Public Key Infrastructure Analysis

Controlled Substances Ordering System (CSOS)/(MADI) PKI Certificate Policy Requirements Analysis

Prepared for

Drug Enforcement Administration
Office of Diversion Control
Suite 3-100
600 Army Navy Drive
Arlington, Virginia 22202

in response to

Assist 5C-A-JMD-0072-DO-220

February 3, 2000

Prepared by PEC Solutions, Inc.

TABLE OF CONTENTS

EXHIBITS AND TABLES

1. Introduction

1.1 Overview and Background

Under the authority of the Controlled Substances Act of 1970, the Drug Enforcement Administration, Office of Diversion Control (OD) regulates the manufacture and distribution of Controlled Substances in the United States. This regulatory control is designed to prevent the diversion of legitimate pharmaceutical drugs into illegal channels and also to ensure that there is a sufficient supply for legitimate medical uses. Title 21, Code of Federal Regulations, Sections 1300-1399 sets forth in details the authority and responsibilities of DEA in this area. It is further intended that their systems prevent the introduction of contraband Controlled Substances into the legal distribution channels.

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 Manufacturers and Distributors (MADI) Public Key Infrastructure (PKI) will be designed to bring to this regulatory process the advantages of PKI. MADI will (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

The Federal Code of Regulations Title 21, Sections 1300-1399, defines the registration, record keeping, inventory, ordering processing, prescribing, and miscellaneous activities as they relate to Controlled Substances. Persons who wish to participate in a Controlled Substances business activity, i.e. manufacturing, distributing, dispensing, research, narcotic treatment programs, import, export, are required to register with the Office of Diversion Control unless otherwise exempted from registration described in §1301.22. Registrants fall into two categories, A-Type registrants and B-Type registrants as shown below.

The MADI Project focuses on both Type B registrants, Manufacturers and Distributors, and Type A registrants, Retail Pharmacies, Hospitals & HMOs. The MADI Project will review the relationships and processes as they pertain to the DEA regulatory process and these two categories of registrants. The MADI Project will determine how the regulatory process can be enhanced through the use of a PKI.

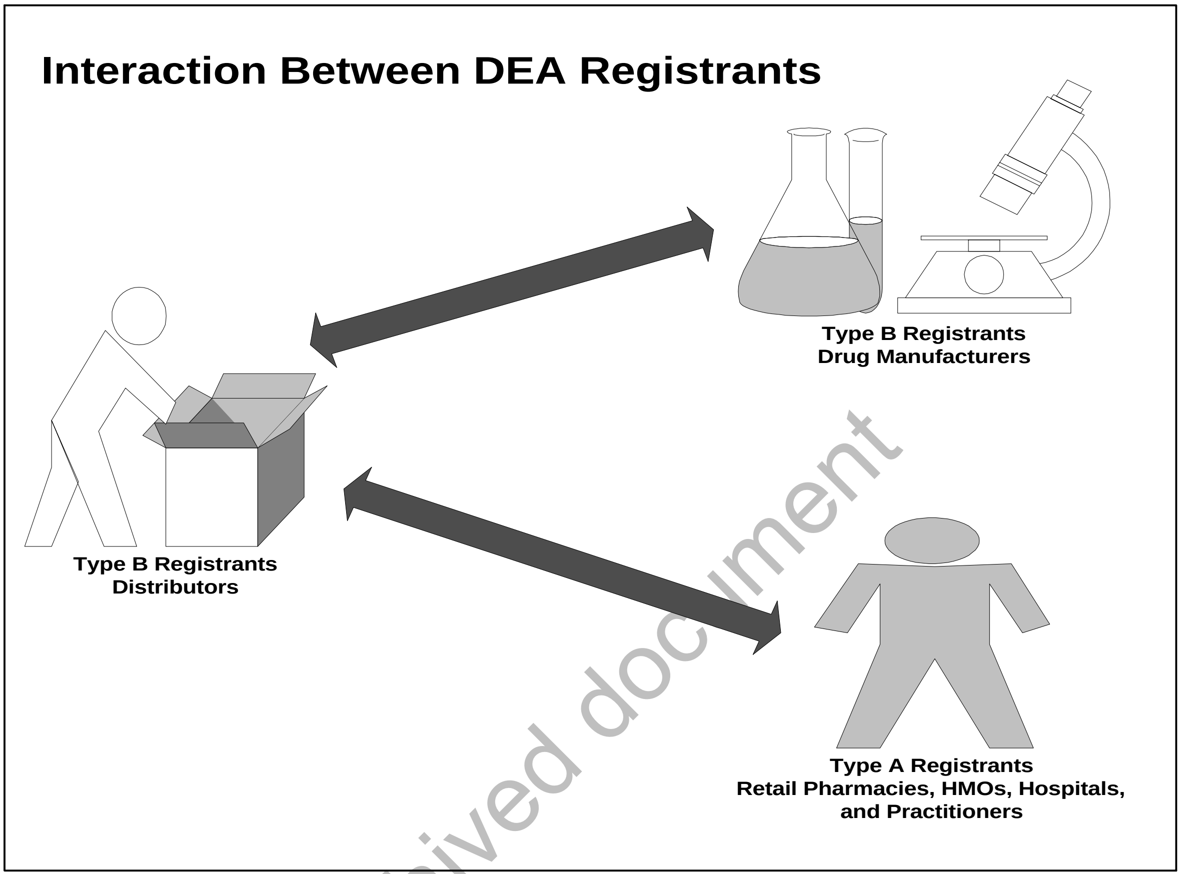


EXHIBIT 1-1. INTERACTION BETWEEN DEA REGISTRANTS

1.3 Document Organization

The document is organized into the following sections:

Section 1– The introduction provides a description for this task and provides 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 and summary data and findings produced by the interviews, meetings, seminars, document reviews and site visits.

Section 4– Section 4 provides Analysis of the data and findings to derive the requirements for the MADI PKI.

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

Appendix B Listing of Documents Reviewed

Appendix C Listing of Acronyms

1.4 Description of Task 2.2.1

Certificate Policy Requirements Analysis Task 2.2.1

The objective of this task is to define the quality of the security services required by the MADI PKI. This analysis will result in a clear general understanding of Certificate Policy (CP) requirements, but will not contain the level of detail found in a CP. During Task 3 a CP and a Certificate Practice Statement (CPS) will be developed drawing from the results of the analysis.

During this task PEC and DEA will define the level of security that the MADI Proof of Concept (POC) PKI must incorporate in order to support the requirements of DEA and 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 and DEA.

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 is based on an understanding of relevant Federal and State laws, DEA Regulations, and accepted customs and practices of the Industry.

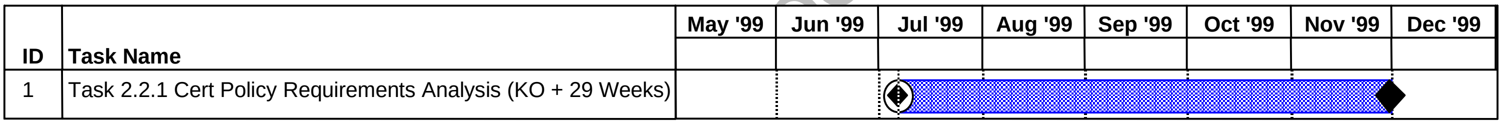
The analysis will provide recommendations in the context of the MADI PKI, regarding the assurances, and guarantees that the Certification Authority must make to the users and relying parties who accept and use the Certification Authority’s certificates and the responsibilities and obligations of users and relying parties of the Certification Authority’s certificates. This will include liability issues, issues of financial responsibility, interpretation and enforcement of the policy or Certification Practice Statement and possible fees associated with the PKI.

PEC will determine the requirements of the MADI Certification Authority pertaining to operational procedures. Some of these requirements may apply to the Registration Authority’s and directories/repositories. The analysis will also focus on the physical, procedural, and personnel security controls that the MADI Certification Authority will implement. In the final Certificate Policy and Certification Practice Statement the MADI Certification Authority 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.

Another type of security control requirements will also be analyzed, technical security controls. In this part of the analysis the technical controls needed by the MADI Certification Authority 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. This part of the analysis will determine the best and most feasible profile for user certificates and CRLs.

During this phase of the analysis PEC will make a determination as to which of the trust models is most appropriate for the MADI PKI. The four models are usually described as hierarchy; network/mesh; trust list; key ring. These models each have advantages and disadvantages. A choice of trust model has implications for decisions on product selection, cost, architecture, policies and procedures, and risk management.



ID	Task Name	May '99	Jun '99	Jul '99	Aug '99	Sep '99	Oct '99	Nov '99	Dec '99
1	Task 2.2.1 Cert Policy Requirements Analysis (KO + 29 Weeks)			▨	▨	▨	▨	▨	

1.5 Analysis Methodology

Analysis Methodology

The methodology used for this analysis:

(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, 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

In the current DEA 222 Form process, Stakeholders that are directly involved in the process are organized and defined here into high level categories.

Each of these categories of Stakeholders are distinct in terms of their:

- ❑ Position in the process flow
- ❑ Impact of the process on their operations
- ❑ Motivation/Desire to Change
- ❑ Technology Infrastructure
- ❑ Acceptance of Technology
- ❑ Sensitivity to IT Cost

Manufacturers

Representative drug manufacturers were chosen from those who manufacture Schedule 2 Controlled Substances and process varying volumes of DEA 222 Forms: Three large volume manufacturers, one medium and two small volume manufacturers for a total of six interviews. Manufacturers process and fill DEA 222 Forms sent from their customers. Some manufacturers also transfer drugs or product internally using the DEA 222 Form.

Distributor

Representative drug distributors were chosen from those who distribute Schedule 2 Controlled Substances and process varying volumes of DEA 222 Forms: Four large volume distributors, two medium and one small volume distributors for a total of seven interviews. Distributors send DEA 222 Forms to their supplier. Distributors also receive DEA 222 Forms from their customers.

Chain Drug Stores/Grocery Chain Stores with In-house Pharmacies

Representative drug store chains and grocery stores that operate in-store pharmacies were chosen from those who either use an independent distributor to provide Schedule 2 Controlled Substances to the stores or those that centrally warehouse and distribute Schedule 2 Controlled Substances to their stores. Four large volume chain drug stores-two that centrally warehouse and distribute and two that do not, one medium chain grocery store with in-store pharmacies and one small chain grocery store with in-store pharmacies were interviewed.

Those that centrally warehouse and distribute Schedule 2 Controlled Substances have a similar volume and processing as a distributor. Those that utilize the services of an independent distributor have the same volume and process as an independent pharmacy.

Pharmacies

Representative pharmacy associations were chosen from those who represent the interests of both independent pharmacists and state boards of pharmacies. Three associations were interviewed. Pharmacies process DEA 222 Forms, which are then sent to a distributor to be filled.

HMOs and Others

Other representative groups who utilize the DEA 222 Form were chosen from healthcare maintenance organizations (HMOs) and drug treatment clinics. Two HMOs and one methadone treatment clinic were interviewed. These groups process DEA 222 Forms, which are then sent to a distributor or directly to a manufacturer to be filled.

DEA/Pharmacy Boards/State Regulators

DEA Headquarters and Field Office personnel were designated by the Office of Diversion Control to participate in the interview process. DEA provided information on the regulatory issues of State Boards of Pharmacies and State regulators.

2. Definitions, Standards, and Initial Design Guidance

2.1 Certificate Policy (CP)

The X.509 Standard defines a Certificate Policy 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 Certificate Policy. 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”. Request For Comment 2527 also defines the Certification Practice Statement. The Certification Practice Statement is a more detailed description of the practices followed by the Certification Authority to implement the Certificate Policy. The Certificate Policy is a document intended for the public, the users and the relying parties; it is normally published in the same Repository that the Certification Authority’s certificates are published. The Certification Practice Statement is not always a public document, as it may contain details of operation useful to an adversary.

It is explained in the Request For Comment 2527 that when a Certification Authority issues a Public Key Certificate (PKC) to an entity, the Certification Authority 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 the subject of the certificate. The Certification Authority 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. Typically the user wants to verify a digital signature of a certificate subject or to encrypt information for the certificate subject.

It is re-stated for emphasis here that the fundamental assumption of PKI is: The subject of a Public Key Certificate does hold the corresponding private key. The Certification Authority establishes this through some Proof of Possession (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 key 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.

2.2 Level of Assurance/Security

There is no universally agreed upon standard for the syntax or semantics to be used in describing Levels of Assurance/Security. There is a Government of Canada (GOC) standard and an evolving US 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. The items should each 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) - (12) of these significant issues is a shorthand method under consideration by the Federal PKI (FPKI) Steering Committee for evaluating the overall level of assurance that a Certificate Policy is written to. For the purposes of this analysis we have adopted a close approximation of the Federal PKI semantic framework.

