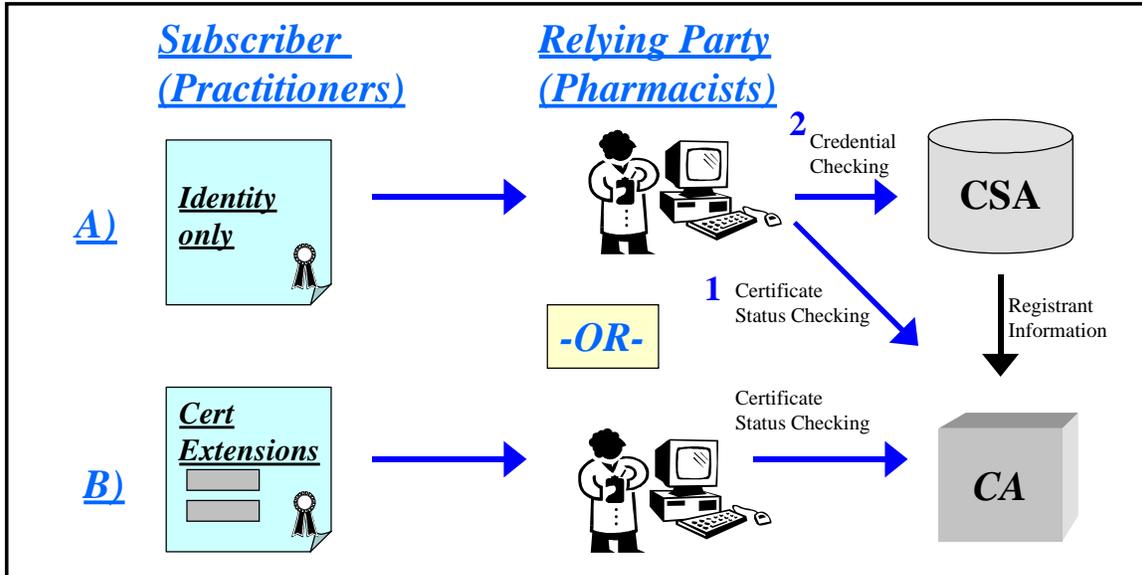


Exhibit 4-3. Single-certificate models

4.1.6.1.2 Multiple-Certificate Models

Exhibit 4-4 illustrates two methods of using multiple certificates for the subscriber. The following bullets summarize the two models.

- **One DEA digital certificate per DEA registration**—This model—shown in Exhibit 4-4 as Method C—avoids the complication associated with attempting to include all of a subscriber’s DEA credentials in a certificate by assigning a registrant one digital certificate for each DEA registration that is held. This model avoids certificate extensions and allows relying parties to perform a single transaction to verify a subscriber’s identity and credentials. Also, to improve performance, relying parties could cache the CRL locally to significantly reduce the number of required CRL requests.
- **Identity certificate with credential-based attribute certificates**—This model is shown in Exhibit 4-4 as Method D. A long-lived identity certificate is used in combination with shorter-lived attribute certificates. CAs operating in accordance with the DEA CP would be responsible for issuing the attribute certificate. This model is attractive because a change in a single credential only affects the digital certificate that is tied to that credential and the problem of certificate thrashing is eliminated. Also, to improve performance, relying parties could cache the CRL locally to significantly reduce the number of CRL requests. At present, attribute certificates are not widely used and software vendors are only in the very early stages of supporting them.

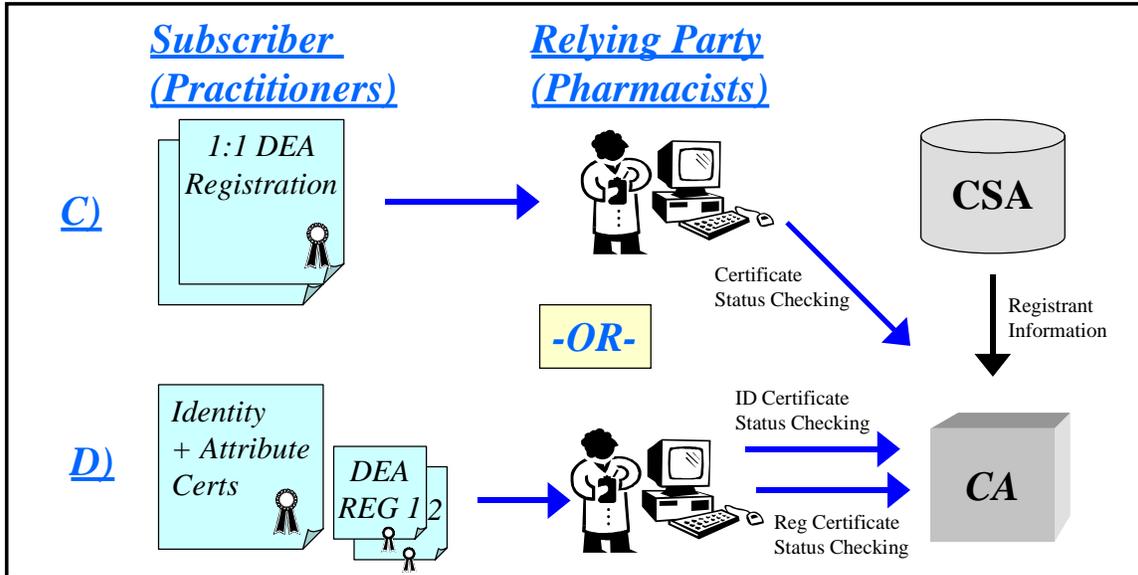


Exhibit 4–4. Multiple-certificate models

4.1.6.1.3 Analysis Summary

Exhibit 4-5 summarizes the results of the above sections. Based on the analysis, the most logical choice for the certificate model would be Model C—one digital certificate per DEA registration. This model leverages mature technology, provides strong assurance, limits the DEA’s involvement—and risk, and avoids issues with certificate thrashing.

