
Public Key Infrastructure Analysis

DEA Diversion Control

E-Commerce PKI Certificate and CRL Profile

Draft 1.2

Prepared for

**Drug Enforcement Administration
Office of Diversion Control
600 Army Navy Drive
Arlington, Virginia 22202**

June 5, 2003

**Prepared by
PEC Solutions Inc.**

Table of Contents

	Page
Section 1—Introduction.....	1
1.1 Document Organization	1
Section 2— Requirements	2
2.1 Properties.....	2
2.2 Statement of Purpose.....	3
2.3 Policy Issues	3
2.4 Uniqueness of Names.....	3
Section 3— Certificate Profile.....	4
3.1 Basic Certificate Fields	4
3.1.1 Certificate Information.....	4
3.1.2 Issuer	4
3.1.3 Subject.....	5
3.2 Standard Certificate Extensions	5
3.2.1 Authority Key Identifier Extension.....	6
3.2.2 Subject Key Identifier Extension	6
3.2.3 Key Usage Extension	6
3.2.4 Certificate Policies Extension	7
3.2.5 Subject Alternative Name Extension	7
3.2.6 Basic Constraints Extension.....	7
3.2.7 CRL Distribution Points Extension.....	8
3.2.8 Authority Information Access Extension.....	8
3.2.9 Private Key Usage.....	8
3.3 DEA Diversion Control E-Commerce PKI Specific Extensions	8
3.3.1 DEA Certificate Version Number Information.....	9
3.3.2 DEA Registrant Name.....	9
3.3.3 DEA Registration Number	9
3.3.4 DEA Valid Schedules.....	10

Table of Contents

	Page
3.3.5 DEA Business Category.....	10
3.3.6 DEA Postal Address.....	11
3.3.7 Hashed DEA Registration Number– SHA-1.....	12
Section 4— CRL Profile.....	14
4.1 tbsCertList.....	14
4.1.1 Version.....	14
4.1.2 Signature.....	14
4.1.3 Issuer Name.....	14
4.1.4 This Update.....	14
4.1.5 Next Update.....	14
4.1.6 Revoked Certificates.....	15
4.1.7 Extensions.....	15
4.2 Signature Algorithm.....	16
4.3 Signature Value.....	16
Section 5— DEA Usage of CRL Revocation Codes.....	17
Overview of Business Case.....	17
5.2 Cause/Source for Revocation.....	18
5.3 Mapping Certificate Policy to Revocation Flags.....	19
5.4 Summary of Revocation Flag Usage.....	21
Section 6— Certificate Profile ASN.1.....	22
6.1 Certificate ASN.1.....	22
6.2 DEA Certificate Extensions ASN.1.....	22
6.3 CRL ASN.1.....	24
Appendix A — Document Acronyms.....	A-1
Appendix B— References.....	B-1
Appendix C- Certificate and CRL profile worksheet.....	C-1

Table of Figures

	Page
Figure 1. Profile Version Table.....	9
Figure 2. DEA Number Values.....	9
Figure 3. Controlled Substance Schedule Bits.....	10
Figure 4. DEA Business Activity Codes for CSOS/EPCS.....	11
Figure 5. Postal Address Example Values.....	12
Figure 6. Hashed DEA Registration Number Value.....	13
Figure 7. DEA Number Values.....	13
Figure 8. CRL Revocation Flags.....	18
Figure 9. Mapping Certificate Policy to Revocation Flags.....	19
Figure 10. Summary of Revocation Flag Usage.....	21
Figure 11. Summary of DEA Extensions.....	22

Section 1—Introduction

This document outlines the minimum information required for the Drug Enforcement Administration's (DEA) Diversion Control E-Commerce Public Key Infrastructure (PKI). It does not address the legal issues associated with the CSOS/EPCS PKI Architecture.

The profile is based on the Federal PKI (FPKI) X.509 Certificate and CRL Extensions Profile, and the Internet Engineering Task Force (IETF) Request For Comment (RFC) 3280, "X.509 Public Key Infrastructure (PKI) for the Internet". The DEA certificate profile complements the current FPKI certificate profile. This document in conjunction with the FPKI certificate profile and RFC 3280 define the format and semantics of X.509 v3 and CRL v2 for transmitting Controlled Substances orders and Electronic Prescriptions for Controlled Substances.

1.1 Document Organization

The requirements outlined in Section 2 and 3 represent current standards. These may change over time with the influence of new ideas and technologies. The remainder of this document is organized as follows:

Section 2— Section 2 describes the DEA Diversion Control E-Commerce PKI Certificate Profile requirements, security requirements, and analysis applied to the design of the CSOS/EPCS digital certificate. Entities being issued certificates covered by this profile include the CSOS Root CA, EPCS Subordinate CAs, and Subscribers. This section is a basic reference to the "X.509 Public Key Infrastructure Certificates Profile."

Section 3— Section 3 describes certificate requirements for the DEA Diversion Control E-Commerce PKI (CSOS/EPCS) model in specific detail. This section includes information that is vital to the organization of the DEA Diversion Control E-Commerce PKI (CSOS/EPCS) digital certificate architecture through defining technical certificate requirements.

Section 4— Section 4 describes the Certificate Revocation List (CRL) requirements for the DEA CSOS/EPCS model in specific detail. This section includes information necessary to help relying parties determine the validity of a DEA CSOS/EPCS certificate.

Section 5— Section 5 describes the DEA usage of Revocation Reason Codes, a non-critical Certificate Revocation List (CRL) entry extension that identifies the reason for the certificate revocation.

Section 6— Section 6 defines the Certificate and CRL profile ASN.1 syntax.

Appendix A— Appendix A defines a reference to document acronyms.

Appendix B— Appendix B lists the references used in this document as well as other documents that have led to the decisions made for the DEA CSOS/EPCS certificates.

Appendix C— Appendix C contains a Certificate and CRL profile worksheet, which has been adopted from the FPKI X.509 certificate and CRL Extensions profile (twg-02-04.xls).

Section 2— Requirements

The certificate profile defined in this document was built using US Federal PKI and industry standards. More generally, this profile describes the certificates to be used in an environment where a subscriber can be identified with a high level of assurance for electronic CSOS/EPCS transactions.

The mechanisms that decide whether a certificate should or should not be considered a CSOS/EPCS certificate with regard to legislation and Federal regulation are outside the scope of this document. The most important aspects that affect the scope of this specification are:

- Definition of names and identity information in order to identify the associated subject in a uniform way,
- Definition of CSOS/EPCS certificate management through the key usage extension,
- Definition of a standardized method to store predefined statements relevant to CSOS/EPCS certificates.

2.1 Properties

A CSOS/EPCS certificate defined in this standard is assumed to have the following properties:

- The Root CA makes a public statement defining the purpose of DEA Diversion Control E-Commerce PKI certificate, as discussed in Section 2.2.
- The Certificate indicates its *Certificate Policy* is consistent with liabilities, practices and procedures undertaken by the CA, as discussed in 2.3.
- A certificate is issued to a Root CA, EPCS Subordinate CAs, CSOS Subordinate CA, Registrant, and Powers of Attorney.
- The certificate contains an identity based on the legal name of the subject.

2.2 Statement of Purpose

For a certificate to serve as a CSOS/EPCS certificate, the issuing CA will include information identifying the governing Certificate Policy in the certificate that explicitly defines the intended certificate use. This information will assist subscriber and relying parties in evaluating the risk associated with creating or accepting signatures that are based on a CSOS/EPCS certificates.

The governing Certificate Policy shall be identified in the certificate using the certificate policies extension. The certificate policies extension shall include a registered OID and a user notice.

2.3 Policy Issues

Certain aspects outlined in the *DEA Diversion Control E-Commerce PKI Certificate Policy* define the context in which this profile is to be understood and used. It is outside the scope of this profile to specify any policies or legal aspects that will govern services that issue or utilize certificates according to this profile. The issuing CA must operate in accordance with the *CSOS/EPCS Certificate Policy*.