FEDERAL PKI SEMANTIC FRAMEWORK APPROXIMATION

		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

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 a 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 personal appearance with two IDs including at least one a picture ID issued by a government entity
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 2048 bit RSA 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 confidentiality private key is compromised; it could cause loss of life, imprisonment, or major financial loss if the end entity private signature key is compromised

Table 2-1. Federal PKI Semantic Framework Approximation

2.3 Initial Design Guidance

Prior to the initiation of the interview phase of the project, MADI project personnel received input from both DEA and Industry. Much of the early input was subsequently echoed in the interviews. The early input was very consistent among both DEA and Industry personnel. This provided PEC with sufficient guidance to allow more focus on other areas of discussion during the interviews. An example of the type of guidance is the need for high availability of the PKI infrastructure.

The input from DEA came primarily in a series of formal meetings. In these meetings DEA personnel (1) attempted to educate the MADI team in the responsibilities and processes of the Office of Diversion Control (2) provided some high level design constraints (3) shared some initial concepts of what the MADI PKI might look like.

The input from Industry came primarily in conversations between MADI project personnel and Industry representatives at Industry conventions and from a few telephone conferences with Industry representatives who wished to support the project with an early input.

The table below contains a selection of significant and useful inputs.

DEA/INDUSTRY PRE-INTERVIEW INPUT ON MADI PROJECT

	Requirement	Stakeholder Groups	Requirement Type
1	Not all DEA Registrants will be enrolled in the PKI.	DEA	Certificate Policy
2	The MADI PKI will be an option to the continuing current paper process for the foreseeable future. A DEA Registrant must choose MADI or the paper process but not both.	DEA	Certificate Policy
3	DEA will not act as the Certification Authority but will establish the Certification Authority and define policy and standards	DEA	Certificate Policy
4	Updated tape of DEA Registrants would be sent to daily to Certification Authority to update CRLs and authenticate end entity applications.	DEA	Certificate Policy
5	Existing Industry ordering processes should be leveraged to extent possible, better to PKI enable existing process than to make a new one	DEA	Certificate Policy
6	The DEA Registration number is a unique number and can be used in a certificate.	DEA	Certificate Policy
7	Certification Authority registration process should leverage the current DEA Registration process to the extent possible	DEA	Certificate Policy
8	The level of security and assurance of MADI will be at least that of the current DEA 222 Form process	DEA	Certificate Policy
9	The best and final measure of the MADI PKI policy will be Industry acceptance	DEA	Certificate Policy

10	Process to obtain PKI certificates should be no more burdensome than activating an ATM card.	DEA	Certificate Policy
11	Certificates should be tied to locations just as DEA Registrations are now tied to locations.	DEA	Certificate Policy
12	Certificate will give same authority as current 223 Registration Certificate. It will give authority to manufacture and distribute Controlled Substances	DEA	Certificate Policy
13	An assignment of a private key could substitute for the Power of Attorney (authorization to sign DEA 222 Form).	Industry	Certificate Policy
14	Certification Authority should be a third party, i.e., not a manufacturer nor a distributor, not DEA	Industry	Certificate Policy
15	Certification Authority must process requests for certificates or revocations within a timely manner, e.g., forty-eight hours.	Industry	Certificate Policy
16	The process of enrolling in the PKI and validating certificates must not be a bottleneck on the flow of business. PKI infrastructure must be available with a high degree of assurance 24x7.	Industry	Certificate Policy
17	Registrants should not be held responsible for errors resulting from relying on certificates improperly issued by the Certification Authority or from out of date CRL information	Industry	Certificate Policy
18	Public key should be valid as long as a DEA registration is valid. If public keys require re-certification, a grace period for re-registration should be extended.	Industry	Certificate Policy
19	The certificate issuance/revocation process should be well defined.	Industry	Certificate Policy
20	The Directory for public keys should show the Registrant's current DEA registration status.	Industry	Certificate Policy
21	Only those with a certificate (i.e. PKI enrollees) should have access to the Directory.	Industry	Certificate Policy
22	Directory information should be human readable in English.	Industry	Certificate Policy
23	Consideration should be given to having no expiration of private keys.	Industry	Certificate Policy

24	Modifications to DEA Registrations that do not require a new DEA registration number should not require new certificates/keys.	Industry	Certificate Policy
25	The cost of enrolling in the PKI is a factor for some potential enrollees. This should be considered before mandating things such as biometrics or key protection hardware	Industry	Certificate Policy
26	Consider allowing each Registrant to act as a Certification Authority and issue certificates to authorized persons in their own organization	Industry	Certificate Policy
27	The speed, and reduced paper characteristics of the MADI PKI are its most attractive features. For high volume distributors the reduction in time of processing an order will result in great savings and profits. Confidence in the Certification Authority’s intent to provide high availability is important.	Industry	Certificate Policy

Table 2-2. DEA/Industry Pre Interview Input on MADI Project

2.4 Trust model

A discussion of Trust Models in connection with PKIs usually describes PKIs as falling into one of four categories; hierarchical; network/mesh; trust list; and key ring. Each of the models has certain characteristics, advantages and disadvantages. While a detailed discussion of trust models is outside the scope of this analysis, it became clear during the initial guidance from DEA and Industry that the MADI PKI would be a hierarchical PKI.

There will be just one Certification Authority and no cross-certification is planned. The one Certification Authority will be the “root Certification Authority”, at the top of the hierarchy, and “Trust” in the PKI will be based on the key of this Certification Authority.

This PKI structure will coincide with the structure of the regulated Industry. DEA is, for regulatory purposes, located at the top of the regulatory structure and Industry components are located in a subordinate position.

This structure will facilitate the organization of the PKI repository into a hierarchical naming scheme.

In a hierarchical PKI the certificate validation process will be less complex both in collecting the certificates and in validating them.

It has the logical advantage in that a user is most likely to trust the Certification Authority that issued the user its certificate. A MADI PKI user will only have to have trust in this one Certification Authority.

3. Findings from Interviews

3.1 Requirements for Security Services

The MADI Public Key Infrastructure must operate at a sufficiently high level of security and assurance that the security and risk management requirements of both Industry and DEA are met.

A PKI can offer 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.
- ❑ Technical 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.

The results of the interviews on the questions of the security services provided by the current paper system and the requirements for MADI, provided for some divergence in the responses that were received.

As can be seen from the exhibits below there were differences between the majority DEA view that the service of confidentiality is not currently employed and the Industry consensus that it is. The difference stems from the fact that DEA and Industry fundamentally interpreted the concept of "system" differently. It should be noted that a minority of DEA respondents did see the same perspective as Industry.

DEA respondents generally saw no DEA business case for confidentiality. The current DEA 222 Form is written in plaintext. Anyone who sees it, who can read English, and who is familiar with certain Industry terminology can understand its contents. There is no DEA enterprise information at risk. A minority DEA position was that the DEA 222 Form is currently handled in an essentially closed system and while the DEA 222 Form does not offer confidentiality, the complete Industry system employed for handling it does provide confidentiality.

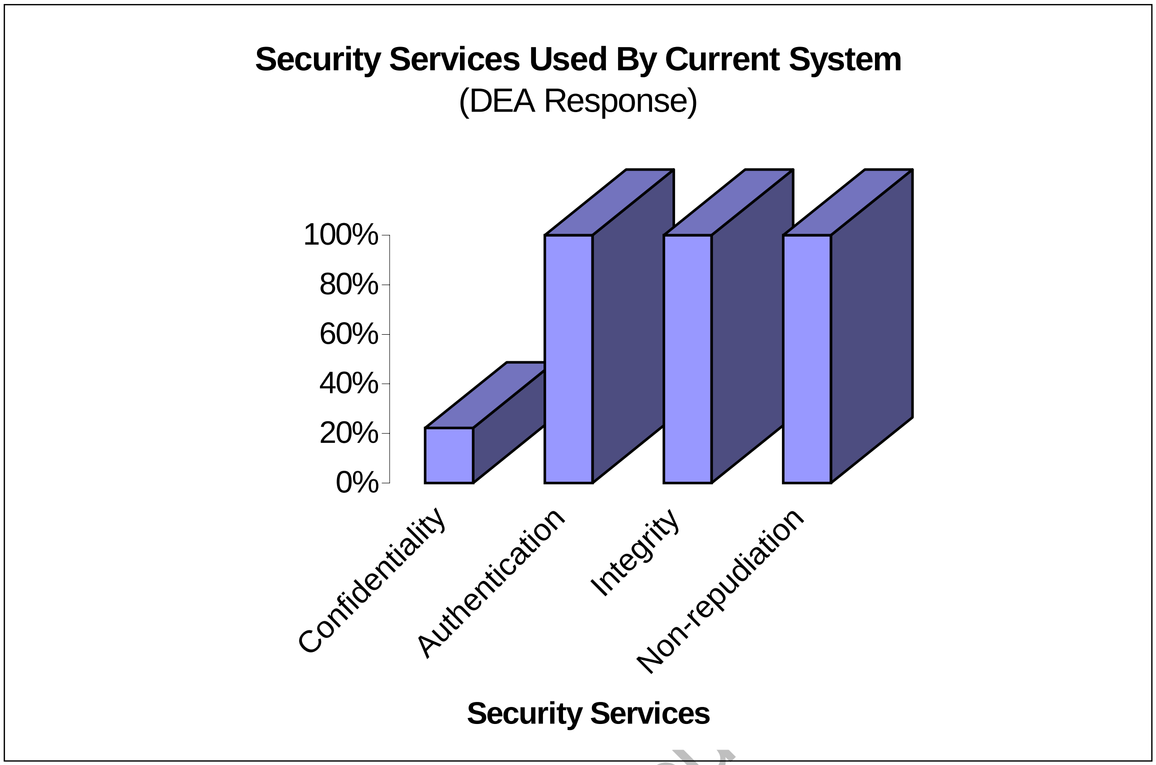


EXHIBIT 3-1. SECURITY SERVICES USED BY CURRENT SYSTEM

The Industry response was that there was a business case for confidentiality and that the service of confidentiality existed in the current system. That is to say that Industry ordering information was protected from persons that did not have a need to know. The confidentiality is not generally provided by encryption but rather by other means such as the use of Value Added Network (VAN), dial up connections with passwords and some dedicated lines. The DEA 222 Forms are sent by courier or by mail. There is little opportunity for unauthorized persons to access the information.

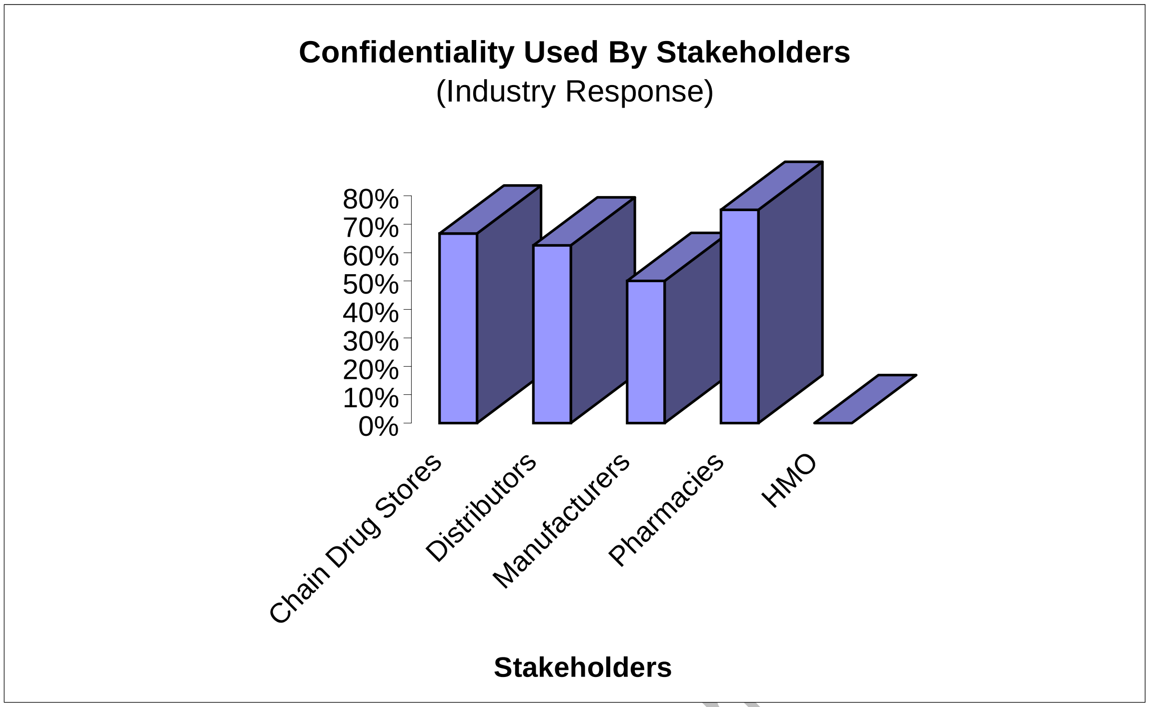


EXHIBIT 3-2. CONFIDENTIALITY USED BY STAKEHOLDERS

This same different perception carried over to the question regarding the security services that should be provided in MADI. DEA generally did not see a requirement for confidentiality and Industry did.

There did not seem to be any significant differences in Industry along Stakeholder lines.