	A) Identity Certificate Only	B) Certificate Extensions	C) Direct mapping to DEA Registration	D) Attribute Certificates
Technology maturity	High	Low	High	Low
Identity and DEA credentials validated with single lookup	No	Yes	Yes	No
Requires DEA to maintain an online database of registrants	Yes	No	No	No
Extension translation required	No	Yes	No	No
Susceptibility to certificate thrashing	Low	High	Low	Low

Exhibit 4–5. Summary of certificate model analysis

4.1.6.2 Certificate Profile

The following sections identify a range of data elements that may be contained in the certificate as well as the certificate's validity period. Based on the fact that practitioners may hold multiple DEA registrations in a number of states, and that these registrations are not required to expire in any synchronized manner, it would be difficult to combine a practitioner's multiple DEA numbers onto a single certificate. Revoking a digital certificate for action taken in one state would impact the practitioner's abilities in another state. This would require that a new certificate be issued showing the elimination of privileges in the original state. The following assumes that certificates will be mapped directly to a single DEA registration.

4.1.6.2.1 Electronic Prescription PKI Pilot Certificate Unique Identifier

In an electronic transaction environment, the use of certificates and digital signature will replace the wet signature currently placed on Schedule II prescriptions. It is generally accepted that wet signatures have a strong element of uniqueness. Similarly, a digital certificate must be uniquely distinguishable from all others. This requires that a unique identifier be included on the certificate. This unique identifier can range from a serial number to a unique representation of the person's name and a number to ensure uniqueness.

4.1.6.2.2 Certificate Contents

This section discusses the range of possible data elements that could be included within the digital certificate. A balance is needed to ensure that adequate information about the subscriber is provided in the digital certificate without causing excessive certificate thrashing—thrashing is defined as the excessive re-issuance of new certificates due to updates or changes in one or more of the subscriber’s attributes. Examples of these attributes include email address and physical location. Exhibit 4–6 lists the possible data elements that would be recommended for inclusion in the certificate.

Data Element	Comments	Recommended for inclusion in certificate
Authority to prescribe specific controlled substances (Practitioners only)	In some cases, DEA registration is granted for the purpose of prescribing specific schedules of controlled substances rather than for the entire range of II-V. For instance, a practitioner may be authorized to prescribe III-V but not IIs. The certificate must identify the range of controlled substances the practitioner is authorized to prescribe.	Yes
Registrant Business Address	DEA registration is based on physical location. The CSA §822 (e) states, “A separate registration shall be required at each principal place of business or professional practice where the applicant manufactures, distributes, or dispenses controlled substances.”	Yes
Registrant’s Email address	This would allow the potential use of email to transmit electronic prescriptions in accordance with other federal regulations concerning patient confidentiality. May impact certificate thrashing if it is found that entities regularly change their email addresses.	Optional
Registrant’s DEA number (Practitioners only)	Having the DEA number in the certificate would provide a good cross checking method for verifying the DEA number that must be included in the prescription. This would eliminate the requirement for a separate lookup of the DEA number based on the unique identifier.	Yes
Employer’s DEA Number (Agent practitioners only)	A practitioner who acts as an agent of a registrant is permitted to prescribe under the registration of the employer. Should the employer’s registration be revoked, the agent should no longer be capable of prescribing. Including this number would allow a check to be performed.	Yes

Exhibit 4–6. Candidate data elements for inclusion in certificate

4.1.6.2.3 Certificate Validity Period

CSA §822 indicates that “Every person who dispenses, or who proposes to dispense, any controlled substance, shall obtain from the Attorney General a registration issued in

accordance with the rules and regulations promulgated by him. The Attorney General shall, by regulation, determine the period of such registrations. In no event, however, shall such registrations be issued for less than one year nor for more than three years.” The current DEA registration period for practitioners is 3 years. Exhibit 4–7 summarizes the advantages and disadvantages of each alternative. The question of how long the validity period should be becomes an issue of weighing the risk of making it too long against the cost savings to be realized by making it longer. Since no compelling advantages were identified for a two-year certificate validity period, it was not included in the table.

Maximum Certificate Validity Period	Advantages	Disadvantages
<p>1 year Initial enrollment– In person Re-key- Electronic</p>	<ul style="list-style-type: none"> ● Divisor of the 3 year registration. ● Better security due to shorter validity period. ● Year 2 and year 3 re-enrollment could be performed electronically to reduce burden on practitioner. 	<ul style="list-style-type: none"> ● More frequent certificate enrollment and renewal. ● Certificate enrollment/re-enrollment would not be synchronized with DEA registration. ● Does not provide a mechanism to support existing grace period for late re-registration.
<p>3 years Initial Enrollment– In person Re-key- Not applicable</p>	<ul style="list-style-type: none"> ● Matches the registration period. ● Certificate enrollment/re-key would be synchronized with DEA registration. 	<ul style="list-style-type: none"> ● Weaker security due to longer certificate validity period. ● The Certificate Revocation List will be larger due to the long life of certificates. Negative impact on performance. ● Does not provide a mechanism to support existing grace period for late re-registration.