2.4 Uniqueness of Names

The Distinguished Name (DN) must be unique, during the lifetime of the CA, for each Subscriber.

Section 3— Certificate Profile

CSOS/EPCS certificates are standard X.509 certificates with special attributes added to support the electronic transmission of controlled substance prescriptions and orders (DEA 222).

3.1 Basic Certificate Fields

Basic certificate fields of the CSOS/EPCS certificates can be further divided into categories such as issuer DN, subject DN, validity, serial number, etc. Detailed descriptions of formats and accepted attributes can be found in section 5 and appendix C. Relying parties MAY have to consult associated certificate policies and/or the issuer's Certificate Practice Statement (CPS), in order to determine the semantics of name fields and the laws under which the issuer operates.

3.1.1 Certificate Information

The certificate must include the certificate X.509 version number, the certificate serial number, and the validity period. The certificate version number for all CSOS/EPCS certificates will be V3 to represent the X.509 V3 certificate type used. This number can be considered a unique identifier among associated certificates. The validity period consists of two sections that indicate how long a certificate is to be valid. The first section is called “notBefore” and represents the beginning point of the validity period. The second section is called “notAfter” and represents the ending point of the validity period.

3.1.2 Issuer

The issuer field is the identity of the organization responsible for issuing the certificate. The name of the issuing CA must be the officially registered organization name as applied to the DEA.

3.1.2.1 Distinguished Name

The identity of the DEA Diversion Control E-Commerce Root CA is defined as:

C=US, O=U.S. Government, OU=Department of Justice, OU=DEA, OU=Diversions Control, OU= E-Commerce, OU= E-Commerce Root, CN= E-Commerce Root CA

The identity of the CSOS CA is defined as:

C=US, O=U.S. Government, OU=Department of Justice, OU=DEA, OU=Diversions Control, OU= E-Commerce, OU=CSOS, OU=CSOS CA

EPCS subordinate CAs will be responsible for creating both their DN and the DN of the Subscriber. However, DEA requires the Subscriber DN to include the Common Name of the individual using the certificate and a serial number that is unique to the subscriber.

3.1.2.2 Signature

The signature of the issuing CA is the algorithm type used to sign the CSOS/EPCS certificates. The CSOS/EPCS CAs and Subscribers will require SHA-1 (FIPS 180-1) as the one-way hash function of choice for use with one of the FIPS 186-2 approved signature algorithms.

3.1.3 Subject

The subject field is the identity of the Subscriber who is being assigned the certificate from the issuing CA. In the CSOS/EPCS architecture, the subject can be one of the following participating parties: Root CA, Subordinate CA, or Subscriber. The Subscriber may be a Practitioner, Hospital, or others eligible subscribers as defined in Title 21 CFR Part 1300.

3.1.3.1 Distinguished Name

The identity of the subject must include certain predefined attributes according to organization.

The identity of the Root CA is defined as:

C=US, O=U.S. Government, OU=Department of Justice, OU=DEA, OU=Diversion Control, OU= E-Commerce, OU= E-Commerce Root, CN= E-Commerce Root CA

The identity of the CSOS CA is defined as:

C=US, O=U.S. Government, OU=Department of Justice, OU=DEA, OU=Diversion Control, OU= E-Commerce, OU=CSOS, OU=CSOS CA

The EPCS CA shall define their own DN and the subscriber must include the following attribute:

CommonName (Name of Registrant, Name of Power of Attorney, or Agent of Institution as defined by DEA Regulations)

SerialNumber

3.1.3.2 Signature Information

The subjectPublicKeyInfo is a basic parameter of the CSOS/EPCS certificate, used to describe the algorithm and public key of the subject. The Root CA, Subordinate CAs, and Subscribers will use a FIPS 186-2 approved signature algorithm with SHA-1 hashing.

3.2 Standard Certificate Extensions

Certificate extensions are the key attributes that allow CSOS/EPCS certificates to efficiently integrate new technology with present DEA regulations. The CSOS/EPCS certificate will include standard X.509 v3 extensions that have been defined in RFC 3280 in addition to additional extensions defined in this document. Making extensions mandatory or critical is addressed differently depending on the extension and how it is used with DEA applications.

3.2.1 Authority Key Identifier Extension

The Authority Key Identifier extension identifies the public key used to verify the signature on the certificate. The Authority Key Identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. Since the extension is considered to be an efficiency-enhancing certificate extension within FPKI standards, it is marked as required. This extension must be marked non-critical.

Root CA Certificate	This extension MUST be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension MUST be included

3.2.2 Subject Key Identifier Extension

The Subject Key Identifier extension identifies the public key being certified. It allows for differentiation of distinct keys used by the same subject. Since the extension is considered to be an efficiency-enhancing certificate, it is marked as required. This extension must be marked non-critical.

Root CA Certificate	This extension MUST be included with SHA-1 as hash identifier
Subordinate CA Certificate	This extension MUST be included with an standardized hash identifier
Subscriber Certificate	This extension MUST be included with SHA-1 as hash identifier

3.2.3 Key Usage Extension

The Key Usage extension serves to limit the technical purposes for which a public key listed in a valid certificate may be used. Subordinate CAs may issue certificates that contain a key usage extension limiting the keys to signing certificates, certificate revocation lists, and other data. This extension must be marked critical.

Root CA Certificate	This extension MUST be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension MUST be included

3.2.4 Certificate Policies Extension

The Certificate Policies extension lists the supporting CA Certificate Policy OID, as well as optional qualifier information pertaining to these policies. The qualifier is a method of adding text information directly into the certificate. The extension is processed by relying party applications during the certificate path validation process. This extension must be marked as non-critical.

Root CA Certificate	This extension MUST not be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension MUST be included

Subordinate CA certificates, Subscriber certificates shall include the user notice qualifier containing an explicit text notice.

3.2.5 Subject Alternative Name Extension

The Subject Alt Name extension provides a name that is bound by the Root-CA or CA to the subject's certified public key.

Root CA Certificate	This extension is OPTIONAL
Subordinate CA Certificate	This extension is OPTIONAL
Subscriber Certificate	This extension is OPTIONAL

3.2.6 Basic Constraints Extension

The Basic Constraints extension identifies whether or not the certificate belongs to a CA and how many entities the certification path permits through that CA. When pathLenConstraint does not appear, there is no limit to the allowed length of the certification path. This extension must be marked as critical.

Root CA Certificate	This extension MUST be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension is OPTIONAL

3.2.7 CRL Distribution Points Extension

The CRL Distribution Points extension identifies how the relying party obtains CRL information. CSOS/EPCS certificates can use LDAP URL, HTTP URL, or DN syntax to access CRL information. This extension must be marked as non-critical.

Root CA Certificate	This extension MUST NOT be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension MUST be included

3.2.8 Authority Information Access Extension

The Authority Information Access extension indicates how to access issuing CA information and services. Information and services may include on-line validation services and CA policy data. This extension must be marked as non-critical.

Root CA Certificate	The use of this extension is OPTIONAL
Subordinate CA Certificate	The use of this extension is OPTIONAL
Subscriber Certificate	The use of this extension is OPTIONAL

3.2.9 Private Key Usage

The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than the certificate.

Root CA Certificate	The use of this extension is OPTIONAL
Subordinate CA Certificate	The use of this extension is OPTIONAL
Subscriber Certificate	The use of this extension is OPTIONAL

3.3 DEA Diversion Control E-Commerce PKI Specific Extensions

The following extensions have been added to support DEA business requirements. These extensions **MUST** be included in Subscriber certificates and marked non-critical. Values for the DEA Diversion Control E-Commerce PKI (CSOS/EPCS) specific extensions should be consistent to the CSA database and the DEA Form 223.

