

(2) A current listing of DEA registrations for which the individual has authority to sign controlled substances orders.

(3) A copy of the power of attorney from the registrant, if applicable. If the registrant does not authorize the applicant to order all schedules allowed under the registrant's registration, the power of attorney form or letter must indicate which schedules of controlled substances the applicant is authorized to order.

(4) A signed Subscriber Agreement stating the applicant has read and understands the agreement and agrees to the statement of subscriber obligations that DEA provides.

(b) The applicant must provide the completed application to the registrant's coordinator for controlled substances order system digital certificate holders who will review the application and submit the completed application and accompanying documentation to the DEA Certification Authority.

(c) When the Certification Authority approves the application, it will send the applicant a one-time use access code and password, via separate channels, and information on how to use them. Using this information, the applicant must then electronically submit a request for certification of the public digital signature key. After the request is approved, the Certification Authority will provide the applicant with the signed public key certificate and the Certification Authority's public key certificate.

(d) Once the applicant has generated the key pair, the Certification Authority must prove that the user has possession of the key. For public keys, the corresponding private key must be used to sign the certificate request.

Verification of the signature using the public key in the request will serve as proof of possession of the private key.

§ 1311.30 Requirements for storing and using a private key for digitally signing orders.

(a) Only the certificate holder may access or use his or her digital certificate and private key.

(b) The certificate holder must provide FIPS-approved secure storage for the private key.

(c) A certificate holder must ensure that no one else uses the private key. While the private key is activated, the certificate holder must prevent unauthorized use of that private key.

(d) A certificate holder must not make back-up copies of the private key.

(e) The certificate holder must report the loss, theft, or compromise of the private key or the password, via a

revocation request, to the Certification Authority within 24 hours of discovery of the loss, theft, or compromise. Upon receipt and verification of a signed revocation request, the Certification Authority will revoke the certificate. The certificate holder must apply for a new certificate under the requirements of § 1311.20.

§ 1311.40 Number of digital certificates needed.

(a) A purchaser of Schedule I and II controlled substances must obtain a separate certificate for each registered location for which the purchaser will order these controlled substances.

(b) [Reserved]

§ 1311.45 Renewal of digital certificates.

(a) A certificate holder must generate a new key pair and obtain a new digital certificate when the registrant's DEA registration expires or whenever the information on which the certificate is based changes. This information includes the registered name and address and the schedules the certificate holder is authorized to handle. A certificate will expire on the date on which the DEA registration on which the certificate is based expires.

(b) The Certification Authority will notify each certificate holder 45 days in advance of the expiration of the certificate holder's digital certificate.

(c) If a certificate holder applies for a renewal before the certificate expires, the certificate holder may renew electronically twice. For every third renewal, the certificate holder must submit a new application and documentation, as provided in § 1311.20.

(d) If a certificate expires before the holder applies for a renewal, the certificate holder must submit a new application and documentation, as provided in § 1311.20.

§ 1311.50 Requirements for registrants that allow powers of attorney individual to obtain digital certificates under their DEA registration.

(a) A registrant that grants power of attorney must report to the DEA Certification Authority within 6 hours of either of the following:

(1) The person with power of attorney has left the employ of the institution.

(2) The person with power of attorney has had his or her privileges revoked.

(b) A registrant must maintain a record that lists each person granted power of attorney to sign controlled substance orders.

§ 1311.55 Requirements for recipients of digitally signed orders.

(a) The recipient of a digitally signed order must do the following before filling the order:

(1) Verify the integrity of the signature and the order by having the software validate the order.

(2) Verify that the certificate holder's digital certificate has not expired by checking the expiration date against the date the order was signed.

(3) Check the validity of the certificate holder's certificate by checking the Certificate Revocation List.

(4) Check the extension data to determine whether the sender has the authority to order the controlled substance.

(b) A recipient may cache Certificate Revocation Lists for use until they expire.

§ 1311.60 Requirements for systems used to process digitally signed orders.

(a) A certificate holder and recipient of an electronic order may use any system to write, track, or maintain orders provided that the system has been enabled to process digitally signed documents and that it meets the requirements of paragraph (b) or (c) of this section.

(b) A system used to digitally sign orders must meet the following requirements:

(1) The cryptographic module must be FIPS 140-2 validated.

(2) The digital signature system and hash function must be compliant with FIPS 186-2 and FIPS 180-1.

(3) The private key must be stored encrypted on a FIPS 140-2 validated cryptographic module using a FIPS-approved encryption algorithm.

(4) The system must use either a user ID and password combination or biometric authentication to access the private key. Activation data must not be displayed as they are entered.

(5) The system must set a 10-minute inactivity time period after which the certificate holder must reauthenticate the password to access the private key.

(6) For software implementations, when the signing module is deactivated, the system must clear the plain text private key from the system memory to prevent the unauthorized access to, or use, of the private key.

(7) The system must be able to digitally sign and transmit an order.

(8) The system must have a time system that is within five minutes of the official National Institute of Standards and Technology time source.

(9) For orders, the system must archive the digitally signed orders and any other records required in Part 1305