Exhibit 4–7. Advantages and disadvantages of certificate validity period alternatives

4.1.6.3 Certificate Revocation List (CRL) Profile

This section discusses the CRL validity period.

4.1.6.3.1 CRL Validity Period

The CRL is maintained by the CA and identifies all of the certificates that have been revoked prior to expiration. CRLs are published by the CA and are valid for a time period defined by the Certificate Policy—anywhere from a few hours to a few days. While the majority of certificates will most likely never be revoked during their validity period, a measurable percentage could be revoked for a number of possible reasons including:

DEA credential-basis for revoking a digital certificate

- The registrant surrenders his/her DEA registration voluntarily or it is revoked or restricted as a result of administrative action.
- Failure to renew registration, due to retirement, death, or lack of need.
- DEA registration information changes such as the registrant’s location.

Other possible reasons for revoking the digital certificate

- End-entity forgets password to private signing key.
- End-entity loses smartcard or it is stolen.

The frequency of user revocations as well as the risk of unauthorized use of a certificate both impact the selection of the CRL update frequency. CRLs are typically published more frequently in systems that experience frequent revocations. Exhibit 4–8 lists the advantages and disadvantages of candidate CRL validity periods.

Maximum CRL Validity Period	Advantages	Disadvantages
Short (1-4 hours)	<ul style="list-style-type: none"> ● Best security due to shorter validity period. ● Caching provides performance benefits ● Matches hours of industry operation (24x7) 	<ul style="list-style-type: none"> ● More frequent certificate CRL checks. ● Requires 24x7 CA staffing
Medium (4-12 hours)	<ul style="list-style-type: none"> ● Caching would provide performance benefits 	<ul style="list-style-type: none"> ● Weaker security due to longer CRL validity period.
Long (12-48 hours)	<ul style="list-style-type: none"> ● Better system performance, fewer CRL checks ● Reduced CA administrative staffing requirements 	<ul style="list-style-type: none"> ● Weaker security due to longer CRL validity period.

Exhibit 4–8. Advantages and disadvantages of CRL validity period alternatives

4.2 Summary of Policy Requirements

Based on the analysis provided in Section 4.1, Exhibit 4–9 lists the recommendations for each of the RFC 2527 provisions that were considered.

<i>Provision</i>	<i>Recommendation</i>
Overview	The purpose of the Electronic Prescription PKI is to bring the security services of authenticity, integrity and non-repudiation to electronic prescriptions for controlled substances. The Electronic Prescription PKI will be composed of a root CA and subordinate end-entity CAs. The DEA will operate the root system while subordinate CAs will be operated by outside entities in accordance with the DEA's Certificate Policy. Subordinate Certification Authorities will be governed by the laws of the US and DEA regulations. All CAs will be operated under a policy that emphasizes and strongly warrants reliability of the PKI and its availability to subscribers 24 hours a day 7 days a week.
Community and Applicability	The community of users for the PKI will be limited to DEA registered practitioners, agents of practitioners, and pharmacists who meet all other requirements. Approved applications include: <ul style="list-style-type: none"> ● New electronic prescriptions ● Electronic refill requests ● Electronic prescription record keeping
Obligations	End-Entities are obligated to perform the following: <ul style="list-style-type: none"> ● Protect Keys by storing on a token in accordance with the CP. ● Notify the CA when the token has been lost or stolen. ● Upon receipt of a signed prescription or refill request, relying parties must verify the subscriber's digital signature. ● Upon receipt of an electronic prescription or a refill request, relying parties must check the status of the end-entity's certificate. ● Pharmacy computer systems must verify the practitioner's ability to prescribe the controlled substance identified on the prescription. ● Relying parties are permitted to cache CRLs for up to four hours.
Initial Registration	Initial registration will be performed either in person or by submitting a written request to the CA. Written requests must be accompanied by a copy of the following information <ul style="list-style-type: none"> ● Registered Practitioners: A copy of the DEA registration ● Pharmacists: A copy of their state registration ● Agent Practitioners: A request certified by the DEA registered employer, and a copy of the employer's DEA registration

Exhibit 4–9. Summary of policy requirements

Provision	Recommendation
Routine Re-key	Routine re-key can occur either in-person or electronically if the re-key request is signed by the end-entity.
Revocation request	End-entities who lose access to their private keys because of theft or loss must report the event to an authorized Revocation Authority (RA).
Certificate Application	End-entities must apply for a certificate in-person.
Certificate Suspension and revocation	<p>Certificates will be revoked for the following reasons.</p> <ul style="list-style-type: none"> ● Loss of DEA registration ● Change of DEA registration information (registrants only) ● Change of affiliation (agents only) ● Forgotten password ● Lost or stolen token
Private key protection	<p>Subscriber Key Storage—Private keys will be required to be stored on a FIPS 140-1 Level 1 token. All entities are responsible for the protection of private keys and activation data.</p> <p>Key Access—End-entities will be required to protect access to the private signing key via a password, a biometric, or both.</p> <p>CA Key Storage—The CA’s signing key must be protected within a hardware storage device that complies with FIPS 140-1 level 2.</p>
Certificate Profile	<p>Certificate Contents—Each certificate will contain the following information:</p> <ul style="list-style-type: none"> ● Practitioner’s authority to prescribe specific controlled substances ● Registrant business address ● Registrant’s email address ● Registrant’s DEA number (practitioners only) ● Employer’s DEA number (agent practitioners only) <p>Certificate Lifetime—The certificate validity period will be one year.</p>
CRL profile	CRL Validity Period —The CRL lifetime will be 4 hours. A new CRL will be issued within 4 hours of any certificate revocation.