3.3.1 DEA Certificate Version Number Information

The DEA Certificate Version Number Information extension allows relying party applications to identify the DEA profile version being used by the particular certificate. This enables multiple profile versions to be used at the same time without ambiguity. This profile is version 1.0 and has an integer value. (Example: 0 for version 01).

Version Number	Integer Value
1	0
2	1
3	2

Figure 1. Profile Version Table

3.3.2 DEA Registrant Name

The DEA Registrant Name extension is used to identify the DEA Registrant. The name must be consistent with the Controlled Substance Act (CSA) database Registrant Name and has a printable string format as it appears in the CSA database and the DEA Form 223. Example: *last name first name middle initial* (Doe, John A) or *business name* (Acme, Inc.).

3.3.3 DEA Registration Number

The DEA registration number extension is obsolete and is only provide here as a reference.

The DEA Registration Number extension is used to identify the assigned DEA Registrant number. The number must be consistent with the CSA database Registrant DEA number and has a printable string format (example, AB1234567).

Individuals that are exempt from registration must have a DEA registration number that is consistent with Title 21 Code of Federal Regulations Part 1300-1399.

For agents of an institution the DEA suffix must be consistent and validated with the current list of internal codes that is maintained by the hospital or institution that has permitted the (agent) individual to dispense, administer, or prescribe drugs within the jurisdiction.

Individual	Institution /Service	Suffix/ identification number	DEA Registration # Value
Jane Doe	AB1234567	JD213452345	AB1234567- JD213452345
John Smith	N/A	N/A	AB12345

Figure 2. DEA Number Values

3.3.4 DEA Valid Schedules

The *DEA Valid Schedule* extension reflects the schedules the certificate owner is authorized to order, distribute, prescribe or dispense. The format of information entered into this extension consists of a bit string value. The assertion of a bit indicates that the corresponding schedule has been authorized by the DEA. If the bit has not been asserted then the schedule has not been authorized. The table below provides a mapping of allowable schedules to bits in the DEA schedule extension.

Bit	Schedule
0	Schedule I Narcotic and Non-narcotic
1	Schedule II Narcotic
2	Schedule II Non-narcotic
3	Schedule III Narcotic
4	Schedule III Non-narcotic
5	Schedule IV
6	Schedule V
7	Unused

Figure 3. Controlled Substance Schedule Bits

A certificate that is issued to a person that is authorized to prescribe or order schedules II, IIIn, III, IIIIn, IV, V would have a bit string value of 01111110.

A listing of Schedules of Controlled Substances is provided in Title 21 Code of Federal Regulations Part 1300-1399.

3.3.5 DEA Business Category

The *DEA Business Category* extension identifies the business classification of the Subscriber. The category must be consistent with the CSA database Business Activity Code and have printable string format. The format of information entered into this extension consists of a sequence of alphanumeric information identifying the DEA business activity and the sub activity when present. The table below provides a listing of the codes that represent the allowable business activities for CSOS/EPCS.

Business Activity	Code	CSOS	EPCS
Pharmacy	A	A	
Hospital/Clinic	B	B	B
Practitioner	C	C	C
Teaching Institution	D	D	
Manufacturer	E	E	
Distributor	F	F	
Researcher	G	G	
Analytical Lab	H	H	
Exporter	K	K	
Mid-Level Practitioner	M	M	M
Narcotic Treatment Programs			
Maintenance	N	N	
Detoxification	P	P	
Maintenance & Detoxification	R	R	
Compounder/Maintenance	S	S	
Compounder/Detoxification	T	T	
Compounder/Maint. & Detox.	U	U	

Figure 4. DEA Business Activity Codes for CSOS/EPCS

3.3.6 DEA Postal Address

The *DEA postal address* extension identifies the postal address associated with the registrant, as indicated in DEA Form 223 (DEA certificate of registration). The DEA postal address is consistent with the postal address extension syntax definition defined by RFC 2252. The values entered into the postal address extension must be consistent with the current values held in the CSA database. The value will be a UTF8 string format delimited by a dollar sign for each value held in the respective address fields of the CSA database. The CSA database fields that represent the postal address are:

- Address 1
- Address 2
- Address 3
- City
- State
- Zip Code

The resulting extension value takes the format of: Address 1\$Address 2\$Address 3\$City\$State\$Zip Code. If a CSA database field value is not present it is omitted while leaving the delimiter fields. Example:

CSA Database Field	CSA Database value
Example 1	
Address 1	Dept 1
Address 2	123 Main Street
Address 3	PO Box 45678
City	Home Town
State	MD
Zip Code	12345-6789
Extension Value	Dept 1\$123 Main Street\$PO Box 45678\$Home Town\$MD\$12345-6789
Example 2	
Address 1	123 Main Street
Address 2	
Address 3	
City	Home Town
State	MD
Zip Code	12345-6789
Extension Value	123 Main Street \$\$\$Home Town\$MD\$12345-6789

Figure 5. Postal Address Example Values

3.3.7 Hashed DEA Registration Number– SHA-1

The extension *Hashed DEA Registration Number– SHA-1* is pending registration with the Computer Security Objects Register (CSOR) operated by the National Institute of Standards and Technology. Therefore, DEA is awaiting final OID assignment from the CSOR.

The Hashed DEA Registration Number extension is used to identify the assigned DEA Registrant number and has an octet string format. This extension obsoletes the DEA registration number extension.

```
(id-dea-RegNumber OBJECT IDENTIFIER ::= { id-dea 3 })
```

The DEA number must be protected within the public certificate to provide strong safeguards against the risk that the DEA registrant's DEA number could be "stolen" or misused when used for purposes other than controlled substance transactions.

Where a DEA number is required in the transaction, the certificate holder can include it in the transaction being signed. The relying party can hash the DEA registration number provided in the transaction and compare the resulting value with the hash value present in the public certificate, thus verifying that the DEA registration number in the transaction is valid—without the plain-text DEA registration number being present in the digital certificate. If no DEA number is required, the certificate holder simply does not include

the number in the transaction and the recipient cannot determine the number from the information contained in the certificate.

A hash value of the DEA registration number must be placed in the public certificate rather than the plain text DEA registration number. The hash value **MUST** be generated using a NIST approved and publicly available one-way hash function. This one way hash function produces a fixed length output that has the following properties: 1) it is computationally infeasible to recreate the input message (DEA registration number) from the hash value, and 2) it is computationally infeasible to construct two different input messages that produce the same output hash value.

The hash value is a function of the respective text values of the DEA registration number concatenated with the serial number attribute value of X.500 distinguished name (DN) contained in the subject name field of the corresponding public certificate using the SHA-1 hash algorithm. The SHA-1 hash implementation must be conformant to FIPS 180-2. The below figure provides an example value of the SHA-1 hashed DEA registration number.

Hash_ValueSHA1=(DEA_Num, Serial_number)	
DEA_Num =	AB1234567
Subject DN=	cn=John Doe+serialNumber=100011,ou=MD,ou=CSOS, ou=E-Commerce,ou=Office of Diversion Control, ou=DEA, ou=DOJ,o=U.S. Government,c=us
Serial number attribute of the subject DN	100011
Concatenated DEA_Num serial number	AB1234567100011
Hash_ValueSHA1=	500addcbc793cc029f8132ffa27b2d1cbf865d45

Figure 6. Hashed DEA Registration Number Value

The DEA number must be consistent with the CSA database Registrant DEA number (AB1234567).

Individuals that are exempt from registration must have a DEA registration number that is consistent with Title 21 Code of Federal Regulations Part 1300-1399.

For agents of an institution, the DEA suffix must be consistent and validated with the current list of internal codes that is maintained by the hospital or institution that has permitted the (agent) individual to dispense, administer, or prescribe drugs within the jurisdiction.

