

using the other key and (2) even knowing one key, it is computationally infeasible to discover the other key.

NIST means the National Institute of Standards and Technology.

Private key means the key of a key pair that is used to create a digital signature.

Public key means the key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair.

Public Key Infrastructure means a structure under which a Certification Authority verifies the identity of applicants, issues, renews, and revokes digital certificates, maintains a registry of public keys, maintains an up-to-date certificate revocation list, and validates digital certificates.

PKI means public key infrastructure.

§ 1311.05 Standards for technologies for electronic transmission of orders.

(a) A registrant or a person with power of attorney to sign orders for Schedule I and II controlled substances may use any technology to sign and electronically transmit orders if the technology provides all of the following:

(1) *Authentication*: The system must enable a recipient to positively verify the signer without direct communication with the signer and subsequently demonstrate to a third party, if needed, that the sender's identity was properly verified.

(2) *Non repudiation*: The system must ensure that strong and substantial evidence is available to the recipient of the sender's identity, sufficient to prevent the sender from successfully denying having sent the data. This criterion includes the ability of a third party to verify the origin of the document.

(3) *Message integrity*: The system must ensure that the recipient, or a third party, can determine whether the contents of the document have been altered during transmission or after receipt.

(b) DEA has identified the following means of electronically signing and transmitting order forms as meeting all of the standards set forth in paragraph (a) of this section.

(1) Digital signatures using Public Key Infrastructure (PKI) technology.

(2) [Reserved]

§ 1311.08 Incorporation by reference.

(a) The following standards are incorporated by reference:

(1) FIPS 140–2, Security Requirements for Cryptographic Modules.

(2) FIPS 180–1, Secure Hash Standard.

(3) FIPS 186–2, Digital Signature Standard. These standards are available from the National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899–8930 and are available at <http://csrc.nist.gov/>.

(b) These incorporations by reference will be submitted to the Director of the Federal Register in accordance with 5 U.S.C. 552(s) and 1 CFR part 51. Copies may be inspected at the Drug Enforcement Administration, 600 Army Navy Drive, Arlington, VA 22202 or at the Office of the Federal Register, 800 North Capitol Street, NW., Suite 700, Washington, DC 20408–0001.

Subpart B—Obtaining and Using Digital Certificates

§ 1311.10 Eligibility to obtain a digital certificate.

(a) The following persons are eligible to obtain a digital certificate from the DEA Certification Authority to sign electronic orders for controlled substances.

(1) The person who signed the most recent DEA registration application or renewal application.

(2) A person granted power of attorney by a DEA registrant to sign orders for one or more schedules of controlled substances.

(b) [Reserved]

§ 1311.15 Limitations on digital certificates.

(a) A digital certificate issued by the DEA Certification Authority will authorize the certificate holder to sign orders for only those schedules of controlled substances covered by the registration under which the certificate is issued.

(b) When a registrant, in a power of attorney letter, limits a certificate applicant to a subset of the registrant's authorized schedules, the digital certificate will allow the certificate holder to sign orders only for that subset of schedules.

§ 1311.16 Coordinators for controlled substances order system digital certificate holders.

(a) Each registrant, regardless of number of digital certificates issued, must designate one or more responsible persons to serve as that registrant's recognized agent regarding issues pertaining to issuance of, revocation of, and changes to digital certificates issued under that registrant's DEA registration.

While the coordinator will be the main point of contact between one or more DEA registered locations and the CSOS Certification Authority, all digital certificate activities are the responsibility of the registrant with whom the digital certificate is associated. Even when an individual registrant, *i.e.*, an individual practitioner, is applying for a digital certificate to order controlled substances a CSOS Coordinator must be designated.

(b) Once designated, coordinators must identify themselves, on a one-time basis, to the Certification Authority. If a designated coordinator changes, the Certification Authority must be notified of the change and the new responsibilities assumed by each of the registrant's coordinators, if applicable. Coordinators must complete the application that the DEA Certification Authority provides and submit the following:

(1) Two copies of identification, one of which must be a government-issued photographic identification.

(2) A copy of each current DEA Certificate of Registration (DEA form 223) for each registered location for which the coordinator will be responsible, if available, or if the applicant (or their employer) has not been issued a DEA registration, a copy of each application for registration of the applicant or the applicant's employer.

(3) The applicant must have the completed application notarized and forward the completed application and accompanying documentation to the DEA Certification Authority.

(c) Coordinators will communicate with the Certification Authority regarding digital certificate applications, renewals and revocations. For applicants applying for a digital certificate from the DEA Certification Authority, and for applicants applying for a power of attorney digital certificate for a DEA registrant, the registrant's Coordinator must verify the applicant's identity, review the application package, and submit the completed package to the Certification Authority.

§ 1311.20 Requirements for obtaining a certificate for a digital signature for orders.

(a) To obtain a certificate to use for signing electronic orders for controlled substances, a registrant or person with power of attorney for a registrant must complete the application that the DEA Certification Authority provides and submit the following:

(1) Two copies of identification, one of which must be a government-issued photographic identification.