Exhibit 4–9. Summary of policy requirements (Concluded)

Appendix A –Requirements Interviews List

A.1 DEA Representatives

DEA Representatives	Title	Location	Interview Date
Patricia Good	Chief Liaison and Policy Section	DEA HQ	12/6/99
Michael Mapes	Deputy Chief Liaison and Policy Section	DEA HQ	9/28/99
Jim Pacella	Chief Registration and Program Support Section	DEA HQ	10/12/99
Terry Woodworth	Deputy Director Office of Diversion Control	DEA HQ	12/6/99
Sharon K. Partlo	Chief Policy Unit	DEA HQ	12/6/99
Denise Curry	Chief Liaison Unit	DEA HQ	10/28/99
Janet Gardner	Staff Coordinator	DEA HQ	10/8/99
Vicky Seeger	Pharmacist, Policy Unit		11/19/99
Elizabeth Willis	Deputy Chief, Drug Operations Section	DEA HQ	10/14/99
Tom Crow	Diversion Program Mgr.	Chicago, IL	10/14/99
Jim Tillman	Diversion Program Mgr.	St. Louis, Mo	9/29/99
Scott Collier	Group Supervisor, Denver	DEA HQ	9/28/99
Larry W. Lockhart	Group Supervisor, Birmingham		
Gale Jones	Diversion Investigator		
Donna Dombourian	Diversion Investigator		
Barbara Health	Diversion Investigator		
Alan Clesi	Diversion Investigator		
Craig Riley	Diversion Investigator		

A.2 Department of Veterans Affairs

Department of Veterans Affairs	Location	Contact Person	Interview Date
Dr. Roy Altman	Florida	Dr. Roy Altman	11/10/99
Practitioner	Maryland	Practitioner	11/28/99
Dr. Van Horn	Maryland	Dr. Van Horn	11/26/99
Dr. Shillingford	Maryland	Dr. Shillingford	11/26/99
Dr. Marshall	Maryland	Dr Marshall	11/30/99
Frederick P. Soette	Maryland	Frederick P. Soette	11/29/99
Maarten Calon	Maryland	Maarten Calon	11/29/99

A.3 Pharmacies

Pharmacy Chains	Location	Contact Person	Interview Date
Walgreens	Deerfield,IL	Audrey Neely, Mike Jonas, and Neil Penco	11/4/99
Eckerd	Clearwater, FL	Laurie Toenjes	11/23/99
Rite Aid	Harrisburg, PA	Jim Krahulec	11/11/99
Publix Super Markets	Lakeland, FL	Ron Miller	10/18/99
Giant of Maryland	Landover, MD	Sheldon Pelovitz	11/8/99
Ukrops	Richmond based company with 18 pharmacies	John Beckner Dave Ylitalo	11/17/99
Wegmans Food Markets, Inc.,	Rochester, NY. Wegmans w/ 57 pharmacies	Mark Valesano	11/19 /99

A.4 Practitioners

Practitioners	Location	Contact Person	Date/Time
Dr. Melvin Sterling	CA	Dr. Melvin Sterling	12/20/99
Dr. Nancy Nielsen	NY	Dr. Nancy Nielsen	11/30/99
Dr. John Schneider	ILL	Dr. John Schneider	11/21/99

A.5 Industry Associations

Associations	Location	Contact Person	Date/Time
American Academy of Family Physicians (AAFP)	Washington D.C.	Susan Rehm	11/22 /99
Academy of Managed Care Pharmacy (AMCP)	Alexandria, VA	Richard Fry	11/9/99
American Society of Health System Pharmacists (ASHP)	Bethesda, Md.	Dr. Gary Stein	11/11/99
Food Marketing Institute (FMI)	Washington, DC	Ty Kelley	11/16/99
National Association of Boards of Pharmacy (NABP)	Park Ridge, ILL	Carmen Catizone	11/8 /99
National Association of Chain Drug Stores (NACDS)	Alexandria, VA	Mary Ann Wagner	10/27/99
American Academy of Physician Assistants (AAPA)	Alexandria, VA	Ann Davis	11/18/99
American Pharmaceutical Assoc. (AphA)		Susan Winkler	11/10/99
Pharmaceutical Care Management Assoc. (PCMA)		Lyle Piper	11/23/99
National Community Pharmacists Assoc. (NCPA)	Alexandria, Va	John Rector Doug Hoey	11/8/99
American Academy of Pain Medicine	Glenview, IL	Jeffrey Engle Executive Director	11/15/99
Federation of State Medical Boards	Ft. Worth Texas	Dr. James Winn Executive Vice Pres.	11/29/99

A.6 State Authorities

State Authorities	Location	Contact Person	Interview Date
Missouri Bureau of Narcotics and Dangerous Drugs	Jefferson City, MO	Dan Crider	11/19/99
Maryland State Board of Pharmacy	Baltimore MD	Melvin Rubin	11/15/99
State of California Bureau of Narcotic Enforcement	Sacramento, CA	Chris Bucher	11/17/99
Ohio Board of Pharmacy	OH	Tim Benedict	11/12/99
Massachusetts Board of Pharmacy	Massachusetts	Chuck Young	11/19/99
Nevada State Board of Pharmacy	Reno, NV	Joanee Quirk	11/10/99
New York Department of Health	Troy NY	James Giglio	11/17/99
New York Board of Pharmacy	Albany, NY	Lawrence H. Mokhiber	Fax