Individual	Institution /Service	Suffix/ identification number	DEA Registration # Value
Jane Doe	AB1234567	JD213452345	AB1234567- JD213452345
John Smith	N/A	N/A	AB12345

Figure 7. DEA Number Values

Section 4— CRL Profile

A Certificate Revocation List (CRL) will be made available to all relying parties. A CRL is a list of all revoked certificates of both End Entities and Certificate Authorities and is composed of a sequence of required field information that describes the CRL, revoked certificates, and the periods a CRL will be updated.

4.1 tbsCertList

The first field in the sequence is the tbsCertList or “to be signed certificate list.” This field is itself a sequence containing the name of the issuer, issue date, issue date of the next list, the list of revoked certificates, and CRL extensions. Furthermore, each entry on the revoked certificate list is defined by a sequence consisting of certificate serial number, revocation date, and optional CRL entry extensions.

4.1.1 Version

The version field describes the version number of the encoded CRL. Since extensions are duplicative as required by this profile, this field **MUST** be present and **MUST** specify version 2 (the integer value is 1).

4.1.2 Signature

The signature field contains the algorithm identifier for the algorithm used to sign the CRL. This field **MUST** contain the same algorithm identifier as the signatureAlgorithm field in the sequence CertificateList (section 4.2).

4.1.3 Issuer Name

The issuer name field identifies the entity that has signed and issued the CRL. The issuer identity is contained in the issuer name field. The issuer name field **MUST** contain an X.500 distinguished name (DN). The issuer name field is defined as the X.501 type Name, and **MUST** follow the encoding rules for the issuer name field in the certificate.

4.1.4 This Update

The “this update” field indicates the issue date of the CRL. Certificate Authorities conforming to this profile **MUST** encode thisUpdate as UTCTime for dates through the year 2049. Where encoded as UTCTime, thisUpdate **MUST** be specified and interpreted as defined in Certificate and CRL Profile Worksheet provided in the *appendix C*.

4.1.5 Next Update

The “next update” field indicates the date by which the next CRL will be issued. The next CRL could be issued before the indicated date, but it will not be issued any later than the indicated date. This profile requires inclusion of nextUpdate in all CRLs issued by conforming Certificate Authorities. A CA conforming to this profile must encode nextUpdate as UTCTime for dates through the year 2049. Where encoded as UTCTime,

nextUpdate must be specified and interpreted as defined in Certificate and CRL Profile Worksheet, *appendix C*.

4.1.6 Revoked Certificates

The revoked certificates field is comprised of a list of all certificates a Certificate Authority has revoked. The certificate serial number and the date on which the revocation occurred uniquely identify revoked certificates. The time for Revocation Date **MUST** be expressed as described in section 4.1.4.

4.1.7 Extensions

The X.509 v2 CRL format also allows communities to define private extensions to carry information unique to those communities. Each extension in a CRL may be designated as critical or non-critical.

4.1.7.1 Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL. The identification can be based on the key identifier (the subject key identifier in the CRL signer's certificate) or on the issuer's name and certificate serial number. This extension is especially useful when an issuer has more than one signing key, either due to multiple concurrent key pairs or due to changeover. Conforming Certificate Authorities **MUST** use the key identifier method, and **SHOULD** include this extension in all CRLs issued.

4.1.7.2 CRL Number

The CRL number is a non-critical CRL extension. It is used to convey a monotonically increasing sequence number for each CRL issued by a CA. This extension allows users to easily determine when a particular CRL supersedes another CRL. A CA conforming to this profile **SHOULD** include this extension in all CRLs.

4.1.7.3 Delta CRL Indicator

The delta CRL indicator is a critical CRL extension that identifies a delta-CRL. The use of delta-CRLs can significantly improve processing time for applications that store revocation information in a format other than the industry standard CRL structure. This allows changes to be added to the local database while ignoring unchanged information that is already in the local database. This extension is **OPTIONAL**.

4.1.7.4 Issuing Distribution Point

The issuing distribution point is a critical CRL extension that identifies whether the certificate revocation list is for end-entity certificates, CA certificates, or contains a limited set of reason codes. CA conforming to this profile **SHOULD** include this extension in all CRLs.

4.2 Signature Algorithm

The signature algorithm field contains the algorithm identifier for the algorithm used by the CA to sign the CertificateList. The field is of type AlgorithmIdentifier, which is defined in the Certificate Profile as being a FIPS 186-2 approved algorithm.

4.3 Signature Value

The signature value field contains a digital signature computed upon the ASN.1 DER encoded tbsCertList. The ASN.1 DER encoded tbsCertList is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the CRLs signature value field.

Section 5— DEA Usage of CRL Revocation Codes

This section defines the revocation reason codes that are associated with every CSOS/EPCS X.509 certificate placed on the CRL.

Overview of Business Case

Once a digital certificate is placed on a Certificate Revocation List (CRL) there needs to be way to indicate to a relying party the reason for the certificate being placed on the CRL.

The revocation reason is meaningful to the business process of the relying party. If the revocation is the result of an action taken by DEA it could be used as an indicator to the relying party that all transactions (electronic and paper) may be suspect. For example if the purchaser's DEA number has been revoked, then CSOS relying parties' action would be to not honor the order and to stop any pending order that may be in the process of being shipped. However if the Certificate is revoked as a result of a change in Power of Attorney, All orders associated with that DEA number would not have to be terminated as a in the previous example.

The revocation reason is conveyed by the use of a revocation flag that is associated with every certificate placed on the CRL. The Internet Engineering Task Force (IETF) Public Key Infrastructure (PKIX) group has defined draft standards that define a set of revocation flags that should be used by PKIs interoperating over the Internet.

The following bullets summarize the issue.

- Differentiate and map revocation reasons to business cases. The revocation reasons that have been defined by PKIX do not clearly map to all the CSOS business cases. As a result, industry Pilot participants have asked for clear mapping and an explanation of how the revocation codes will be used.
- Provide a reason code that could be used to trigger or map to a business process flow in the paper process when encountering a revoked digital certificate. Industry had asked whether the relying party must take action in the paper world as a result of information obtained through a CSOS CRL? This question arises when encountering dual paper and electronic orders/prescriptions. If the certificate used to sign an electronic order/prescription is revoked as a result of DEA action at the time of validation, then a flag/trigger should be raised to invalidate any paper orders/prescriptions that may also have been received. A fatal DEA action is an action that would result in the termination of a registrant's authority to order/prescribe. This reason flag however would not overrule the use of sound judgment by a pharmacist in evaluating the validity of the prescription on a prescription-by-prescription basis.
- Identify unique reason code(s) that would alert the relying party of a registrant's loss of DEA registration (Would also be relevant to POA certificates).

5.2 Cause/Source for Revocation

To map revocation reason flags to business cases all parties that initiate a revocation request must be identified. A revocation request can be made by the following four entities.

- **DEA**— The revocation request is initiated as a result of DEA action against a registrant.
- **Subscriber**— The revocation is requested . by the Subscriber.
- **DEA Registrant/Grantor**— The revocation is requested by the DEA registrant.
- **CA-Directed** .— The revocation is requested by the CA.

The below figure lists the nine standard revocation flags that are defined by PKIX. The second column indicates if the reason flag is used. The third column indicates the entity requesting/authoritative for the revocation.

Reason Flag	Used by	Used by Cause/Source
Unused	x	N/A
Key Compromise	✓	Grantor/Subscriber/PMA/DEA
CA Compromise	✓	DEA/PMA/CA
Affiliation Changed	✓	Grantor/Subscriber/PMA/DEA
Superseded	✓	DEA
Cessation Of Operation	✓	DEA
Certificate Hold	✓	DEA/Subscriber
Privilege Withdrawn	x	N/A
AA Compromise	x	N/A

Figure 8. CRL Revocation Flags

5.3 Mapping Certificate Policy to Revocation Flags

This section provides a description of revocation flag usage with respect to revocation business cases and Certificate policy (CP) provisions. The below figure list business cases and CP circumstances that cause a digital certificate to be revoked to a PKIX revocation flag.