PEC's analysis is that if Industry is satisfied with the confidentiality provided by the use of Value Added Network, dial up connections with passwords and dedicated lines and if their commerce is going to continue to be handled through such channels then encryption is not necessary for MADI. <u>However, to the extent that Industry migrates to use of the Internet, then encryption may be necessary.</u>

Industry reported that the services of authenticity, integrity, and non-repudiation existed today in their electronic ordering systems and in the DEA 222 Form paper system. DEA was unanimous in their estimate that the above listed services were present in the current DEA 222 Form system. Both Industry and DEA concurred in the requirement for these services in MADI.

There were no significant differences in Industry along Stakeholder lines.

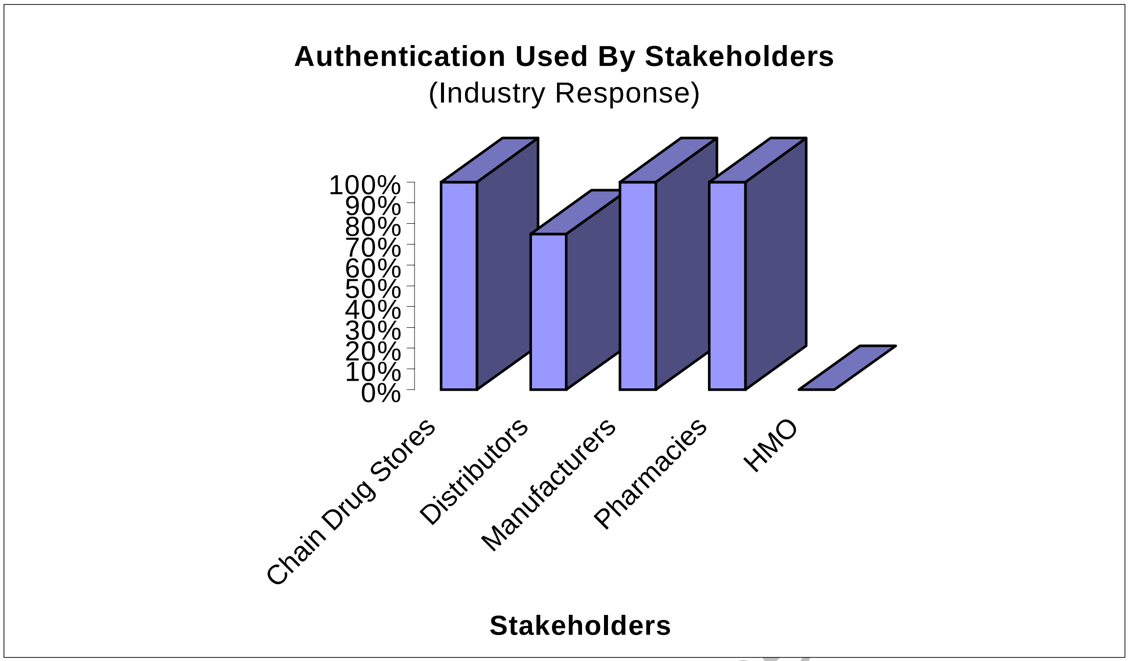


EXHIBIT 3-3. AUTHENTICATION USED BY STAKEHOLDERS

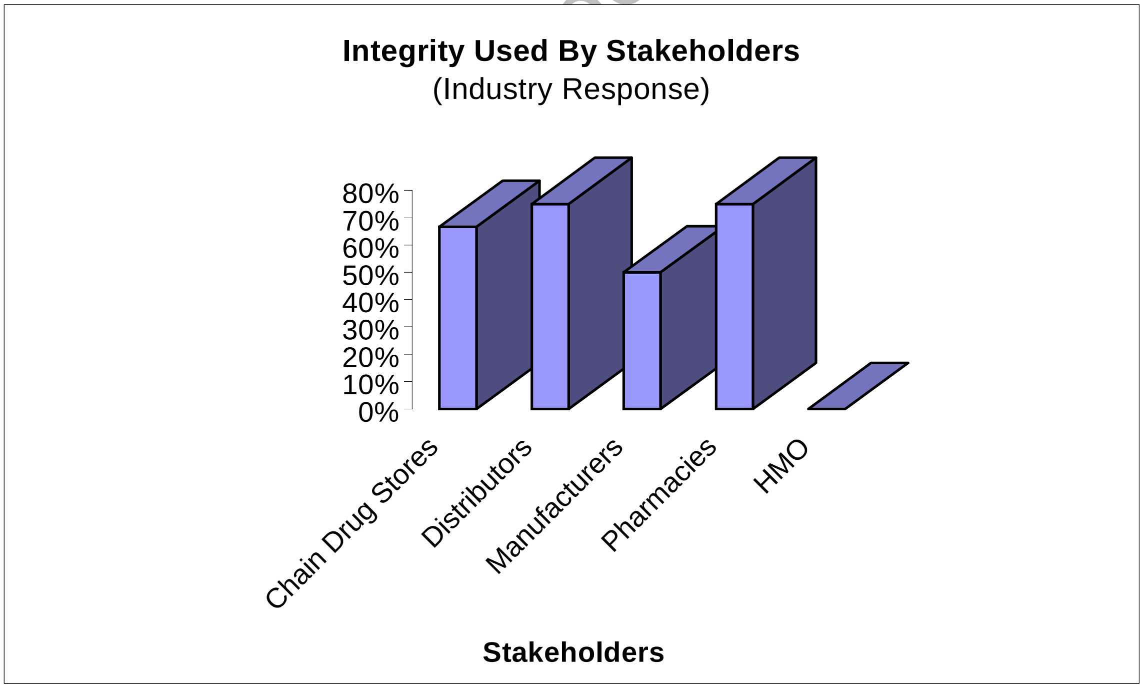


EXHIBIT 3-4. INTEGRITY USED BY STAKEHOLDERS

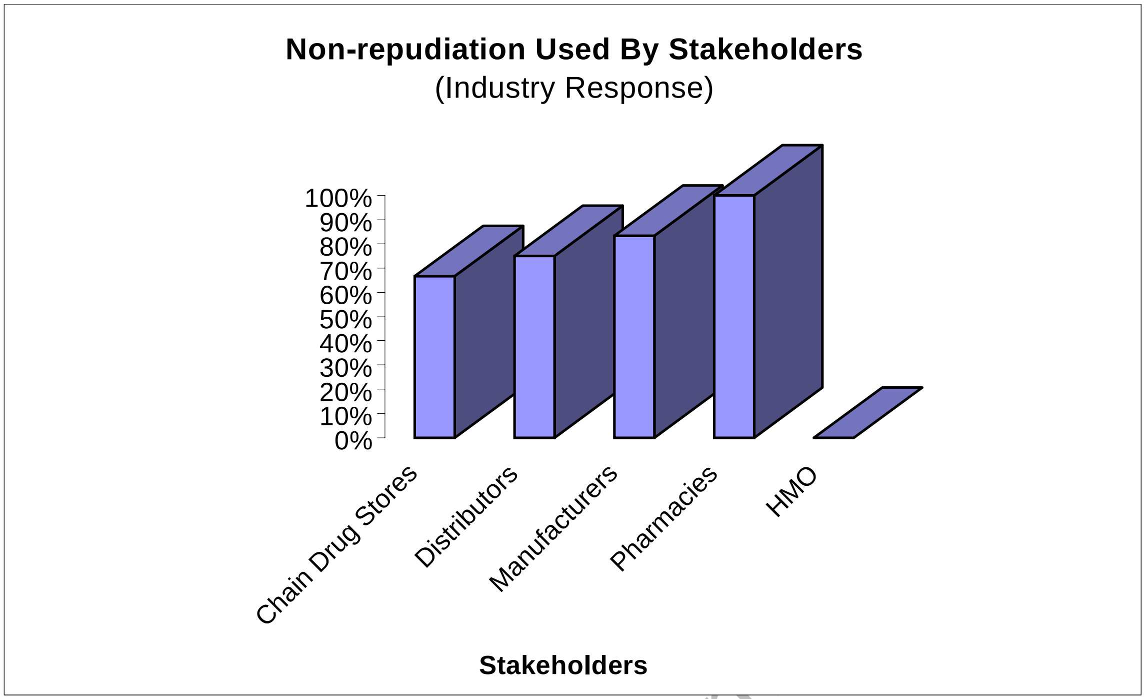


EXHIBIT 3-5. NON-REPUDIATION USED BY STAKEHOLDERS

3.2 Existing Security Standards/Environment

The Certificate Policy under which the MADI 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 current ordering process and DEA 222 Form process operate. This current level of security is, at least, a baseline for determining the security requirements for MADI. (Note: throughout the remainder of this document, the process wherein Industry generates and receives orders will be referred to as “the ordering process” and the order form as “DEA 222 Form”.)

Initial project discussions with DEA made it clear that security requirements for MADI would not be less than the current level of security. That is to say that the introduction of MADI could not bring about a reduction in the security services necessary for DEA to perform its 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, and so as not to be inconsistent with the realities of the current regulatory and political climate.

The exhibits below support the overall finding that all levels of the regulated Industry operate with a conscientious effort at security. Most implement some form of personnel security, facility security, document security, and communication security. The larger the organization, the more likely it is that the security program is well planned, well organized and implemented.