A.7 Others

Others	Location	Contact Person	Date/Time
Kaiser Permanente	CA	Steven Gray	11/23/99
St. Elizabeth's Med. Center	Ky	Don Ruwe	11/15/99
Proxymed	FL	Phillip Giordano	11/8/99

Appendix B – Documents Reviewed

B.1 Associations

The National Association of State Controlled Substances Authorities (NASCSA)

American Society for Automation in Pharmacy (ASAP)

National Council for Prescription Drug Programs (NCPDP)

B.2 Documents Reviewed

Author	Title	Date	Source
Adams C. Farrell S.	Internet X.509 Public Key Infrastructure; Certificate Management Protocols	March 1999	http://www.ietf.org/rfc/rfc2510.txt
Arsenault A. Turner S.	Internet X.509 Public Key Infrastructure PKIX; Roadmap	October 22, 1999	http://search.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-04.txt
Chokhani S. Ford W.	Internet X.509 Public Key Infrastructure; Certificate Policy and Certificate Practices Framework	March 1999	http://www.ietf.org/rfc/rfc2527.txt
DEA's Office of Diversion Control	Pharmacist's Manual 8 th Edition	March 12, 1999	Controlled Substances Act of 1970
DEA's Office of Diversion Control	Prescription Accountability Resource Guide	September 1998	Prescription Programs Resource Guide
DEA's Office of Diversion Control	Technological Advances to Enhance Diversion Programs	January 1995	DEA
Department of Veterans Affairs and Cygnacom Solutions	VA PKI: Certificate Policy, Draft	June 14, 1999	Department of Veterans Affairs
Ford W.	Certificate and CRL profile;	October 22, 1999	http://www.ietf.org/inte

Housley R. Polk W. Solo D.	Internet X.509 Public Key Infrastructure		rnet-drafts/draft-ietf-pkix-new-part1-00.txt
Management of Federal Information	Office of Management and Budget	March 5, 1999	Federal Register
Muirhea, Greg	New program reveals whether the patient filled the Rx	June 26, 1995	Drug Topics
Shirey R.	Security Glossary	October 17, 1999	http://search.ietf.org/internet-drafts/draft-shirey-security-glossary-01.txt
Stieghorst, Tom	Prescriptions can be written on-line	July 31, 1995	Sun-Sentinel
Treasury Board of Canada Secretariat	Digital Signature and Confidentiality; Certificate Policies	April 1999	GOC PKI Certificate Policies Version 3.02
Tunitas Group	Healthcare Model Certificate Policy, Tunitas, Draft model policy from 10/15/99	October 15, 1999	http://www.tunitas.com/pages/PKI/pki.htm
Unknown	Electronic Prescriptions	November 19, 1998	NACDS
Unknown	ProxyMed Expands its Electronic Scripts Reach	Unknown	Health Data Network News

B.3 Internet Resources

The Federation of State Medical Boards of the United States, Inc (1999). URL <http://www.fsmb.org/>

American Academy of Family Physicians (1999). URL <http://www.aafp.org/>

Academy Managed Care Pharmacy (1999). URL <http://www.amcp.org/>

American Society of Consultant Pharmacists. URL <http://www.ascp.net/>

American Society of Health-Care Pharmacists. URL <http://www.ashp.org/>

National Community Pharmacists Association. URL <http://www.ncpanet.org/>

B.4 Regulatory Bodies, Laws, Regulations and Proposed Legislation

Drug Enforcement Administration (DEA)

Controlled Substance Act (CSA) of 1970

Code of Federal Regulations (21 CFR, Parts 1300 to end)

Government Paperwork Elimination Act (GPEA)

FDA, HHS 21 CFR Part 11

National Conference of Commissioners on Uniform State Law (NCCUSL)

Health Care Financial Administration (HCFA) Internet Security Policy

Health Insurance Portability and Accountability Act of 1996 (HIPAA): Security and Electronic Signature Standard (45 CFR Part 142), National Standard Health Care Provider Identifier (NPI), National Standard Employer Identifier, Standards for Electronic Transactions and Code Sets, National Standard for Identifiers of Health Plans, National Standard for Health Claim Attachments, Standards for Privacy of Individually Identifiable Health Information

National Archives and Records Administration (NARA)

B.5 Conferences and Seminars

Public Key Infrastructure Analysis, DEVA PKI Pilot Program Plan, August 6, 1999, Author: PEC, DEA Office of Diversion Control.

Appendix C – Relevant Section of the CFR (Part 1300 to the end)

The following tables detail the parts of the Code of Federal Regulations (CFR)—part 1300 to the end—that greatly affect the dispensing process that practitioners and pharmacies must follow.

- **Part 1301 of the CFR**—*Registration of manufactures, distributors, and dispensers of controlled substances*—defines the registration process for those who wish to become involved in the dispensing business activity.
- **Part 1304 of the CFR**—*Records and reports of registrants*—outlines the requirements for the storage and maintenance of controlled prescriptions by pharmacies.
- **Part 1306 of the CFR**—*Prescriptions*—defines the requirements for prescribing and the responsibilities of the practitioners and pharmacies involved. The following charts summarize these sections.

Part	Description Summary	Practitioner Impact	Pharmacy Impact
1301.11	Persons required to register	Practitioners are required to register.	Pharmacies are required to register.
1301.12	Separate registration for separate locations	Practitioners who only prescribe need to be registered only at one location per state. Additional registrations are required when controlled substances are stored, administered, and/or dispensed at the location.	A separate registration is required for each physical location.
1301.13	Registration application for independent activities (dispensing)	Practitioners fall into the dispensing business activity.	Pharmacies fall into the dispensing business activity.
1301.22	Persons exempt from registration	A practitioner may prescribe using the DEA number of the institutional practitioner (hospital) with a unique suffix.	Pharmacists are exempt from registration for the dispensing of controlled substances—provided the pharmacy location is registered to dispense controlled substances.

