

would serve as proof of possession of the private key. The user would not need to learn the keys. The user would employ an authentication mechanism to access the private key. The authentication mechanism could be a user name and password. Although DEA is not requiring use of biometrics, DEA recognizes the advantages of biometric passwords to ensure that a private key cannot be shared and suggests that registrants consider their use.

- When the users want to digitally sign an order, they would authenticate themselves to access the private key to sign the document. Specific procedures may vary depending on the exact nature of the system employed, but basically, once the certificate holder has accessed the private key, a single key stroke would "sign" the document. At the keystroke, the software would perform the hashing functions and encryption, attach the encrypted hash and digital certificate to the plain text order, and transmit.

At the supplier end, the steps are equally simple:

- The supplier would receive the order electronically. The digital certificate attached to the order would contain the information necessary for the supplier to determine whether the person is eligible to write the order received.
- The supplier would validate the order.
- The supplier's software would automatically check the certificate revocation list to verify that the user's certificate had not been revoked. It would also verify that the certificate was signed with the DEA CA certificate.
- The software would use the sender's public key to decrypt the signature, obtain the hash, and automatically compare it with the hash of the plain text message generated by the supplier's software to determine if the file had been altered.
- The software system would check the expiration date on the certificate to ensure that the certificate had not expired when the order was signed.
- The software would compare the controlled substances ordered with the schedules listed in the certificate to verify that the certificate holder is authorized to order the schedule.
- Only if all the checks indicate a valid order would the system indicate that the order was valid.

The supplier's system would have to require that all authentication and validation steps be carried out before allowing the order to be processed.

What Is a Certification Authority and Why Is It Needed?

In the Form 222 system, DEA issues the forms to registrants, providing assurance to suppliers that the orders they receive are from registrants authorized to order Schedule I and II controlled substances. In a PKI system, a Certification Authority (CA) acts as a credible and neutral trusted third party and is central to the operation of the digital certificates. Each party (the certificate holder and recipient of a digitally signed document) relies on the CA. If they trust the CA, they can trust the certificates the Certification Authority issues. Without a trusted third party, each recipient would have to determine whether each sender could be trusted. A Certification Authority makes it possible for a recipient to receive orders from persons who have never before placed orders with them and quickly determine whether the person has a right to order the substance. This process is similar to the Form 222 issued by DEA, which contains preprinted registrant information, including the registrant's name, address, DEA registration number, and schedules.

What Would the Certification Authority Do?

The Certification Authority would enroll certificate holders and verify the identity of an applicant and the applicant's DEA status before issuing a certificate. The Certification Authority would maintain a public directory of certificate holders' public keys and a Certificate Revocation List (CRL), both of which recipients of digitally signed documents must check to verify the validity of a certificate. The Certification Authority would operate under a publicly available Certificate Policy, a set of rules that covers subjects such as obligations of the Certification Authority, the certificate holders, and those relying on the Certification Authority for validation; enrollment and renewal procedures; operational requirements; security procedures; and administration.

Who Would Serve As the Certification Authority?

Because a digital certificate is the functional equivalent of a Form 222 that DEA is required to issue, only DEA can serve as the Certification Authority for issuing digital certificates for signing electronic orders for Schedule I and II controlled substances. Registrants and their designated power of attorney holders (POA) who are eligible to sign Forms 222 would apply to the DEA

Certification Authority and obtain a digital certificate from it. DEA proposes to act in this capacity either directly or through a contractor.

III. Discussion of the Proposed Rule on Electronic Orders

A. Digital Certificates

How Are Digital Certificates Obtained?

Anyone eligible to sign orders for controlled substances would be able to apply to the DEA Certification Authority for a digital certificate. Under the current rules, DEA requires only orders for Schedule I and II substances to be signed. That requirement will not change. DEA recognizes, however, the registrants who order or fill orders for Schedule III-V substances may want the ability to digitally sign these orders. The digital certificate attached to a digitally signed order would provide the supplier with instant verification of DEA status, which suppliers are required to make a good faith effort to determine. Consequently, DEA intends to make digital certificates available to registrants who are eligible to order only Schedule III through V substances and to employees at Schedule II through V registrants who are authorized to issue only Schedule III through V orders. The requirements for applying for a digital certificate would be the same for any applicant.

Who Are CSOS Coordinators and What Is Their Role in the Digital Certificate Enrollment Process?

CSOS Coordinators are one or more responsible persons designated by a DEA registrant 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. These individuals serve as knowledgeable liaisons between one or more DEA registered locations and the CSOS Certification Authority. While the CSOS Coordinator is the main point of contact between the DEA Certification Authority and the DEA registrant, all digital certificate activities are the responsibility of the registrant with whom the digital certificate is associated. To that end, the CSOS Certification Authority will communicate with the CSOS Coordinator regarding digital certificate applications, renewals, revocations, and other matters. 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. It is acceptable to have the person applying for the registrant digital