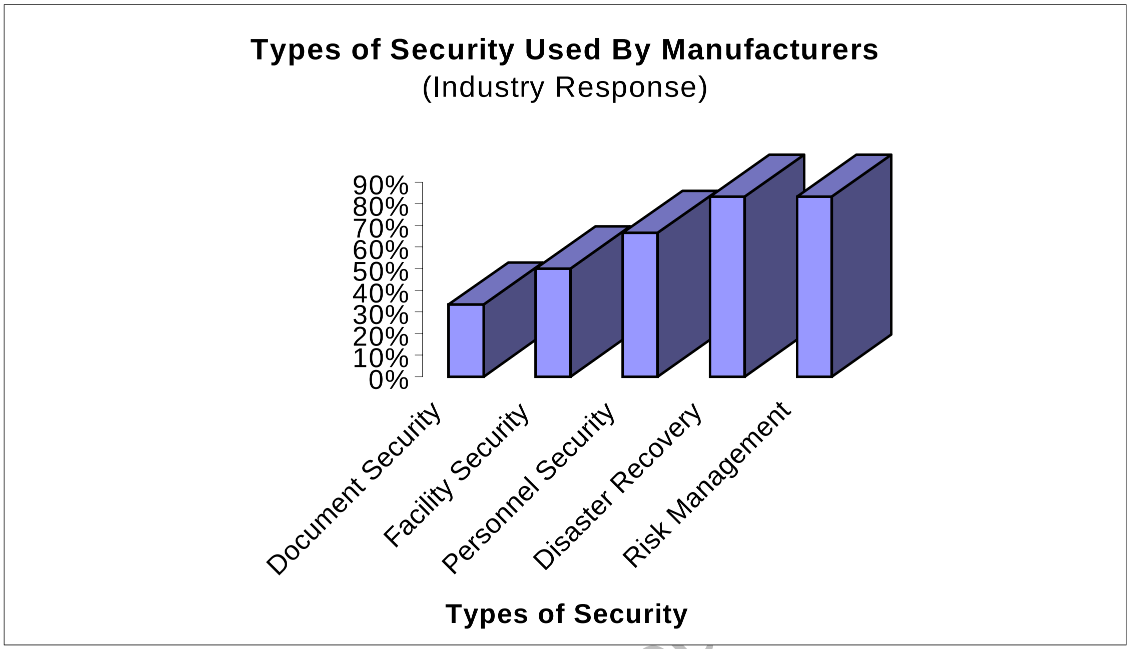


EXHIBIT 3-6. TYPES OF SECURITY USED BY MANUFACTURERS

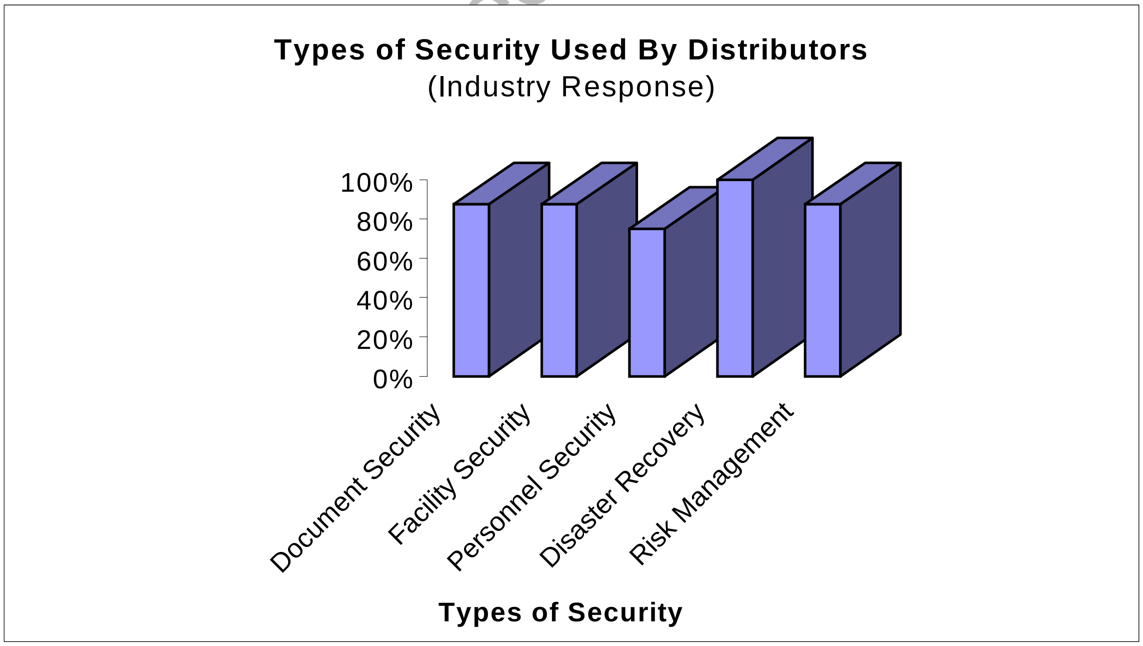


EXHIBIT 3-7. TYPES OF SECURITY USED BY DISTRIBUTORS

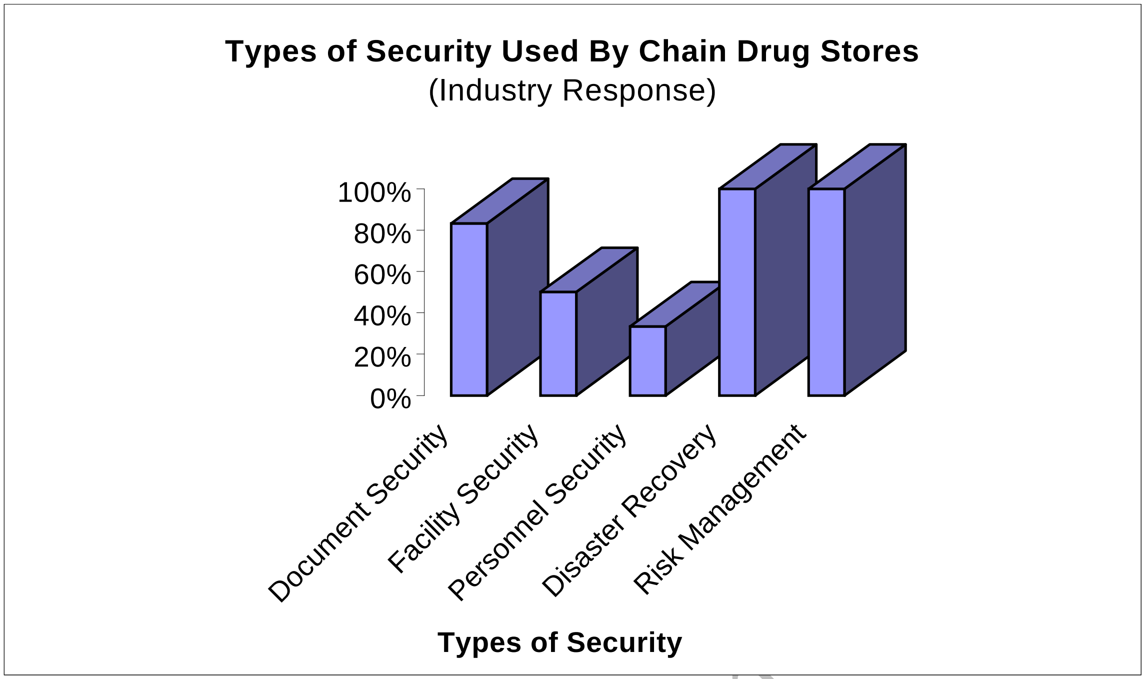


EXHIBIT 3-8. TYPES OF SECURITY USED BY CHAIN DRUG STORES

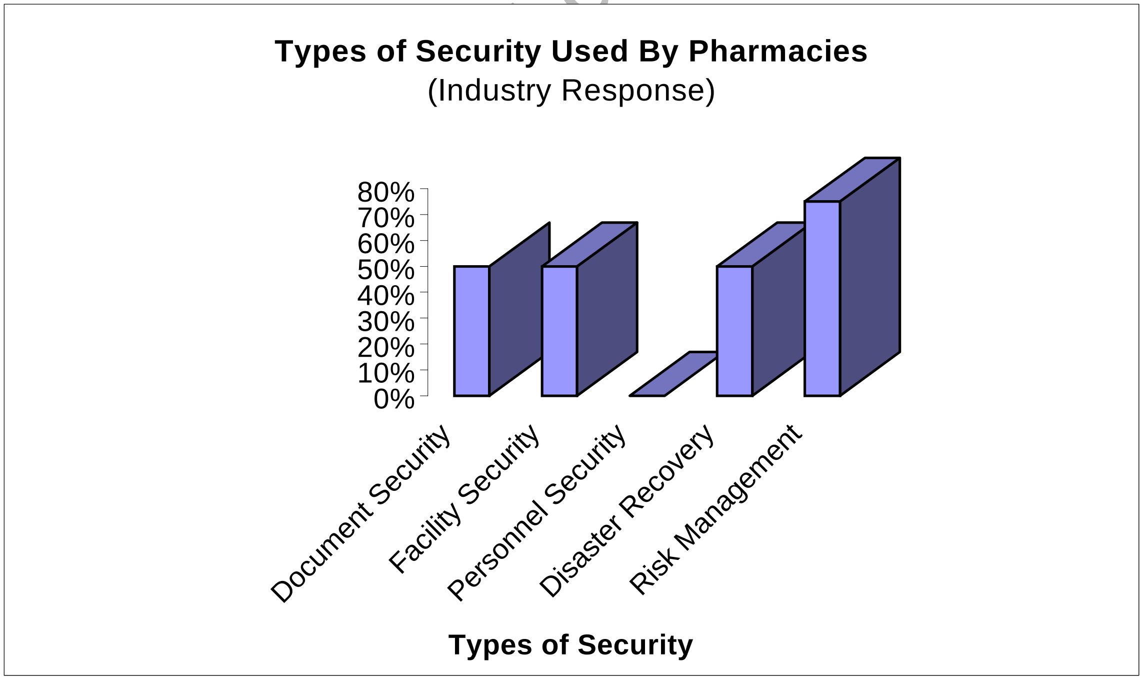


EXHIBIT 3-9. TYPES OF SECURITY USED BY PHARMACIES

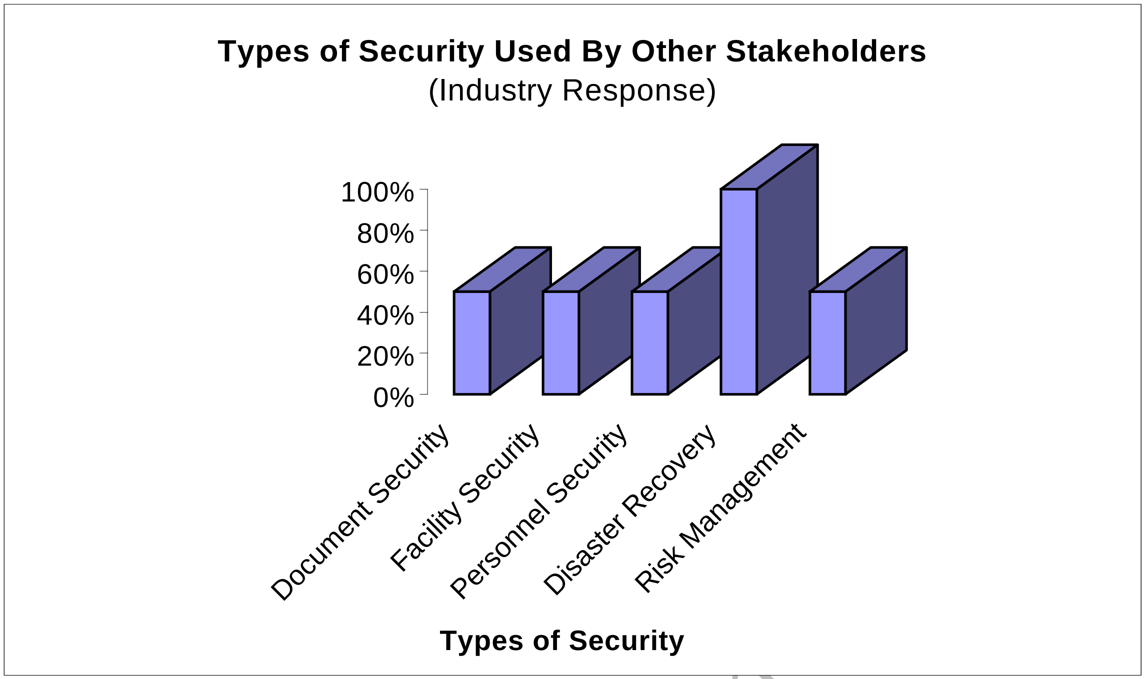


EXHIBIT 3-10. TYPES OF SECURITY USED BY OTHER STAKEHOLDERS

Not all the security concern is driven by DEA requirements or state and local requirements. As the exhibit below indicates, a significant number of respondents advised that some aspects of the security program were driven by internal business concerns such as their accounting, legal counsel and insurance company requirements.

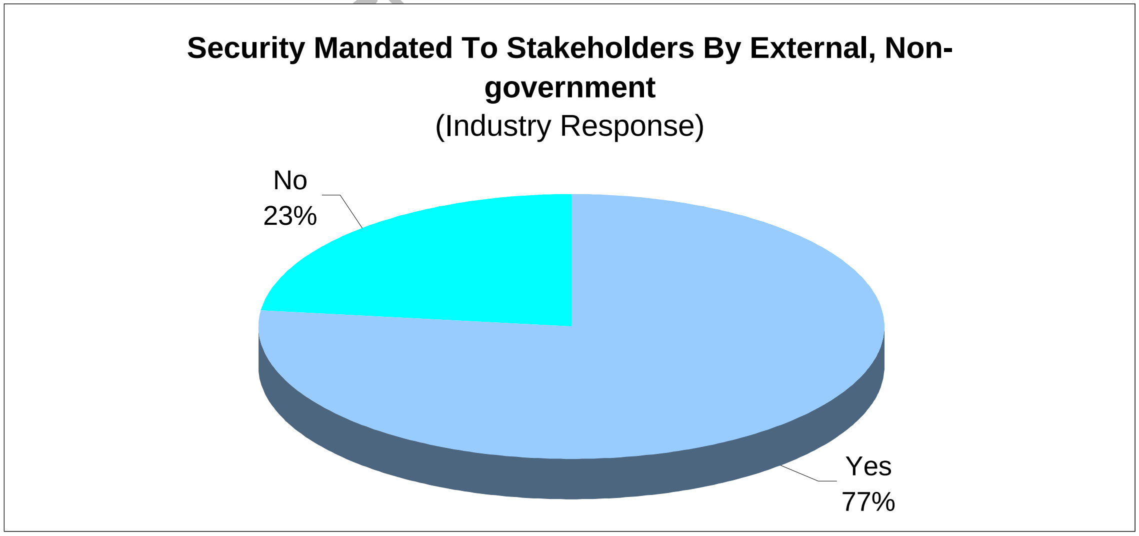


EXHIBIT 3-11. SECURITY MANDATED TO STAKEHOLDERS BY EXTERNAL, NON-GOVERNMENT

The initial project discussions had set forth the requirement of acceptability to Industry as a MADI goal. This certainly included considerations of cost and the leveraging existing architecture. The exhibit below reveals that there are not any significant, legacy PKIs that must be considered. There are a few pilot type PKIs in various stages implementation.