Exhibit C–1. §1301 Registration Process

Part	Description Summary	Practitioner Impact	Pharmacy Impact
1304.03	Persons required to keep records	<ul style="list-style-type: none"> ▪ <i>Prescribing Records:</i> Not required to keep records for prescribing unless prescribed for maintenance or detoxification. ▪ <i>Dispensing Records:</i> Required to maintain records of controlled substances dispensed, ▪ <i>Administering Records:</i> Required to maintain records of controlled substances administered in the course of maintenance or detoxification treatment 	Required to keep records of controlled drugs dispensed.
1304.04	Maintenance of records	<ul style="list-style-type: none"> ▪ If required to keep records, the practitioner must keep associated records for a period of at least two years from the date of such records ▪ Schedule II records must be kept separate from all other, III-V. All records must be kept in a readily retrievable manner. ▪ Records may be kept on an in-house computer system 	<ul style="list-style-type: none"> ▪ The pharmacy must keep prescriptions for a period of at least two years from the date of dispensing ▪ Schedule II prescriptions must be kept separate from all other prescription in a separate prescription file, Schedule III-V records may be kept separate or if kept with other records, must be in a readily retrievable manner
1304.22	Records for dispensers and others	Not applicable	<ul style="list-style-type: none"> ▪ Number of units or volume of substance dispensed ▪ Name of Person to whom it was dispensed ▪ Dispensing Date ▪ Written or typewritten initials for the individual who dispensed or administer the substance.

Exhibit C-2. §1304 Records and Reports of Registrants

Part	Description Summary	Practitioner Impact	Pharmacy Impact
1306.03	Persons entitled to issue prescriptions	Must be authorized in their practicing jurisdiction and be registered or exempted from DEA registration.	Pharmacists in some states have the prescribing authority of a mid-level practitioner.
1306.04	Purpose of issue of prescription	Must issue a prescription for a valid medical purpose.	Carry a corresponding responsibility as the practitioner.
1306.05	Manner of issuance of prescriptions	Practitioners must adhere to the information required on a prescription.	Pharmacists must verify and validate required prescription information.
1306.06	Persons entitled to fill prescriptions	None	Pharmacist acting in usual course of professional practice and must be employed by a registered pharmacy or a registered institution such as a hospital/hospital pharmacy.
1306.11	Requirements of prescription (Schedule II)	Schedule II must be manually signed	Prior to dispensing (Schedule II) pharmacists must have the original written prescription, except in an emergency situation when signed original may be obtained later.
1306.12	Refilling Prescriptions (Schedule II)	Refills on Schedule II substances are prohibited.	Refills on Schedule II substances are prohibited.
1306.13	Partial Filling of Schedule II	Practitioners are not directly affected by this.	Partial fillings are permitted, remaining qty must be dispensed within 72 hours, qty supplied must be noted on the face of the written prescription, partial fillings are also permitted in quantities to include individual dosage units for LTFC or terminally ill patients
1306.21	Requirements of prescription (Schedules III-V)	Schedules III-V can be written, faxed, or phoned in.	A pharmacist may dispense a Schedule III-V controlled substance after receiving the original prescription, receiving a fax of the prescription, or receiving a phone call from the practitioner and immediately reducing it to writing. All three forms serve as the original prescription.

Exhibit C-3. §1306 Prescriptions

Part	Description Summary	Practitioner Impact	Pharmacy Impact
1306.22	Refilling Prescriptions (Schedule III-V)	Limited to 5 refills within a six month period.	Limited to 5 refills within a six month period and the pharmacist must document each refill on the reverse side of the prescription, refill information may also be retained in an electronic database.
1306.23	Partial Filling of Schedules III-V	Practitioners are not directly affected by this.	Partial fillings are permitted, they must be recorded in the same manner as a refill for III-V

Exhibit C-3. §1306 Prescriptions (concluded)

Appendix D – Regulatory/Legal Environment

The following sections summarize the enacted Federal legislation that supports the use of PKI for digital signature or gives legal guidance for the use of digital signatures. Additional sections discuss legal and regulatory considerations for the DEVA project.

D.1 Government Paperwork Elimination Act (GPEA)

The 105th Congress, 2d Session, signed the GPEA into law on October 8, 1998. The Act mandates the electronic availability of Government agency forms, questionnaires and surveys. In the case that a signature is required, a digital signature shall be recognized as having the same legitimacy as a “wet” (ink) signature.

The Act establishes the legal foundation for the acceptance and use of electronic signatures. It defines electronic signature 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.”⁴

The Office of Management and Budget (OMB) has been charged with the responsibility to establishing procedures and guidelines for the implementation of the GPEA and 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. 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.

D.2 FDA, HHS 21 CFR Part 11

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

The health care industry has traditionally used what the FDA classifies as a closed system. In a closed system, access is controlled by persons who are responsible for the content of electronic records stored in the system. The health care industry typically

⁴ GPEA §6

implements a closed system using expensive dedicated/leased computer connections. There has been an increased need in the health care industry to use inexpensive computer inter-connections that can be provided by the Internet. The FDA would classify such a computing environment as an open system. In an open system, system access is not controlled by persons who are responsible for the content of electronic records stored in the system.