Business Case	CP Circumstances	Revocation Code	Cause/Source
Change of subscriber/POA Name <ul style="list-style-type: none"> Termination of employment or POA 	Identifying information or affiliation components of any names in the certificate become invalid	Affiliation Changed	Registrant Subscriber
Change of Registrant Name <ul style="list-style-type: none"> Due to marriage or other legal name change 	Identifying information or affiliation components of any names in the certificate become invalid	Affiliation Changed	DEA
Change of DEA extensions <ul style="list-style-type: none"> Address change, Schedule change 	Privilege attributes asserted in the subscriber's certificate are reduced	Affiliation Changed	DEA
Compromise of Key <ul style="list-style-type: none"> Know theft of Token or storage media of private key 	The private key is lost or compromise is suspected	Key Compromise	Registrant Subscriber
Lose or forgotten Password	The private key is lost or compromise is suspected	Superseded	Registrant Subscriber
Self revocation or termination. <ul style="list-style-type: none"> No longer performing Electronic transactions 	The subscriber or other authorized party (as defined in the CA's CPS) asks for his/her certificate to be revoked	Affiliation Changed	Registrant Subscriber
Unauthenticated Revocation request	unauthenticated Revocation request	Certificate Hold	CA
Subscriber Agreement violation <ul style="list-style-type: none"> Access to the private key has been shared *no paper equivalent	It can be demonstrated that the subscriber has violated the stipulation of the Subscriber Agreement	Key Compromise	Sub CA

Figure 9. Mapping Certificate Policy to Revocation Flags

The following paragraphs summarize the revocation flag mapping listed above.

Change of DEA extensions—If a schedule change has been made for a non-prejudicial reason then the reason flag for revocation should be affiliation change. This could occur in two different ways:

- 1) The registrant desires to have a subset of schedules in the certificate because of State Law and regulations. The State Law or regulation may be more restrictive than the DEA regulation and therefore not allow for the electronic transmission of electronic orders/prescriptions.
- 2) The registrant does not want to permit a POA or agent to have the full range of allowable schedules electronically.

Subscriber Agreement violation—EPCS subordinate CAs have the ability to establish subscriber agreements that provide the EPCS subordinate CA the discretion to revoke a subscriber's digital certificate in the event that a subscriber agreement is violated.

Loss, forgotten password, key compromise—The key compromise flag will denote when there is suspension of a compromise or loss of control of the private key. An example would be the know theft of a token or the know theft or intrusion of the information system protecting the private key. An intrusion on the information system would be the discovery of a virus or other malicious code on the computer of the subscriber that could threaten the security of the private key. In the event of a forgotten password or a loss token the certificate will be revoked with a reason flag as superseded.

5.4 Summary of Revocation Flag Usage

This section provides an overall summary of revocation flag usage. The below figure summarizes the result of the revocation flag with the cases for using the revocation flag.

Revocation Flag	Case for using
Key compromise	Lose or compromise of key. Damaged Token Subscriber Agreement violation (only by EPCS Sub CAs this action will not be initiated by DEA. Access to the private key has been shared
Affiliation Change	Change of subscriber/POA Name Termination of employment or POA Change of Registrant Name Due to marriage or other legal name change Non-prejudicial change of DEA extensions Address change, Schedule change Self-revocation or termination. No longer performing Electronic transactions
Superseded	DEA registration Restricted for Cause
Cessation Of Operation	Used for to indicate if a revocation is a result of loss of the registrants DEA number. DEA registration Surrendered for Cause, Revoked, Out of Business, or Suspended
Certificate Hold	Unauthenticated Revocation request

Figure 10. Summary of Revocation Flag Usage

Section 6— Certificate Profile ASN.1

This section defines the Abstract Syntax Notations (ASN.1) for DEA Diversion Control E-Commerce PKI X.509 certificates.

6.1 Certificate ASN.1

The following RFCs should be referenced for the ASN.1 syntax that describes the certificate data objects.

Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

Bassham, L, Housley, R., Polk, W, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, April 2002.

Santesson, S, Polk, W, Barzin, P, Nystrom, M, "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", RFC 3039, January 2001.

6.2 DEA Certificate Extensions ASN.1

The following private extensions have been registered with the Computer Security Objects Register (CSOR) operated by the National Institute of Standards and Technology. The table below provides a summary of the ASN.1 structures for the DEA extensions.

Extension	OID id-dea {2 16 840 1 101 3 5}
Certificate version number	{ id-dea 1 }
RegistrantName	{ id-dea 2 }
RegNumber	{ id-dea 3 }
Schedules	{ id-dea 4 }
BcRole	{ id-dea 5 }
PostalAddress	{ id-dea 6 }
RegNumSHA1	{id-dea 7}

Figure 11. Summary of DEA Extensions

```
DEA-EXT DEFINITIONS ::=
BEGIN -- EXPLICIT TAGS

id-dea OBJECT IDENTIFIER ::= { 2 16 840 1 101 3 5 }

id-dea-CertVerInfo OBJECT IDENTIFIER ::= { id-dea 1 }
CertVerInfo ::= INTEGER { v0-1(0), v0-2 (1), v0-3(2) }

id-dea-RegistrantName OBJECT IDENTIFIER ::= { id-dea 2 }
RegistrantName ::= PrintableString

id-dea-RegNumber OBJECT IDENTIFIER ::= { id-dea 3 }
RegNumber ::= PrintableString

id-dea-Schedules OBJECT IDENTIFIER ::= { id-dea 4 }

Schedules ::= BIT STRING {
    schedule1    ( 0 ), -- Schedule I Narcotic and Non-narcotic
    schedule2    ( 1 ), -- Schedule II Narcotic
    schedule2n   ( 2 ), -- Schedule II Non-narcotic
    schedule3    ( 3 ), -- Schedule III Narcotic
    schedule3n   ( 4 ), -- Schedule III Non-narcotic
    schedule4    ( 5 ), -- Schedule IV
    schedule5    ( 6 )  -- Schedule V
}
id-dea-bcRole OBJECT IDENTIFIER ::= { id-dea 5 }

-- this is limited to one major role, zero or one minor roles
BcRole ::= SEQUENCE {
    majorRole    PrintableString, -- contains CSA code
                                     -- ex: for "Pharmacy" contents are "A"
    subRole      PrintableString OPTIONAL -- future use
                                     -- will contain CSA sub-codes once defined
}

id-dea-postalAddress OBJECT IDENTIFIER ::= { id-dea 6 }
Dea-postalAddress ::= UTF8String -- contains address fields as a single
string
                                     -- each line of the address is delimited by a '$'

id-dea-RegNumSHA1 OBJECT IDENTIFIER ::= { id-dea 7 }
RegNumSHA1 ::= OCTET STRING

END
```

6.3 CRL ASN.1

The following RFCs should be referenced for the ASN.1 syntax that describes the CRL data objects.

Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

Appendix A — Document Acronyms

CA	Certificate 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
DEA	Drug Enforcement Administration
DN	Distinguished Name
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards & Technology
PEC	Performance Engineering Corporation
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, & Adleman

Rx	Prescription
TCP/IP	Transmission Control Protocol / Internet Protocol
UID	Unique Identifier
X.500	The standard for directory services
X.509	The standard for PKI certificates

Appendix B— References

- [CONOPS] *Controlled Substances Ordering System Concept of Operations*, Drug Enforcement Administration, October 13, 2000
- [CONOPS] *Electronic Prescriptions for Controlled Substances Concept of Operations*, Drug Enforcement Administration, September 1, 2000
- [CSOSCP] *Controlled Substances Ordering System Certificate Policy*, Drug Enforcement Administration, Draft Revision 4, October 2001
- [EPCSCP] *Electronic Prescriptions for Controlled Substances Certificate Policy PKI Draft Revision 3*, Drug Enforcement Administration, October 31, 2001
- [RFC3039] *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*, Internet Draft <draft-ietf-pkix-qc-06.txt>, January 2001
- [RFC3279] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
- [RFC3280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
- [RFC2459] *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, Network Working Group, January 1999
- [DRAFT] *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, Network Working Group, January 2002
- [ITU-T] *X.680: Information Technology - Abstract Syntax Notation One*, X.680 ITU-T Recommendation, 1997.
- [RFC822] “*Standard for the format of ARPA Internet text messages*”, Crocker, D., STD 11, RFC 822, August 1982.
- [FPKI] *Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile*, FPKI twg-00-18, April 18, 2000
- [XLS] *ICSA’s PKIX Certificate Profile*, Robert Moskowitz, September 6, 1999
- [ASTMCP] Standard Certificate Policy for Healthcare PKI, ASTM 31.20, April 2, 200

E-Commerce Root Certificate

Name	Critical Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be Signed
version		2	Version 3
serial number			
certificateSerialNumber			Unique within the CA
signature			
algorithmIdentifier			Must match Algorithm Identifier in Signature Algorithm field
algorithm		1.2.840.113549.1.1.5 (for RSA/SHA-1)	SHA-1 with RSAEncryption
parameters		NULL	Only populate when using SHA-1 WithRSAEncryption
issuer			X.501 type DN of CA which created the Certificate
Name			Name of Root CA issuing Certificate
RDNSequene			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		(2.5.4.6)	id-at-countryName C=Country Name
AttributeValue		"US"	
AttributeTypeAndValue			
AttributeType		(2.5.4.10)	id-at-organizationName O=Organization Name
AttributeValue		"U.S. Government"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Department of Justice"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"DEA"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Diversion Control"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"E-Commerce"	
AttributeTypeAndValue			
AttributeType		(2.5.4.3)	id-at-commonName CN=Common Name
AttributeValue		"E-Commerce Root CA"	
validity			Validity period of Certificates
noBefore			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
noAfter			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
subject			
Name			Name of Root CA issuing Certificate
RDNSequene			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		(2.5.4.6)	id-at-countryName C=Country Name
AttributeValue		"US"	
AttributeTypeAndValue			
AttributeType		(2.5.4.10)	id-at-organizationName O=Organization Name
AttributeValue		"U.S. Government"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Department of Justice"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"DEA"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Diversion Control"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit

AttributeValue		"E-Commerce"	
AttributeTypeAndValue			
AttributeType		(2.5.4.3)	id-at-commonName CN=Common Name
AttributeValue		"E-Commerce Root CA"	
subjectPublicKeyInfo			Public Key for this Certificate
algorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.1 (RSA)	Must contain same algorithm identifier as the signatureAlgorithm field in the signatureAlgorithm outside the certificate (used to sign the certificate).
parameters			For RSA include NULL; for DSA and ECDSA include parameters if subject and issuer have different parameters. If parameters are inherited, omit field for DSA and include NULL for ECDSA.
subjectPublicKey		BIT STRING	Subjects Public Key Bit String
extensions			Required Version 3 Certificates
AuthorityKeyIdentifier	FALSE		
KeyIdentifier		SHA-1 hash	SHA-1 Hash for Authority Public Key
SubjectKeyIdentifier	FALSE		
KeyIdentifier		SHA-1 hash	SHA-1 Hash for subjects Public Key
KeyUsage	TRUE	BIT STRING	Restricts how keys may be used
digitalSignature		1	for entity authentication or data origin integrity/authentication only
nonRepudiation		1	for verification of digital signatures
keyEncipherment		1	if public key is used for key transport
dataEncryption		1	encrypting user data
keyAgreement		1	public key used key agreement (e.g., D-H)
keyCertSign		1	Certificate signing. Always Asserted in CA certificates.
cRLSign		1	Revocation List signing. Asserted if this key is also used to sign CRLs
encipherOnly		0	if keyAgreement bit is on, this can only be used to encrypt data during key agreement.
decipherOnly		0	if keyAgreement bit is on, this can only be used to decrypt data during key agreement.
certificatePolicies	FALSE	not used	Indicate the policies under which the certificate has been issued. Applications with policy requirements are expected to be able to process this extension
PolicyInformation			
policyIdentifier			
policyQualifiers			
qualifier			
UserNotice			UserNotice should only appear in EE or CA certs issued to other organizations to prevent multiple duplicate displays.
policyMappings	FALSE		Maps policies of one CA to that of another in cross certificates
issuerDomainPolicy			
subjectDomainPolicy			
BasicConstraints	TRUE		Identifies whether subject is a CA
cA		TRUE	
pathLenConstraint		INTEGER	The use of a path length constraint is optional.
NameConstraints	TRUE		Limit security domain of Root-CA
PolicyConstraints	TRUE		Can be used to prohibit or limit policy mapping
cRLDistributionPoints	FALSE		This extension is required in all CA certificates
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
UniformResourceIdentifier		"ldap://url"	
cRLIssuer			Defaults to CA. If not different, there is no reason to use this extension.
AuthorityInfoAccessSyntax	FALSE		Only used for non-CRL revocation methods.
AccessDescription			
accessMethod		id-ad-ocsp, id-ad-calssuers	See RFC 2560 for use of id-ad-ocsp for OCSF responders
accessLocation			For id-ad-calssuers, this MUST be a URI if the information is available via http, ftp, or ldap.
GeneralName			
rfc822Name		IA5String	Required if information is available via e-mail
uniformResourceIdentifier		IA5String	URI required if information is available by http, ldap, or ftp
IPAddress		OCTET STRING	

EPCS Subordinate CA Certificate

Name	Critical Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be Signed
version		2	Version 3
serial number			
certificateSerialNumber			Unique within the CA
signature			
algorithmIdentifier			Must match Algorithm Identifier in Signature Algorithm
algorithm		1.2.840.113549.1.1.5 (for RSA/SHA-1) 1.2.840.10040.4.3 (for DSA/SHA-1) 1.2.840.10045.1 (ECDSA/SHA-1)	Choice of following three algorithms. SHA-1 with RSAEncryption DSA with SHA-1 ECDSA with SHA-1
parameters		NULL	Only populate when using SHA-1 WithRSAEncryption
issuer			X.501 type DN of CA which created the Certificate
Name			Name of Root CA issuing Certificate
RDNSequene			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		(2.5.4.6)	id-at-countryName C=Country Name
AttributeValue		"US"	
AttributeTypeAndValue			
AttributeType		(2.5.4.10)	id-at-organizationName O=Organization Name
AttributeValue		"U.S. Government"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Department of Justice"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"DEA"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Diversion Control"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"E-Commerce"	
AttributeTypeAndValue			
AttributeType		(2.5.4.3)	id-at-commonName CN=Common Name
AttributeValue		"E-Commerce Root CA"	
validity			Validity period of Certificates
notBefore			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
notAfter			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
subject			
Name			
RDNSequene			C= ; O= ; OU=-CN= & DC= are recommended
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		(2.5.4.6)	id-at-countryName C=Country Name
AttributeValue			
subjectPublicKeyInfo			Public Key for this Certificate
algorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10040.4.1	Digital Signature Algorithm
		1.2.840.10045.2.1	Elliptic Curve Algorithms