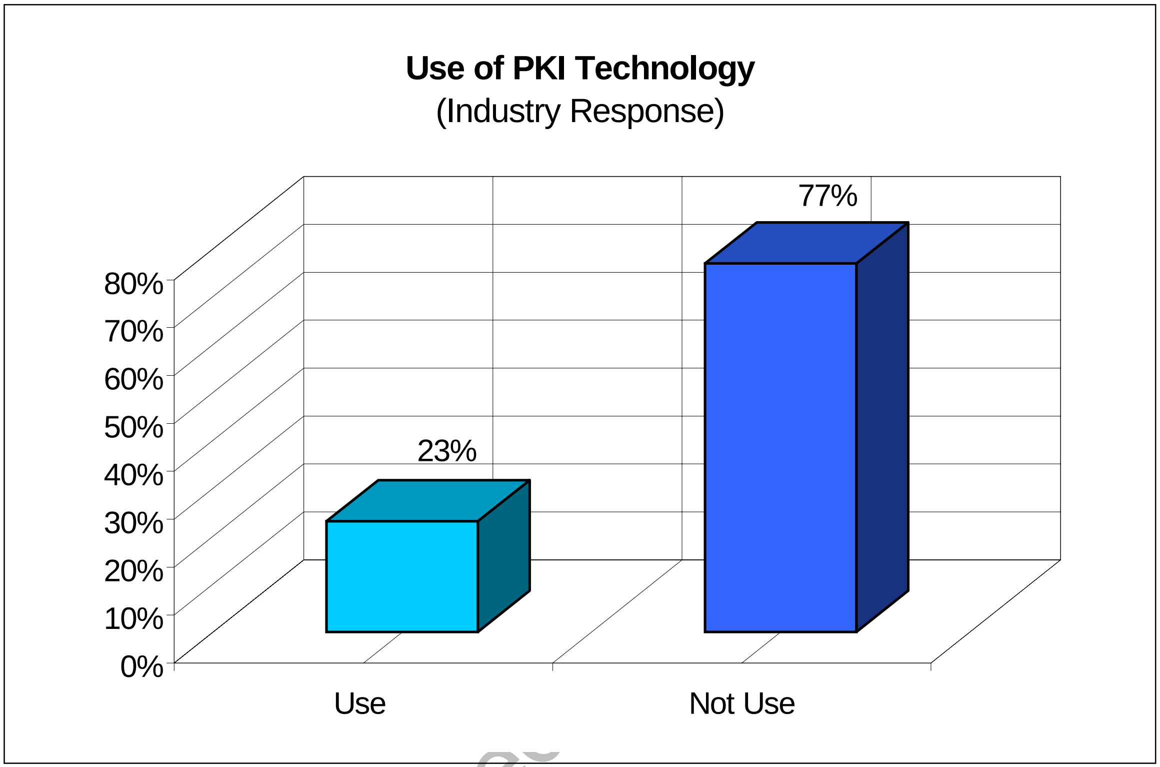


EXHIBIT 3-12. USE OF PKI TECHNOLOGY

The following exhibit captures very clearly the overwhelming, nearly unanimous sentiment of Industry regarding the nature of their support for the MADI project. The true purpose of a PKI is to provide the previously listed security services. A PKI is an electronic system, therefore it also has some characteristics common to all electronic systems and some advantages of all electronic systems over paper systems. Electronic systems are generally faster, cheaper over time, and can certainly reduce the amount of paper in the system.

Industries' support of MADI is based on their interest in "faster, cheaper, less paper" rather than their interest in the security services. Presumably, an electronic DEA 222 Form system with no security services would be just as or nearly as acceptable to Industry.

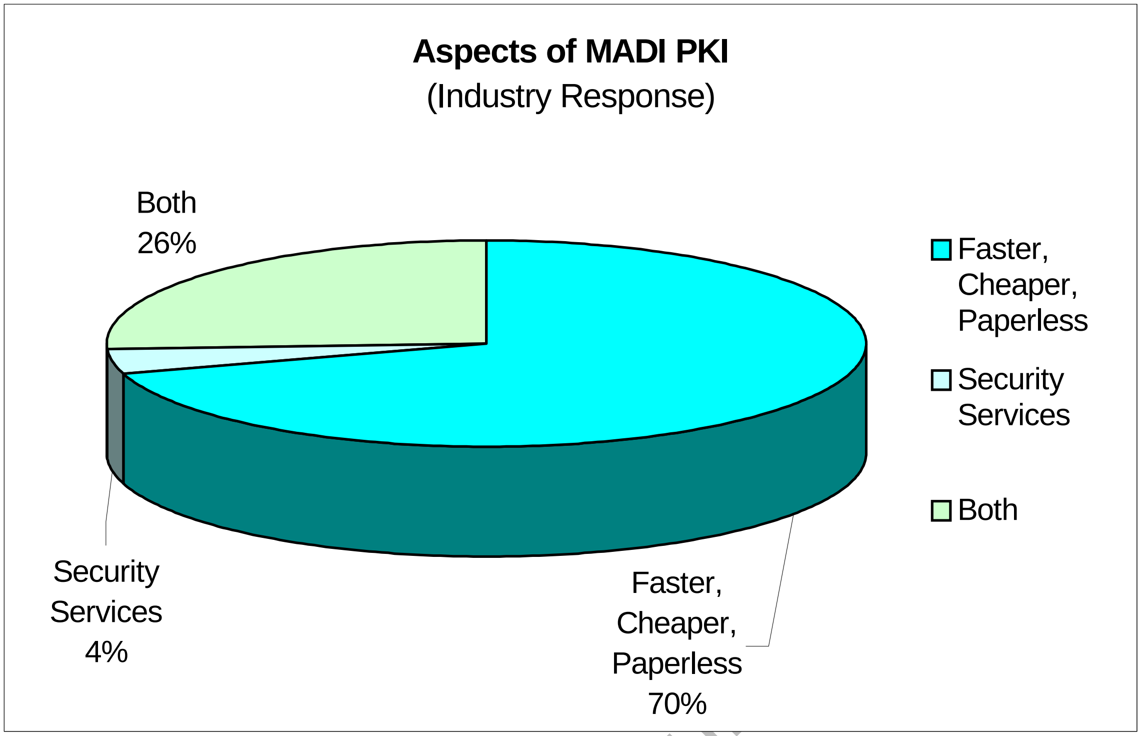


EXHIBIT 3-13. ASPECTS OF MADI PKI

Although this question was not posed to DEA, the unanimous DEA sentiment, across a range of related questions was that while every effort could be made to accommodate Industry interests, the responsibility of DEA to perform its statutory regulatory role is the primary concern.

During questions on what security services were present in the existing system, DEA respondents regularly listed the services of authenticity, integrity and non repudiation and described how they were present. The service of Authenticity exists in the DEA 222 Form process because the DEA 222 Form is issued to a specific registrant at a specific address and the DEA 222 Form is hard to counterfeit. The service of Integrity exists in the DEA 222 Form process because of the strict rules regarding erasures, alterations, and illegible entries. The recipient is either satisfied that the form received is the form intended or it is not valid. The service of Non-repudiation exists because regardless of what authority the registrant delegates to others, the responsibility can not be delegated. These security services were described as essential to the efficient and effective diversion control mission.

DEA respondents indicated a clear preference for a balanced approach in deciding the trade-off between ease of enrolling in MADI and the security standard in enrolling in MADI. The exhibit below portrays this preference.

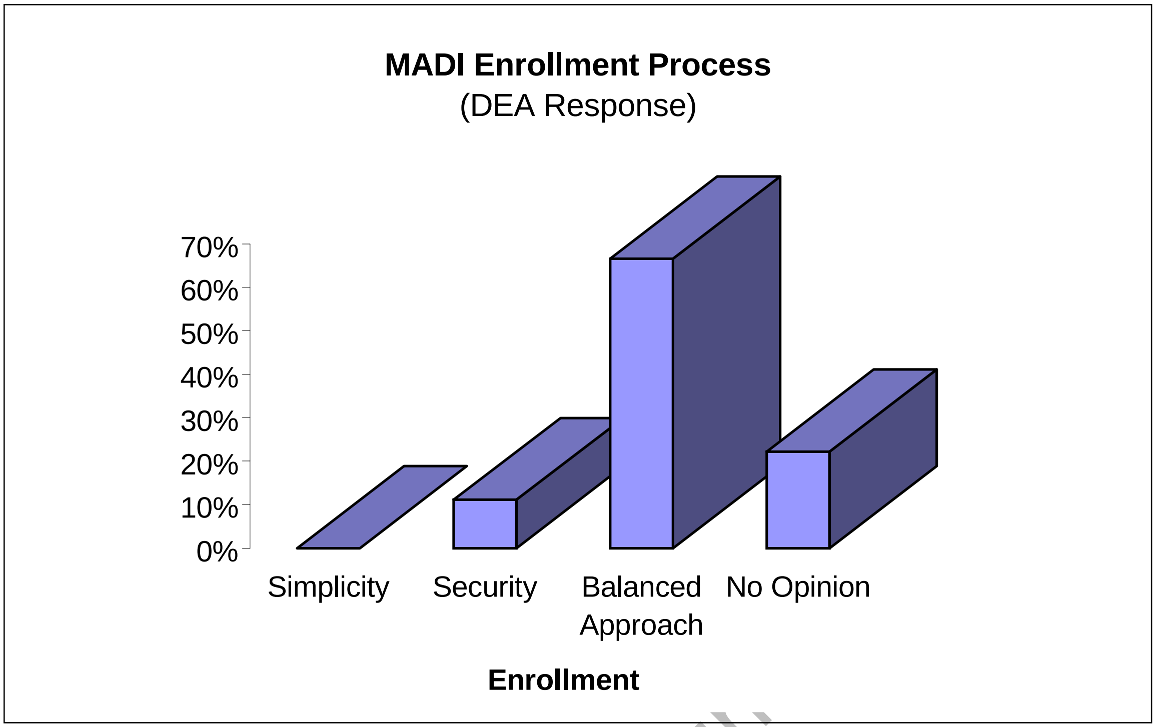


Exhibit 3-14. MADI Enrollment Process

This will be an important issue for the MADI PKI Certificate Policy. It would be possible to make the process of proving one’s identity and obtaining a certificate so undemanding that a relying party would have little confidence in the subsequent binding of identity and key. Stating one’s identity in a telephone call is an example. It would also be possible to make the proof of identity so complete and foolproof, and correspondingly more demanding that it would not be practical or acceptable to Industry. Requiring personal appearance of the applicant before the Certification Authority or Registration Authority along with letters of authorization and numerous IDs would be an example of this. The balanced approach supported by DEA respondents requires just the necessary level of identity proofing but no more, particularly if more would negatively impact Industry acceptance.

The current DEA Registration process takes a similarly balanced approach. A sufficient level of identity proofing is achieved. Unacceptably burdensome, additional proofing methods are not required. The best proof of this optimum balance is that the process is considered acceptable and not burdensome, and the nearly unanimous DEA and Industry opinion that the system is rarely spoofed.

One question asked of both DEA and Industry was the question regarding integrating MADI into existing ordering systems or alternatively creating a new, separate network. The two approaches would have profoundly different implications for cost, Industry acceptability, a host of other factors and also for security requirements. For example, the service of Confidentiality might already exist in a current ordering process to a sufficient degree to satisfy a set of trading partners. If a new ordering system with MADI were to be implemented over the Internet, then the same trading partners might require MADI to have the service of Confidentiality.

In any case this turned out to be a non-issue. The exhibits below indicate a clear consensus among DEA and Industry respondents that integration into existing networks is a preferred solution.