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

D.3 National Conference of Commissioners on Uniform State Law (NCCUSL)

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

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

D.4 Health Care Financial Administration (HCFA) Internet Security Policy

In response to the security threats on the Internet, HCFA published an Internet security policy on November 24, 1998. The policy affects the transmission of all HCFA Privacy Act-protected and other sensitive HCFA information by its components and Medicare/Medicaid partners, as well as other entities authorized to use this data. The Internet may be used as long as the following cryptographic services are met.

- **Data Confidentiality**—ensures that only authorized parties can read a communication.
- **Data Integrity**—ensure that the content of a communication has not been altered in transit.
- **Authentication/Identification**—Authentication refers to generally automated and formalized methods of establishing the authorized nature of a communications partner over the Internet communications data channel itself (in-band process). Identification refers to less formal methods of establishing the authorized nature of a communication partner, which are usually manual,

involve human interaction, and do not use the Internet data channel itself (out-of-band).

- **Authorization**—Sender and recipient of the data are privileged to receive and decrypt such information.

Additional safeguards such as firewalls or some other mechanism must be used to protect systems from the Internet. Policies regarding the use of firewalls are not covered by the HCFA Internet security policy document. The policy does not supersede the forthcoming HCFA regulation protecting electronic health information mandated by HIPAA. The HCFA Internet security policy is consistent with the proposed regulations.

- The HCFA policy explicitly identifies the minimum encryption standards and approaches.
- Organizations deciding to use the Internet for transmittal of sensitive HCFA information must be able to show adherence to the requirements of this policy. HCFA may audit such organizations for adherence to the requirements of this policy.
- Organizations desiring to use the Internet must communicate their intent to HCFA.

D.5 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA is a federal law that increases patient rights and simplifies requirements. HIPAA set a deadline of August 21, 1999 for Congress to pass legislation protecting patient rights. The following items summarize the purpose of HIPAA.

- Recognize established industry standards for electronic health information transactions.
- Mandate a timetable for providers and health plans to become compliant with recognized standards.
- Recommend privacy standards for health information.
- The bill supersedes state laws, except where HHS determines that the State law is necessary. HHS will make exception when necessary to prevent fraud and abuse, to ensure appropriate state regulation of insurance or health plans, addresses controlled substances, or for other purposes.
- The bill defines penalties for violations of the law.

In the absence of legislation, HIPAA calls for Health and Human Services (HHS) to issue regulations for patient rights and administrative simplification. Since Congress did not meet the August 21, 1999 deadline, HCFA—under HHS—has issued or is planning to issue the following seven *Notice of Proposed Rule Making* (NPRM) which are summarized in sections 3.4.5.1 to 3.4.5.7.

D.5.1 Security and Electronic Signature Standard (45 CFR Part 142)

The HCFA NPRM is applicable to transactions defined in HIPAA. HCFA's current proposed standard for security and electronic signature standards strongly identifies PKI

as the most viable technology that will ensure the proper level of protection for health care information.

"Currently there are no technically mature techniques that provide the security service of non-repudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques. Therefore, if electronic signatures are employed, we would require that digital signature technology be used."⁵

The HCFA NPRM is not mandating any one type of technology over another nor are they requiring the use of digital signature. However, they recognize the necessity for electronic signatures for a completely paperless environment. HCFA does not define the services of digital signature to include a PKI. It does state that a PKI is a required infrastructure for digital signature.

The strength of electronically binding a certificate to an identity is also founded on the soundness of the mathematical framework of the enabling technology. It is dependent on the policies and procedures that are adopted in the operation and maintenance of the enabling technology. HCFA has outlined requirements that address such issues.

The need to utilize technical standards that are maintained by a recognized standards body for the enabling security technology is an integral aspect of any security system. Employing standards assures that the enabling technology survives and evolves with changes in technology. The HCFA's proposed security standard impacts the DEVA project and directs the project's technical requirements.

D.5.2 National Standard Health Care Provider Identifier (NPI)

The NPI is being created by HCFA to implement some of the requirements of the Administrative Simplification subtitle of HIPAA. HCFA would issue NPI numbers using the National Provider System (NPS). HCFA issued a notice of the new system in the federal register on 7/28/98. HCFA will use Medicare and other Federal health plan information to automatically issue NPI numbers to providers. This covers approximately 85% of health care providers. The remaining health providers will fill out a form. The NPI number is an 8 digit alphanumeric number—the 8th digit is a checksum. The NPI number will not contain any embedded intelligence about the health care provider. The following is a list of who would get an NPI number.

- Physicians and other practitioners
- Physician/practitioner groups
- Institutions (i.e. Hospitals, laboratories, and nursing homes)
- Organizations (i.e. health maintenance organizations, pharmacies, medical supply companies)

² Vol. 63, No. 155, Federal Register pg. 43257 (Aug 12, 1998)

It is possible that the NPI number may be used to uniquely identify users across time in the DEVA PKI.

D.5.3 National Standard Employer Identifier

The employer identifier is part of health insurance reform. HCFA published the NPRM on June 16, 1998. The employer identifier does not have an impact on the DEVA PKI at this time.

D.5.4 Standards for Electronic Transactions and Code Sets

This standard was developed for administrative simplification. The standard was published on May 7, 1998 and the comment period ended July 6, 1998. HCFA's standard for electronic transactions and code sets shows a trend to define particular industry standards in federal regulation. The HCFA security standard would be applicable to transactions and code sets.

D.5.5 National Standard for Identifiers of Health Plans

HCFA will issue identifiers for health plans. It is part of the HIPAA administration simplification provision. HCFA has published this standard. The identifier could impact industry standards for communicating prescription data from the pharmacy to PBM/switches for the purpose of drug interaction and formulary reviews that are performed by the pharmacist.