parameters		See comment	For RSA include NULL; for DSA and ECDSA include parameters if subject and issuer have different parameters. If parameters are inherited, omit field for DSA and include NULL for ECDSA.
subjectPublicKey		BIT STRING	Subjects Public Key Bit String
extensions			Required Version 3 Certificates
AuthorityKeyIdentifier	FALSE		
KeyIdentifier		SHA-1 hash	Derived using the SHA-1 hash of the public key.
SubjectKeyIdentifier	FALSE		
KeyIdentifier		OCTET STRING	Match the authority key identifier included in certificates and CRLs signed by the subject with this public key.
KeyUsage	TRUE	BIT STRING	Restricts how keys may be used
digitalSignature		1	for entity authentication or data origin integrity/authentication only
nonRepudiation		1	for verification of digital signatures
keyEncipherment		1	if public key is used for key transport
dataEncryption		1	encrypting user data
keyAgreement		1	public key used key agreement (e.g., D-H)
keyCertSign		1	Certificate signing. Always Asserted in CA certificates.
cRLSign		1	Revocation List signing. Asserted if this key is also used to sign CRLs
encipherOnly		0	if keyAgreement bit is on, this can only be used to encrypt data during key agreement.
decipherOnly		0	if keyAgreement bit is on, this can only be used to decrypt data during key agreement.
certificatePolicies	FALSE		A CRL issuer certificates should not include policy qualifiers.
PolicyInformation			
policyIdentifier		2.16.840.1.101.3.2.1.9.2	
policyQualifiers			
qualifier			
UserNotice		This is a DEA EPCS Digital Certificate. It is Specifically intended for use in signing controlled substance prescriptions - any other signing uses are at the discretion of the certificate holder.	UserNotice should only appear in EE or CA certs issued to other organizations to prevent multiple duplicate displays.
subjectAltName	FALSE		This extension is optional.
issuerAltName	FALSE		This extension is optional.
cRLDistributionPoints	FALSE		If not used, then all CRLs MUST be issued by the CA that issued the certificate
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
UniformResourceIdentifier		"ldap://uri"	RFC 1738
cRLIssuer			Defaults to CA. If not different, there is no reason to use this extension.
AuthorityInfoAccess	FALSE		Only used for non-CRL revocation methods.
AccessDescription			
accessMethod		id-ad-ocsp, id-ad-calssuers	See RFC 2560 for use of id-ad-ocsp for OCSP responders
accessLocation			For id-ad-calssuers, this MUST be a URI if the information is available via http, ftp, or ldap.
GeneralName			
rfc822Name		IA5String	Required if information is available via e-mail
uniformResourceIdentifier		IA5String	URI required if information is available by http, ldap, or ftp
IPAddress		OCTET STRING	

CSOS CA Certificate

Name	Critical Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be Signed
version		2	Version 3
serial number			
certificateSerialNumber			Unique within the CA
signature			
algorithmIdentifier			Must match Algorithm Identifier in Signature Algorithm
algorithm		1.2.840.113549.1.1.5	SHA-1 with RSAEncryption
parameters		NULL	Only populate when using SHA-1 WithRSAEncryption
issuer			X.501 type DN of CA which created the Certificate
Name			Name of Root CA issuing Certificate
RDNSquence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		(2.5.4.6)	id-at-countryName C=Country Name
AttributeValue		"US"	
AttributeTypeAndValue			
AttributeType		(2.5.4.10)	id-at-organizationName O=Organization Name
AttributeValue		"U.S. Government"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Department of Justice"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"DEA"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Diversion Control"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"E-Commerce"	
AttributeTypeAndValue			
AttributeType		(2.5.4.3)	id-at-commonName CN=Common Name
AttributeValue		"E-Commerce Root CA"	
validity			Validity period of Certificates
notBefore			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
notAfter			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
subject			
issuer			X.501 type DN of CA which created the Certificate
Name			Name of CSOS CA issuing Certificate
RDNSquence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		(2.5.4.6)	id-at-countryName C=Country Name
AttributeValue		"US"	
AttributeTypeAndValue			
AttributeType		(2.5.4.10)	id-at-organizationName O=Organization Name
AttributeValue		"U.S. Government"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Department of Justice"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit

AttributeValue		"DEA"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"Diversion Control"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"E-Commerce"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"CSOS"	
AttributeTypeAndValue			
AttributeType		(2.5.4.11)	id-at-organizationalUnitName OU=OrganizationalUnit
AttributeValue		"CSOS CA"	
subjectPublicKeyInfo			Public Key for this Certificate
algorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.1	RSA Encryption
parameters		See comment	For RSA include NULL; for DSA and ECDSA include parameters if subject and issuer have different parameters. If parameters are inherited, omit field for DSA and include NULL for ECDSA.
subjectPublicKey		BIT STRING	Subjects Public Key Bit String
extensions			Required Version 3 Certificates
AuthorityKeyIdentifier	FALSE		
KeyIdentifier		SHA-1 hash	Derived using the SHA-1 hash of the public key.
SubjectKeyIdentifier	FALSE		
KeyIdentifier		OCTET STRING	Match the authority key identifier included in certificates and CRLs signed by the subject with this public key.
KeyUsage	TRUE	BIT STRING	Restricts how keys may be used
digitalSignature		1	for entity authentication or data origin integrity/authentication only
nonRepudiation		1	for verification of digital signatures
keyEncipherment		1	if public key is used for key transport
dataEncryption		1	encrypting user data
keyAgreement		1	public key used key agreement (e.g., D-H)
keyCertSign		1	Certificate signing. Always Asserted in CA certificates.
cRLSign		1	Revocation List signing. Asserted if this key is also used to sign CRLs
encipherOnly		0	if keyAgreement bit is on, this can only be used to encrypt data during key agreement.
decipherOnly		0	if keyAgreement bit is on, this can only be used to decrypt data during key agreement.
certificatePolicies	FALSE		A CRL issuer certificates should not include policy qualifiers.
PolicyInformation			
policyIdentifier		2.16.840.1.101.3.2.1.9.1	
policyQualifiers			
qualifier			
UserNotice		This is a DEA CSOS Digital Certificate. It is Specifically intended for use in signing controlled substance orders - any other signing uses are at the discretion of the certificate holder.	UserNotice should only appear in EE or CA certs issued to other organizations to prevent multiple duplicate displays.
subjectAltName	FALSE		This extension is optional.
issuerAltName	FALSE		This extension is optional.
cRLDistributionPoints	FALSE		If not used, then all CRLs MUST be issued by the CA that issued the certificate
DistributionPoint			
distributionPoint			

DistributionPointName			
fullName			
GeneralNames			
UniformResourceIdentifier		"ldap://uri"	RFC 1738
cRLIssuer			Defaults to CA. If not different, there is no reason to use this extension.
AuthorityInfoAccess	FALSE		Only used for non-CRL revocation methods.
AccessDescription			
accessMethod		id-ad-ocsp, id-ad-calssuers	See RFC 2560 for use of id-ad-ocsp for OCSP responders
accessLocation			For id-ad-calssuers, this MUST be a URI if the information is available via http, ftp, or ldap.
GeneralName			
rfc822Name		IA5String	Required if information is available via e-mail
uniformResourceIdentifier		IA5String	URI required if information is available by http, ldap, or ftp
IPAddress		OCTET STRING	