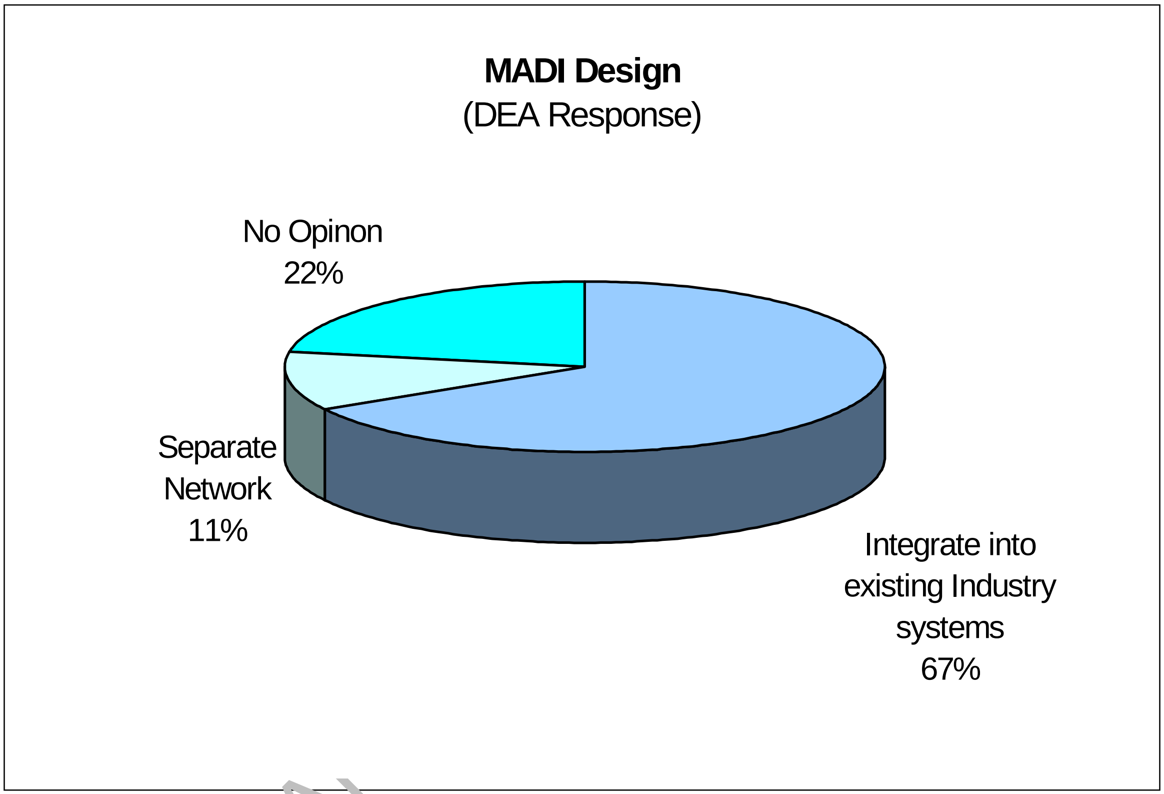


EXHIBIT 3-15. MADI DESIGN

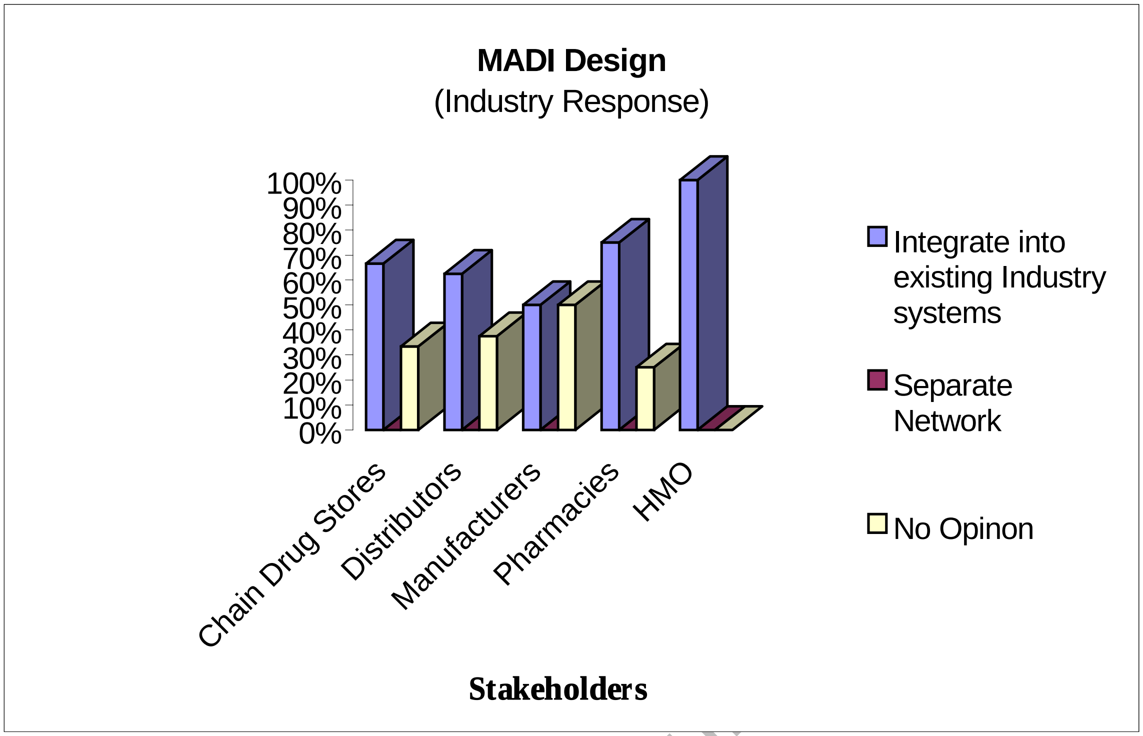


EXHIBIT 3-16. MADI DESIGN

Related to the issue of MADI integration into existing networks was the question of whether the PKI certificate would be sufficient for orders of Controlled Substances or whether some additional digital DEA 222 Form would be required to satisfy DEA requirements. The question was basically whether the certificate alone would meet at least the current standard of security. The DEA respondents overwhelmingly endorsed the concept of the PKI certificate as sufficient to make orders for Controlled Substances.

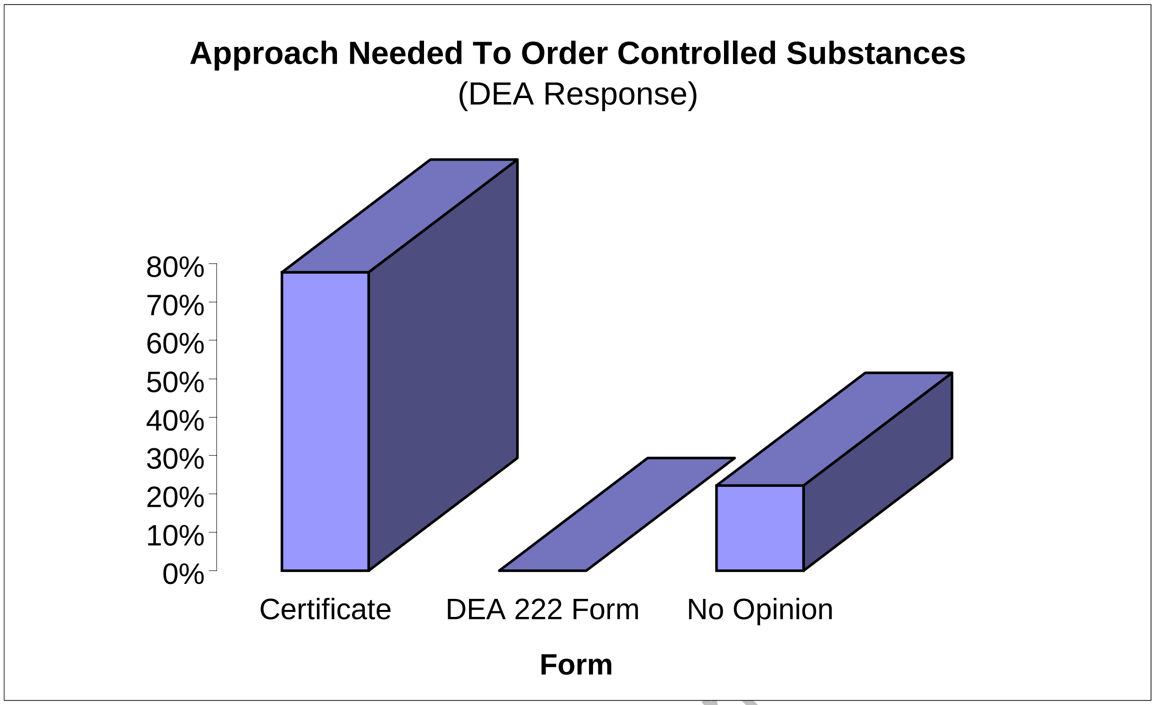


EXHIBIT 3-17. APPROACH NEEDED TO ORDER CONTROLLED SUBSTANCES

3.3 Current Threat Environment

There was a strong consensus among DEA and Industry respondents that there were few practical attacks against the current DEA 222 Form process.

Counterfeiting of DEA 222 Forms is rare or non-existent. Respondents agreed that even a perfectly counterfeited DEA 222 Form would be of little use to effect diversion in the manufacturing and distributing Industry. Industry accepts only orders from established trading partners.

Identity fraud is rarely or never encountered. Assuming the identity of a registrant on a stolen or otherwise fraudulently obtained DEA 222 Form would be of little use because the delivery of the items would be made to the legitimate Registrant's address.

Fraudulent registration with DEA to obtain DEA 222 Forms is a rare or non-occurring attack. One DEA respondent reported that a limited examination of DEA records showed no indication of those persons reported in various newspapers to have been detected as fraudulently representing themselves as Practitioners to have attempted to obtain DEA Registrant status. One such impersonator was reported to have stated that he specifically avoided going through the DEA registration process for fear of detection.

The subversions of the DEA 222 Form process that were reported were all variations of one generic problem area. This was the problem of a trusted employee of a Registrant who abused the trust. In this scenario, (1) the employee has insider knowledge (2) the employee authority is broad (i.e. signs checks, keeps books, places orders, authorizes orders, etc) (3) a distributor has to willingly or carelessly ignore indications of a "dangerous order". This type of diversion is not reported at the manufacturer or distributor level but sometimes occurs at the health practitioner level.

Both DEA and Industry respondents were provided a brief, summary explanation of the standard used to describe certificate policies and asked to choose the level of security that seemed most appropriate for their interests. The results are set forth in the exhibits below.

Medium was the level selected most often by both DEA and Industry respondents with a significant minority selecting High. The answers are useful as a general guide to respondent understandings and expectations regarding security levels.

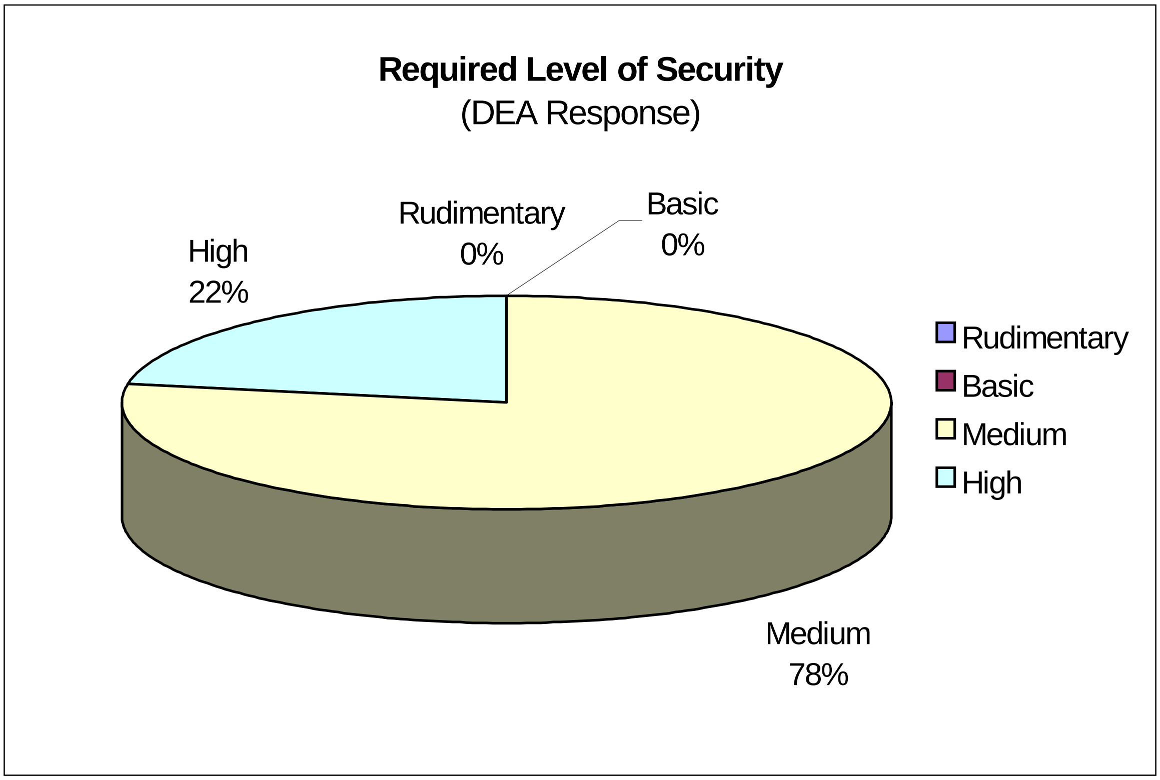


EXHIBIT 3-18. REQUIRED LEVEL OF SECURITY

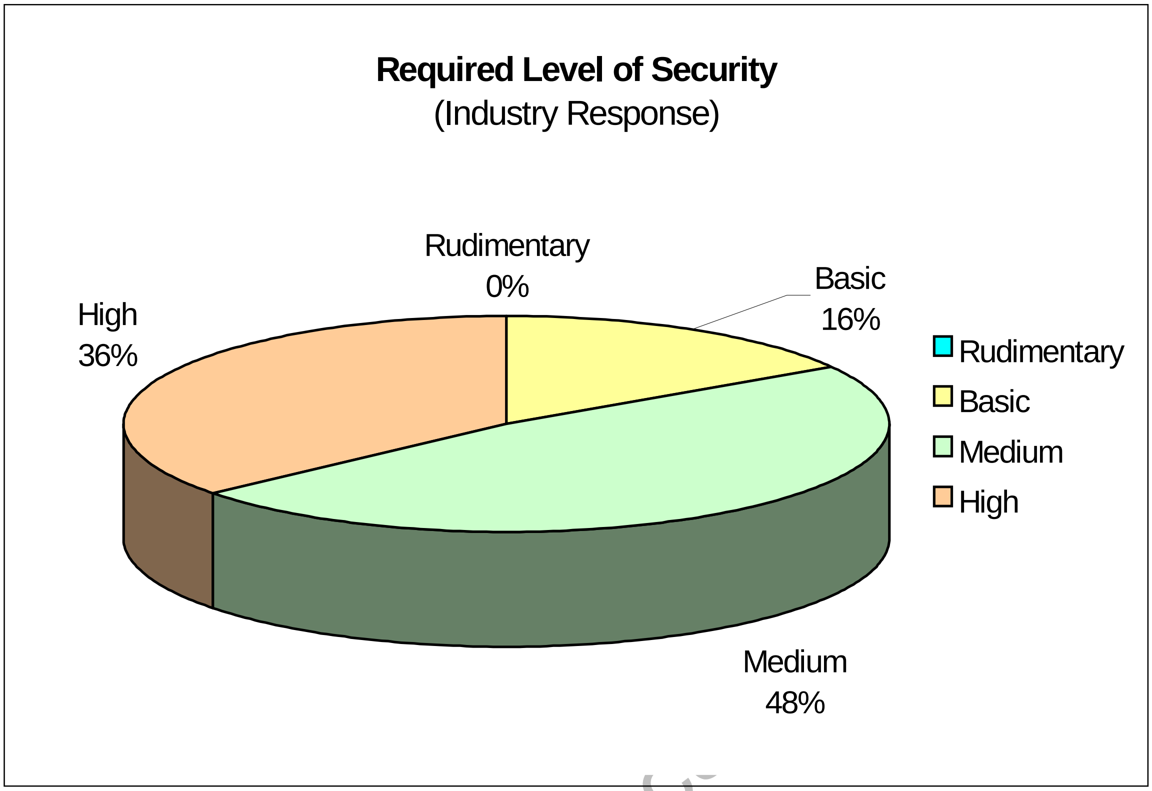


EXHIBIT 3-19. REQUIRED LEVEL OF SECURITY

A particularly significant question in terms of certificate policy requirements was the one posed to DEA respondents regarding the extent to which the Certification Authority could bear some of the risk currently borne by Industry Registrants. This could be an attractive part of the MADI concept for Industry companies considering "buy-in".