D.5.6 National Standard for Health Claim Attachments

This standard has not yet been published by HCFA. The impact of this standard on the DEVA project would have to be evaluated when the standard becomes available.

D.5.7 Standards for Privacy of Individually Identifiable Health Information

HCFA published this standard on November 3, 1999 and the comment period ends January 3, 2000. This standard has a direct impact on DEVA since a patient's C2 prescription contains individually identifiable health information.

D.6 National Archives and Records Administration (NARA)

It is critical to the mission of DEA and state agencies that electronic prescription and filling records be admissible in court. The NARA published procedures to enhance the legal admissibility of electronic records in the federal registry on 7/1/98 (CFR title 36 Subchapter B PART 1234 Electronic Records Management §1234.26, Judicial use of electronic records. Amended 7/1/98). The following four actions must be taken to ensure the admissibility of electronic records.

- Standard creation and retrieval process.
- Prevent unauthorized addition, modification and deletion.
- Identify the electronic storage medium throughout the life of the record and the time spent on the storage medium.

- Coordinate Information Resource Management (IRM) with legal counsel, senior IRM, and management staff.

The following bullets summarize the required security controls for electronic records (§1234.28).

- Authorized access
- Backup and recovery
- Personnel trained in safeguarding sensitive or classified electronic records.
- Minimize the possibility of unauthorized deletion or alteration of records.
- Include electronic records security in computer security plan.

D.7 Organizations

D.7.1 Alliance of States with Prescription Monitoring Programs

Alliance of States with Prescription Monitoring Programs is an association that represents and promotes the interests of state controlled substance authorities. Alliance of States with Prescription Monitoring Programs created a model prescription accountability act that could be used for establishing a prescription monitoring program and holds annual conferences for the promotion and discussion of issues surrounding state monitoring programs. PEC had the opportunity to present the DEVA project and meet with states that currently have or are planning reporting systems at the November 1999 conference. PEC gathered concerns state controlled substance authorities have about an electronic prescription system for controlled substances. The results of those talks are reflected in later sections.

D.7.2 American Society for Automation in Pharmacy (ASAP)

ASAP is dedicated to assisting its members with new information technologies that enhance a pharmacist's mission as a caregiver and in the operation and management of a pharmacy. ASAP published Voluntary Industry Guidelines for Prescription Reporting Version 2 Release 1, in September 1999. The ASAP guidelines provide support for the following business functions.

- Reporting of Controlled Substances in states where this is required.
- Reporting information to participate in a patient refill-reminder program.
- Providing data for market research.
- Participating in university research projects on patient compliance, directions of use for specific drugs, and the like.

Appendix E – RFC 2527 Certificate Policy Components

<i>RFC 2527 Component</i>	<i>Provision</i>
<i>Introduction</i>	
	Overview
	Identification
	Community and Applicability
	Contact Details
<i>General Provisions</i>	
	Obligations
	Liability
	Financial Responsibility
	Interpretation and enforcement
	Fees
	Publication and repositories
	Compliance Audit
	Confidentiality
	Intellectual Property rights
<i>Identification & Authentication</i>	
	Initial Registration
	Routine Re-key
	Rekey after revocation
	Revocation request
<i>Operational Requirements</i>	
	Certificate Application
	Certificate Issuance
	Certificate Acceptance
	Certificate Suspension and revocation
	Security Audit procedures
	Records archival
	Key Changeover
	Compromise and disaster recovery
	CA termination

<i>RFC 2527 Component</i>	<i>Provision</i>
<i>Physical, procedural and personnel security controls</i>	
	Physical controls
	Procedural controls
	Personnel security controls
<i>Technical security controls</i>	
	Key pair generation
	Private key protection
	Other aspects of key management
	Activation data
	Computer security controls
	Life-cycle security controls
	Network security controls
	Cryptographic module engineering controls
	<i>Certificate and CRL Profiles</i>
Certificate Profile	
CRL profile	
<i>Specification Administration</i>	
	Specification Change Procedures
	Publication and Notification Procedures
	CPS Approval Procedures

Appendix F – Listing of Acronyms

ACF	Access Control Facility
ASAP	American Society for Automation in Pharmacy
ATM	Asynchronous Transfer Mode
CA	Certification Authority
CFR	Code of Federal Regulations
CN	Common Name
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSA	Controlled Substances Act
DEA	Drug Enforcement Administration
DEVA	DEA-Department of Veterans Affairs
DN	Distinguished Name
DUR	Drug Utilization Review
EDI	Electronic Data Interchange
EDT	Electronic Data Transmission
EMR	Electronic Medical Records
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
GOC	Government Of Canada

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

NPRM	Notice of Proposed Rule Making
NPS	National Provider Service
NTP	Narcotic Treatment Programs
OD	Office of Diversion Control
OMA	Operations Management Authority
OMB	Office of Management and Budget
PBM	Pharmacy Benefit Management
PEC	Performance Engineering Corporation
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMA	Policy Management Authority
POC	Proof Of Concept
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, & Adleman
Rx	Prescription
TCP/IP	Transmission Control Protocol / Internet Protocol
UCF	Universal Claims Form
UCITA	Uniform Computer Information Transaction Act
UETA	Uniform Electronic Transaction Act
UID	Unique Identifier
VA	Veterans Affairs
VPN	Virtual Private Network
X.500	The standard for directory services

X.509	The standard for PKI certificates
XML	Extensible Markup Language