AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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.

§ 1311.25 Requirements for obtaining a CSOS digital certificate.

(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.

(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.

(4) An acknowledgment that the applicant has read and understands the Subscriber 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 CSOS 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 reference number and access code, 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.

(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, as discussed by FIPS 140–2, 180–2, 186–2, and accompanying change notices and annexes, as incorporated by reference in § 1311.08.

(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 substantiation 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 § 1311.25.

§ 1311.35 Number of CSOS digital certificates needed.

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

§ 1311.40 Renewal of CSOS digital certificates.

(a) A CSOS certificate holder must generate a new key pair and obtain a new CSOS 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, the subscriber's name, and the schedules the registrant is authorized to handle. A CSOS 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 CSOS certificate holder 45