DEA respondents were strongly supportive of the concept that an Industry relying party who followed all certificate validation procedures and who accepted an order validated by a certificate that subsequently turned out to be invalid would have a defense against a charge of lack of due diligence.

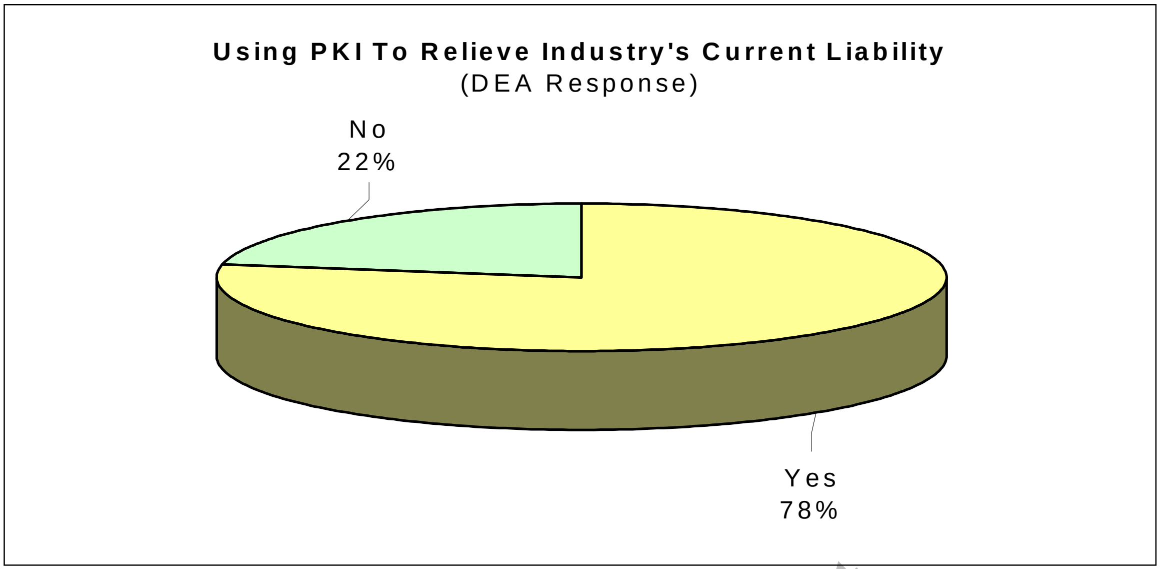


EXHIBIT 3-20. USING PKI TO RELIEVE INDUSTRY'S CURRENT LIABILITY

The next exhibit was derived from Industries responses to a question designed to determine the extent to which the regulated Industry used Risk Management to address concerns of risk. The underlying idea was that the response to this question might be a "truth teller" as it would indicate their real perception of the threat environment. The responses indicated rather widespread use of risk management techniques.

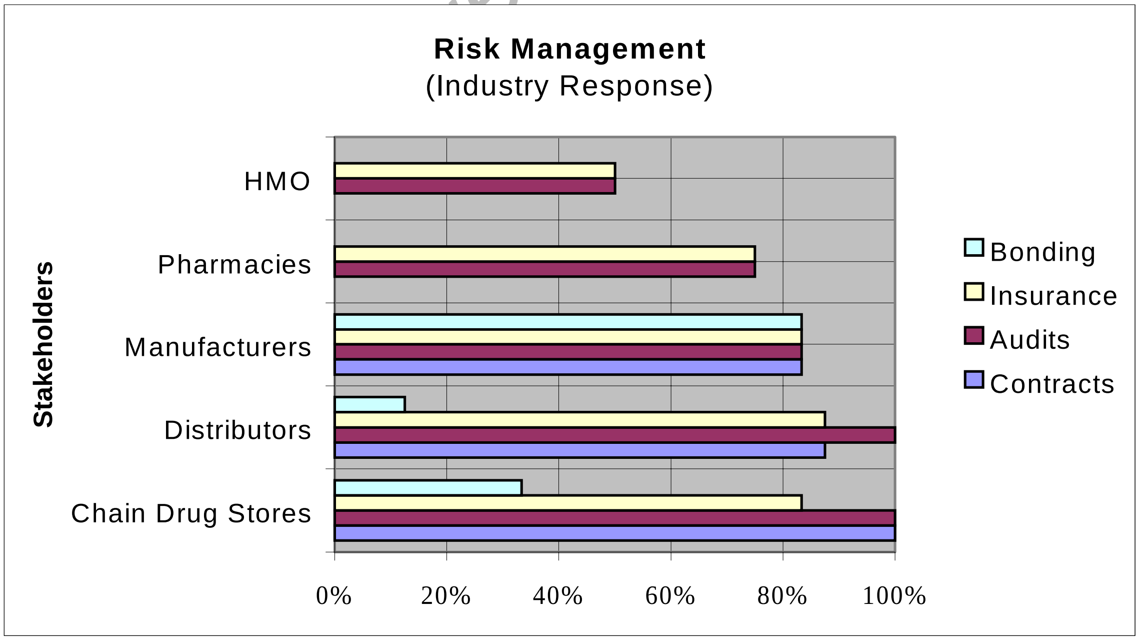


EXHIBIT 3-21. RISK MANAGEMENT

4. MADI PKI Certificate Requirements

4.1 Background

This MADI PKI Certificate Requirements section is not a Certificate Policy, rather, it is a statement of the general level of certificate requirements for the MADI PKI. It is based on the analysis of the assurance and security requirements of Industry and DEA as found to date. A Certificate Policy would contain much more specific detail for those items addressed. It should be noted, further, that not every item recommended in the Internet Engineering Task Force Request For Comment 2527 is even addressed.

The level of detail, in most instances, does not extend below the level of “component”. As expressed in Request For Comment 2527, the provisions (or items in this document) of a Certificate Policy 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 Certificate Policy that can be dismissed as “boilerplate”. Having established that, some items are more useful and informative to the general reader in understanding the general framework of the policy under which certificates are to be issued.

The set of items included in the Requirements section below was selected by the following process. All of the data collected in the interviews with Industry and DEA, and the guidance given by DEA personnel was evaluated and plotted.

The data appeared to fit best around a line defining a medium level policy for a Certification Authority as defined in the significant subsets of items contained in section 3 above. The full set of items or provisions of a medium level policy as defined by the “Digital Signature and Confidentiality Certificate Policies for the Government of Canada Public Key Infrastructure” were reviewed. This document is widely cited as the best single document on the subject of the meaning of levels of security for PKIs.

The full set of items, or provisions in Request For Comment 2527 were examined and mapped to the MADI project. The items considered most informative and or thought provoking to DEA decision-makers were selected for this document. The language and terminology of a Certificate Policy would be more precise than in this requirement document.

The Object Identifier (OID) of the Certificate Policy under which a certificate is issued will provide a means to distinguish between the class of certificate subjects authorized to distribute Schedule 2 Controlled Substances and subjects of certificates authorized to distribute Schedule 3-5 Controlled Substances.

4.2 Requirements

MADI PKI REQUIREMENTS

1	Overview	The MADI PKI will be operated under the authority of the DEA Office of Diversion Control Policy Management Authority (PMA). The purpose of the MADI PKI is to bring the security services of authenticity, integrity and non-repudiation to the DEA 222 Form process. The Certification Authority will be governed by the laws of the US and DEA regulations. The Certification Authority will be operated under a policy that emphasizes and strongly warrants reliability of the PKI and its availability to subscriber’s 24 hours a day 7 days a week.
2	Policy Management Authority (PMA)	The Office of Diversion Control will establish a MADI PKI PMA. The PMA is responsible for setting, implementing, and managing certificate policy decisions regarding the MADI PKI. The PMA is composed of Office of Diversion Control personnel. It will meet quarterly or as required. At each meeting there will be an opportunity for PKI enrollees from Industry to present matters for consideration.
3	Operations Management Authority (OMA)	The PMA will establish an OMA. The OMA will carry out the policy of the PMA The OMA will direct the activities of the MADI PKI Manager. The OMA is composed of Office of Diversion personnel. It will be at least 1 full time position.
4	The PKI Manager	The PKI Manager will run the MADI PKI on a day to day basis. The PKI Manager will be subordinate to the OMA. The PKI Manager and its staff may be Office of Diversion personnel, may be contractor personnel or may be a combination of both.
5	Community and Applicability	The community of users for the MADI PKI is limited to DEA employees and DEA Registrants who meet all other requirements. The certificates are limited in applicability to the signing of orders by Registrants engaged in the manufacture, distribution, and dispensing of Controlled Substances and to the signing of official transactions to DEA.
6	Certification Authority	The MADI Certification Authority is responsible for (1) issuing, signing, and managing through their life cycle, certificates binding subscribers with their signature verification keys (2) promulgating certificate status through CRLs (3) ensuring adherence to the provisions of the Certificate Policy. The Certification Authority will issue and operate in accordance with the provisions of its Certification Practice Statement.
7	Certification Authority obligations and warranties	The Certification Authority warrants to Subscribers that identities of subjects of certificates are correct and that subjects do hold the corresponding private signature key. Further it warrants that relying parties who correctly perform certificate validation procedures may rely on the validity of the outcome in making identity decisions required under the Controlled Substances Act (CSA). The Certification Authority will make warranties (to be determined) regarding reliability and availability.

8	Legal and financial liability of Certification Authority	To be described fully in the Certificate Policy. The essence will be that the CA disclaims any liability of any kind whatsoever for any award, damages, or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon, a MADI PKI certificate or its associated public/private key pair.
9	Adjudication of disputes	To be fully described in the Certificate Policy. Will describe the procedures for users and relying parties to resolve disputes with the CA.
10	Registration Authority	Registration of PKI subscribers will be handled by the Certification Authority. There are no provisions for Registration Authority's at this time.
11	Repository	The Certification Authority will ensure that there is a repository wherein MADI PKI certificates are published and are available to members of the community to validate signatures. The repository will be an X.500 compliant directory with LDAP access. The Certification Authority will assert a very high (to be defined) level of reliability and availability of the repository. The MADI Certificate Policy will be published in the repository. CRLs will be published in the repository.
12	Certificates	MADI PKI certificates will be X.509v3 for end entity certificates and X.509v2 for CRLs. End entity certificate validity period will be the same as the current DEA Registration period for a registrant. The certificates will use the appropriate FPKI/PKIX profile.
13	Subscribers	Subscribers hold certificates issued by the Certification Authority. Subscribers will be limited to fully qualified members of the community. In the event there were to be cross certification between the MADI Certification Authority and another Certification Authority, the other Certification Authority would be a relying party. Subscribers have obligations in the MADI PKI Certificate Policy. The Certification Authority will ensure that the Subscriber enters into a written agreement to abide by all the terms and conditions of the Certificate Policy regarding Subscribers. An OID will be used in the certificate to classify subscribers as to the schedules of controlled substances they may manufacture, distribute, and dispense.
14	Relying Parties	Relying parties are limited to subscribers or cross-certified Certification Authority's. Relying parties are responsible to perform checks for validity and appropriateness on each certificate presented. Relying parties are responsible to examine the Certificate Policy to understand all of their rights and obligations under the Certificate Policy.
15	Approved and prohibited applications	The Certification Authority must be satisfied that all applications that intend to use MADI PKI certificates use the certificates properly. The manner in which the CA is satisfied will be described in the CP. The Certification Authority will set the minimum requirements for such applications. One of the requirements will be that the CRL is automatically checked at each transaction.