EPCS/CSOS Subscriber Certificates

Name	Critical Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be Signed
version		2	Version 3
serial number			
certificateSerialNumber			Unique within the CA
signature			
algorithmIdentifier			Must match Algorithm Identifier in Signature Algorithm
algorithm		1.2.840.113549.1.1.5 (for RSA/SHA-1) 1.2.840.10040.4.3 (for DSA/SHA-1) 1.2.840.10045.1 (ECDSA/SHA-1)	Choice of following three algorithms. SHA-1 with RSAEncryption DSA with SHA-1 ECDSA with SHA-1
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
		1.2.840.10040.4.3	id-dsa-with-sha-1
		1.2.840.10045.4.1	ecdsa-with-SHA1
parameters		NULL	Only populate when using SHA-1 WithRSAEncryption
issuer			
Name			This is the DN of the subject of the CA that created the certificate. See CSOS CA and EPCS sub CA profiles.
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType			
AttributeValue			
validity			
notBefore			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
notAfter			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
subject			X.500 DN of subject for whom the Certificate was created
Name			Name of certificate holder.
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType			
AttributeValue			see main text on naming
subjectPublicKeyInfo			
algorithm			Public key algorithm used.
AlgorithmIdentifier			Choice of following three algorithms.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10040.4.1	Digital Signature Algorithm
		1.2.840.10045.2.1	Elliptic Curve Algorithms
parameters			For RSA include NULL; for DSA and ECDSA include parameters if subject and issuer have different parameters. If parameters are inherited, omit field for DSA and include NULL for ECDSA.
subjectPublicKey		BIT STRING	Subjects Public Key Bit String
extensions			Required Version 3 Certificates
AuthorityKeyIdentifier	FALSE		
KeyIdentifier		OCTET STRING	SHA-1 Hash for Authority Public Key
SubjectKeyIdentifier	FALSE		
KeyIdentifier		OCTET STRING	SHA-1 Hash for subjects Public Key
KeyUsage	TRUE	BIT STRING	Only indicated values are acceptable.
digitalSignature		1	for entity authentication or data origin integrity/authentication only
nonRepudiation		1	for verification of digital signatures
keyEncipherment		0	if public key is used for key transport
dataEncryption		0	encrypting user data
keyAgreement		0	public key used key agreement (e.g., D-H)

keyCertSign		0	Certificate signing
cRLSign		0	Revocation List signing
encipherOnly		0	if keyAgreement bit in on, this can only be used to encrypt data during key agreement.
decipherOnly		0	if keyAgreement bit in on, this can only be used to decrypt data during key agreement.
certificatePolicies	FALSE		Indicate the policies under which the certificate has been issued. Applications with policy requirements are expected to be able to process this extension
PolicyInformation			
policyIdentifier			See DEA Diversion Control E-Commerce PKI Certificate policy
policyQualifiers			
qualifier			
UserNotice			See DEA Diversion Control E-Commerce PKI Certificate policy
subjectAltName	FALSE		This extension is optional.
GeneralNames			
GeneralName			
rfc822Name			
dNSName			
IpAddress			
directoryName			See CPS
Name			
RDNSSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType			
AttributeValue			
IssuerAltName	FALSE		This extension is optional.
GeneralNames			
GeneralName			
rfc822Name			
cRLDistributionPoints	FALSE		This extension is required.
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName		"Distinguish Name"	
GeneralNames			
UniformResourceIdentifier		"ldap://url"	RFC 1738
directory name			See CPS
Name			
RDNSSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType			
AttributeValue			
cRLIssuer			Defaults to CA. If not different, there is no reason to use this extension.
AuthorityInfoAccess	FALSE		Only used for non-CRL revocation methods.
AccessDescription			
accessMethod		id-ad-ocsp, id-ad-calssuers	See RFC 2560 for use of id-ad-ocsp for OCSP responders
accessLocation			For id-ad-calssuers, this MUST be a URI if the information is available via http, ftp, or ldap.
GeneralName			
rfc822Name		IA5String	Required if information is available via e-mail
uniformResourceIdentifier		IA5String	URI required if information is available by http, ldap, or ftp
IPAddress		OCTET STRING	
Private Extensions			
id-dea-CertVerInfo	FALSE	0	The version of the DEA certificate
id-dea-RegistrantName	FALSE	"Jane Doe"	The Registrant Name (business or person name)
id-dea-Schedules	FALSE		The schedules the certificate owner is authorized to order, distribute, prescribe or dispense
schedule1			
schedule2			
schedule2n			
schedule3			
schedule3n			
schedule4			

schedule5			
id-dea-bcRole	FALSE		DEA business Category of the certificate holder.
majorRole		see main text	DEA sub business Category of the certificate holder.
subRole		see main text	DEA major business Category of the certificate holder.
id-at-postalAddress	FALSE	"123 Street Ave\$\$City\$ST\$12345"	This is the postal address of the Registrant
id-dea-RegNumSHA1	FALSE	OCTET STRING	Derived Hash of the DEA number and Serial number

Revocation Lists

Name	Critical Flag	Value	Comments
CRL Certificate			
CertificateList			
tbsCertList			Fields to be Signed
version		1	Version 2 CRL
signature			
algorithmIdentifier			Must match Algorithm Identifier in Signature Algorithm
algorithm		1.2.840.113549.1.1.5 (for RSA/SHA-1) 1.2.840.10040.4.3 (for DSA/SHA-1) 1.2.840.10045.1 (ECDSA/SHA-1)	Choice of following three algorithms. SHA-1 with RSAEncryption DSA with SHA-1 ECDSA with SHA-1
parameters		NULL	Only populate when using SHA-1 WithRSAEncryption
issuer			
Name			C= ; O= ; OU= ; CN= ; and DC= are recommended
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType			
AttributeValue			
thisUpdate			issue date of CRL
Time			
utcTime		YYMMDDHHMMSSZ	Used for dates up to and including 2049
generalTime		YYYYMMDDHHMMSSZ	Used for dates after 2049
nextUpdate			date by which the next CRL will be issued
Time			
utcTime		YYMMDDHHMMSSZ	Used for dates up to and including 2049
generalTime		YYYYMMDDHHMMSSZ	Used for dates after 2049
revokedCertificates			
userCertificate			
certificateSerialNumber			The serial number of Certificate
revocationDate			
Time			
utcTime		YYMMDDHHMMSSZ	Used for dates up to and including 2049
generalTime		YYYYMMDDHHMMSSZ	Used for dates after 2049
crEntryExtensions			
reasonCode	FALSE		
CRLReason			
unspecified			
keyCompromise			
cACompromise			
affiliationCompromise			
superseded			
cessationOfOperation			
certificateHold			
removeFromCRL			
invalidityDate	FALSE		This extension may be included if the invalidity date precedes the revocation date.
certificateIssuer	TRUE		This extension MUST appear if this certificate was issued by a different issuer than the previous certificate in the list, or the certificate is the first on an indirect CRL. If the first certificate in the list was issued by the CRL issuer, this extension may be omitted from that entry.
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
crExtensions			
authorityKeyIdentifier	FALSE		The authority key identifier extension provides a means of identifying the public key used to sign a CRL
keyIdentifier			Derived using SHA-1 hashing
cRLNumber	FALSE		
crNumber			Monotonically increasing seq. number
deltaCRLIndicator			
BaseCRLNumber			
CRLNumber			This value shall be identical to the value in the cRLNumber extension of the base certificate.

issuerAltName	FALSE		This extension is optional. Any name types may be present; only the most common are specified here. Other names may be included to support local applications.
issuingDistributionPoint	TRUE		This extension appears in segmented CRLs and indirect CRLs.
distributionPoint			
distributionPointName			If the issuer generates segmented or indirect CRLs, this field must be present.
onlyContainsUserCerts			If set to TRUE, this CRL only covers end entity certificates
onlyContainsCACerts			If set to TRUE, this CRL only covers CA certificates. If onlyContainsUserCerts is TRUE, this field must be FALSE.
onlySomeReasons			
reasonFlags			
unused			
keyCompromise			
cACompromise			
affiliationChange			
superseded			
cessationOfOperation			
certificateHold			
indirectCRL			If set to true, this CRL covers certificates that were not issued by the issuer of this CRL.
deltaCRLIndicator	TRUE		This extension is included if and only if the CRL is a delta CRL.
BaseCRLNumber			This value shall be identical to the value in the cRLNumber extension of the base certificate.
signatureAlgorithm			
algorithmIdentifier			Must match Algorithm Identifier in Signature Algorithm
algorithm		1.2.840.113549.1.1.5 (for RSA/SHA-1) 1.2.840.10040.4.3 (for DSA/SHA-1) 1.2.840.10045.1 (ECDSA/SHA-1)	Choice of following three algorithms. SHA-1 with RSAEncryption DSA with SHA-1 ECDSA with SHA-1
parameters		NULL	Only populate when using SHA-1 WithRSAEncryption
signatureValue			Issuer's digital Signature of certificate