16	Revocation of certificates	Certification Authority will revoke end entity certificates if end entity private key is lost or compromised or if certificate information changes. CRLs will be published at least every 12 hours. Certificates will be revoked for subscriber failure to abide by subscriber obligations. Certificates will be revoked if DEA registration is revoked. DEA will provide Registration revocation information to Certification Authority daily. Subscribers will be permitted to cache CRL data daily.
17	Certification Authority trusted roles	All critical functions of the Certification Authority, those functions that impact on security policy, must be performed by at least 3 persons.
18	Personnel security	Certification Authority staff will have appropriate DEA clearances, training and experience.
19	Recorded events	The Certification Authority will record all events relating to the security of the Certification Authority.
20	Compliance inspection	External audit of the Certification Authority for Certificate Policy compliance is required every year.
21	Certification Authority records	The Certification Authority activity records will be maintained, 7 years, the statute of limitations for violations of the Controlled Substances Act.
22	Types of names	Names of certificate subjects must be x.500 Distinguished Names (DN) and the same Common Name (CN) as used in the DEA Registration process. The DEA Registration Number issued to each Registrant will be included in the DN as a Unique Identifier (UID). The address of the DEA Registrant will be included in the altName field of the certificate.
23	Key pair generation	End entities will generate their digital signature key pair. The public key will be delivered to the MADI Certification Authority in accordance with RFC 2510 Certificate Management Protocols or via an equally secure manner approved by the PMA. The key generation will be performed in a FIPS 140-1 level 1 module.
24	Cryptography	Cryptographic modules must be FIPS 140-1 validated. Cryptographic algorithms must be FIPS approved. Keys must have the equivalent of 1024 bit RSA modulus.
25	Protection of private keys	Certification Authority signing key must be in hardware FIPS 140-1 level 2; end entity private key in hardware or software. All entities are responsible for the protection of private keys and activation data.
26	Certification Authority public key delivery to end entity	The Certification Authority public key must be delivered to the end entity in accordance with RFC 2510 Certificate Management Protocols or via an equally secure manner approved by the PMA.

27	Application for a certificate	End entity certificates will be issued within a maximum of 48 hours of receipt of a completed application for a certificate from a DEA Registrant. The Certification Authority will not be a "choke-point" for commerce. The Certificate Policy and Certification Practice Statement will contain provisions for routine re-key and re-key after revocation.
28	Authentication of individual identity	End entity proof of identity is required. The proof of identity may be presented on-line or in person. The proof of identity will consist of (1) a copy of the DEA Registration Certificate, (2) one government issued photo ID, and (3) a proof of current employment document, may be a letter on letterhead stationary, with current work address, IP address, e-mail address and telephone number.
29	End entity proof of possession of private key	End entity will have to prove possession of private key.
30	Site location, construction and physical access	The facility that houses the Certification Authority and the Repositories will meet a high standard of protection. It will be located in an area sufficiently remote from other activity or traffic. The facility will be of reinforced construction, locked, alarmed, and guarded or under surveillance 24x7. Access will be limited to authorized personnel and authorized and escorted visitors. There will be high quality security storage containers within the facility for the storage of sensitive materials.
31	Disaster recovery	The Certification Authority will operate a "hot" running spare co-located with the Certification Authority and repository. There will be a remote alternate site ready to assume the Certification Authority function in 6 hours. The remote and alternate sites will have the same level of protection as the principal sites. Disaster recovery planning will include a high degree of protection in the areas of: power; air conditioning; water; fire; media storage. The Certificate Policy and Certification Practice Statement will address procedures to be followed in the event of Certification Authority signing key compromise.
32	Network security	The Certification Authority will be protected from attack through the network to which it is attached through a combination of network security methods.
33	Computer security	The appropriate level of functionality will be achieved through a combination of operating system, PKI software and physical safeguards.
34	Fees	MADI PKI end entities will pay charges (to be determined) to the CA for services; possibly a fixed enrollment fee and a fee for accesses to the directory.

Table 4-1. MADI PKI Requirements

Appendix A- List of Interviews, Site Visits, Meetings and Conferences

Manufacturers

Abbot Laboratories Abbot Park, Illinois	Marieta Neiss, Director Controlled Substance Corporate Regulatory Affairs
Mallinckrodt St. Louis, Illinois	Karen Harper, DEA Compliance Coordinator Ted Loucks, Information Services Group Jack Frauenhoffer, Interim Compliance Manager Joan Levy, Director of Administration for Dosage Products
Wyeth- Ayerst Cherry Hill, New Jersey	Peaches Larro, Associate Director Controlled Substance Compliance
Noramco Wilmington, Delaware	Ann Strusowski, Compliance Coordinator
Novartis East Hanover, New Jersey	Tracey Hernandez, DEA Auditor Earl Calloway, Systems Consultant IT Dave Krozser, EDI Specialist Lorretta Wolf, Manager EDI (Business Department) John Renolds, Distribution Coordinator Jan Hodge, Customer Service Representative
Barr Laboratories Northvale, New Jersey	Dave Mendelsohn, Director of Security/DEA Affairs Ralph Goldstein, IT Specialist

Distributors

Barnes Wholesale Drug Engelwood, California	Robert Swartz, CEO Angelo Grandi, Operations Manager
McKesson HBOC	Donald Walker, Senior Vice President Distribution Bruce Russell, Vice President Distribution and Operations Gary Hilliard, Director of Regulatory Affairs Tom McGill, IT Systems Richard Wood, Distribution Center Manager
Cardinal Health	Rodney Waller, Vice President Corporate Compliance Steve Reardon, Director Corporate Compliance Carol Verrastro, Manager Customer Service Jill Flieman, Manager EDI

Bergen Brunswig Drug Company Orange, California	Jim Snyder, Vice President Operations Chris Zimmerman, Director Regulatory Compliance and Security Services Leia Andrews, Manager EDI Technologies David Tessman, Manager IT Brian Jones, Manager IT Katherine DeVera, Manager Customer Service Jim McLaughlin, Research and Development Tom Bergman, Project Systems Specialist Danny Moore, Distribution Center Manager
The F. Dohman Company Minneapolis, Minnesota	Francis Charland, Vice President Compliance Steve Strobel, Manager Purchasing Steve Deloat, Manager IT Group
Walsh Distribution Texarkana, Texas	Randy Wilson, Vice President Purchasing Tina Emilia, EDI Coordinator

Chain Drug Stores

Eckerd Corporation Largo, Florida	Mickey Carter, Director of Loss Prevention and Regulatory Compliance Ken Fisher, Manager IT
Giant Food Incorporated Landover, Maryland	Sheldon Pelovitz, R.Ph., Director Pharmacy Professional Services Mark Stachowski, Manager EDI Systems Development
Rite Aid Corporation Harrisburg, Pennsylvania	Janet Getzey Hart, R.Ph., Manager Government Affairs August J. Dobbish, R.Ph., Esquire, Manager Government Affairs
Publix Super Markets Lakeland, Florida	Ron Miller, Director of Pharmacy Operations
CVS Corporation Woonsocket, Rhode Island	Bill Masters, Vice President of Health Care Business Carlos Ortiz, Government Affairs Linda Cimpbron, Licensing Manager Scott Jacobson, Operations Analyst John Rinkas, Information Systems Security Audit Manager Mike McGint, Director Internal Audit Russ Pierce, Security Administrator
Walgreen Company Deerfield, Illinois	Audrey H. Neely, R.Ph., Manager Professional Affairs Health Services Dwyne Pinon, Attorney Jim Ash, Pharmacy Marketing and Inventory Control Trish Smith, Centralized Purchasing John Martello, IT Group

Pharmacies

National Community Pharmacists Association Alexandria, Virginia	B. Douglas Hoey, R.Ph., M.B.A., Associate Director Management, Professional, and Student Affairs
Academy of Managed Care Pharmacy Alexandria, Virginia	Richard N. Fry, R.Ph., Senior Director of Pharmacy Affairs Merle S. Fossen, Pharm. D., Pharmacy Affairs Manager
McArthur Drugstore Washington, DC	Roy Goldstone, Pharmacist

Associations

National Association of Chain Drugstores Alexandria, Virginia	Mary Ann Wagner, Director Brian Gallagher, R.Ph., J.D., Director, Pharmacy Regulatory Affairs
National Wholesale Druggists' Association Reston, Virginia	Diane P. Goyette, R.Ph., J.D., Director Regulatory Affairs Robert Borger, Director, Standards and Guidelines
Food Marketing Institute Washington, D.C.	Ty Kelley, Director Government Affairs
National Association of Boards of Pharmacy Park Ridge, Illinois	Carmen Catizone, Executive Director

Other Registrant Types

American Methadone Treatment Association New York, New York CODAC Treatment Center Cranston, Rhode Island	Michael Rizzi, Director
George Washington Health Plan (HMO) Bethesda, Maryland	Dr. John Zatti, Pharmacy Operations Consultant
Merck Medco	Robert Swartz, Compliance Manager

DEA Office of Diversion Control

Terrance W. Woodworth, Deputy Director
Patricia Good, Chief Liaison and Policy Section
Jim Pacella, Chief Regulatory and Program Support Section

Michael Moy, Chief Drug Operations Section
Michael Mapes, Deputy Chief Liaison and Policy Section
Elizabeth Willis, Deputy Chief Operations Section
Denise Curry, Chief Liason Unit
Sharon K. Partlo, Chief Policy Unit
Terrance Boyle, DPM DEA ODC, New Orleans, Louisiana
Larry Lockhard, Supervisor, DEA ODC Birmingham, Alabama

Site Visits, Meetings, Conferences and Seminars

May 10, 1999 DEA and Industry MADI PKI Project Kick Off Meeting
July 1-2, 1999 NWDA Productivity and Technology Conference
July 8, 1999 Federal Public Key Infrastructure/Technical Working Group
August 12, 1999 Midwest Controlled Substance Handlers Meeting
September 8, 1999 Federal Public Key Infrastructure/Technical Working Group
September 9-10, 1999 DEA/Industry Conference Biloxi Mississippi
September 14, 1999 Bindley Western Distribution Center Site Visit
September 20, 1999 Rite Aid Corporation Site Visit
September 21, 1999 NWDA Technical Working Group Meeting
October 13, 1999 Federal Public Key Infrastructure/Technical Working Group
October 19, 1999 Bergen Brunswig Distribution Center Richmond Virginia
October 21, 1999 McKesson HBOC Distribution Center Landover Maryland
November 12, 1999 Federal Public Key Infrastructure/Technical Working Group
November 16, 1999 NWDA Compliance Working Group Meeting

Appendix B- List of 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
American Management Systems, Inc. (AMS)	Analysis of Electronic Data Interchange	May 25, 1990	AMS Deliverable 3.1
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
Baroni, Tracy	Changes to CFR Section 1300	January 8, 1998	National Associating of Chain Drug Stores (NACDS)
Bukar, Nancy	National Wholesale Druggists' Association 's Comments	September 18, 1998	National Wholesale Druggists' Association (NWDA)
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 8th 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
Ford, W. Housley, R. Polk, W. Solo, D.	Certificate and CRL profile; Internet X.509 Public Key Infrastructure	October 22, 1999	http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-00.txt

Kocot, Lawrence S.	Testimony by NACDS	August 6, 1998	NACDS
Leibovich, Mark	Certified Mail Web-Style	Unknown	Washington Post
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
Schultz, William B.	FDA rules and regulations	March 20, 1997	Federal Register Vol. 62, No. 54
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
Unknown	Electronic Prescriptions	November 19, 1998	NACDS
Unknown	Supplementary issue in NACDS Proposal to change 1306	January 8, 1997	Unknown
Unknown	Capitalizing on an opportunity	November 1995	Health Data Management Vol. 3, No. 10
Unknown	ProxyMed Expands its Electronic Scripts Reach	Unknown	Health Data Network News
Wagner, Mary A.	Proposed Amendments to CFR 1306	October 31, 1997	Mary Ann Wagner

Appendix C– Document Acronyms

ACF	Access Control Facility
ARCOS	Automation of Reports and Consolidated Orders System
ATM	Asynchronous Transfer Mode
CA	Certification Authority
CN	Common Name
CONOPS	Concept of Operations
COTS	Commercial Off the Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Controlled Substances Act
DN	Distinguished Name
DEA	Drug Enforcement Administration
EC	Electronic Commerce
EDI	Electronic Data Interchange
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
GEIS	General Electric Information Systems
GOC	Government of Canada
GPEA	Government Paperwork Elimination Act of 1999
HMO	Healthcare Maintenance Organizations
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MADI	Manufacturers and Distributors
MOU	Memorandum of Understanding
NDC	National Drug Code
NTIS	National Technical Information Service
OD	Office of Diversion Control
OID	Object Identifier
OMA	Operations Management Authority
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMA	Policy Management Authority

POC	Proof of Concept
POP	Proof of Possession
RA	Registration Authority
RACF	Resource Access Control Facility
RFC	Request For Comment
RSA	Rivest Shamir Adleman
SNA	Systems Network Architecture
TCP/IP	Transmission Control Protocol / Internet Protocol
UID	Unique Identifier
VAN	Value Added Network
VPN	Virtual Private Network
WAN	Wide Area Network
X.500	The standard for directory services
X.509	The standard for PKI certificates
XML	Extensible Markup Language