

automatically without the applicant having to enter codes individually. DEA believes that these steps will facilitate the application and certificate generation process while retaining the basic integrity of the Form 222 system that links every order to a specific registered location.

What Is the Renewal Period for Digital Certificates?

Digital certificates must be renewed when the DEA registration expires. DEA considered requiring annual renewal of digital certificates, which is the current industry practice. DEA determined, however, that this frequency was not necessary to maintain the security of the system and is proposing that certificates be valid for the life of the registrant's DEA registration. Certificates cannot be valid beyond the life of a DEA registration because the certificate's validity is based on having an active DEA registration. Practically, therefore, manufacturers, distributors, exporters, researchers, chemical analysts, and narcotic treatment programs would have to renew annually because their DEA registrations are valid for one year. Pharmacies, institutional practitioners, teaching institutions, and individual practitioners would have to renew every three years.

The Certification Authority would notify certificate holders of the need to renew the certificate. DEA would permit the digital certificate to be renewed online twice after the original application process, so long as the certificate holder applies for renewal before the DEA registration and digital certificate expire. Upon the third renewal request, the digital certificate holders must re-establish their identity using the initial application process. Although this process is considered a renewal because a new application is not needed, at each renewal, a new set of key pairs would be generated and a new certificate issued. The Certification Authority would arrange a simple online process to renew a certificate. When a certificate holder files a renewal request before the DEA registration expires, DEA would not issue the new certificate until the Certification Authority has determined that the DEA registration on which the certificate is based has been renewed.

If the certificate holder fails to apply for a new certificate before the date on which the DEA registration expires, the certificate holder would have to submit a new application for a certificate, including all of the documents required for an initial application. The same is true if the certificate holder's digital certificate is revoked for any reason.

What Are the Requirements for Companies That Grant Power of Attorney to Authorize Use of Their DEA Registrations?

As noted above, all registrants must designate a CSOS Coordinator to serve as the registrant's recognized agent regarding issues pertaining to issuance of, revocation of, and changes to digital certificates issued under that registrant's DEA registration. One of the responsibilities of the CSOS Coordinator is to oversee the application process for persons applying for a digital certificate as powers of attorney for a registrant. The CSOS Coordinator(s) will be responsible for ensuring that those persons applying for power of attorney authority are permitted by the registrant to possess such authority. DEA believes that the designation of CSOS Coordinators will streamline the power of attorney application process and will provide a safeguard to ensure that only personnel authorized by the registrant are granted power of attorney digital certificates.

Registrants who grant power of attorney status to certain employees to sign orders would be required to do the following:

- Provide a letter granting power of attorney to be submitted with the person's application for a digital certificate.
- Read the statement of registrant obligations regarding power of attorney contained in the subscriber agreement provided by the Certification Authority and sign a statement agreeing to meet the obligations.
- Ensure that powers of attorney use their digital certificates appropriately.
- Notify the Certification Authority, through the CSOS Coordinator responsible for the registered location at which the power of attorney works, within 6 hours of revocation of the power of attorney.
- Notify the Certification Authority, through the CSOS Coordinator responsible for the registered location at which the power of attorney worked, within 6 hours of the time the person leaves the registrant's employ.

The obligations in the statement of registrant obligations are basically to oversee the use of certificates to ensure that they are used only by the certificate holder and to notify the Certification Authority if a certificate holder is no longer authorized to use the registrant's DEA number to order controlled substances.

What Systems Are Required To Use a Digital Signature?

Any system enabled to handle digital signatures may be used provided it meets the following requirements:

1. The cryptographic module must be FIPS 140-2 validated.
2. The digital signature system must be FIPS 186-2 validated and use the RSA algorithm.
3. The hash function must be FIPS 180-1 validated.
4. The system must control the activation of the private key with an authentication mechanism.
5. The system must employ a ten-minute inactivity time period after which the certificate holder must re-authenticate 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 digitally sign and transmit the electronic order.
8. The system must communicate with the Certification Authority directory.
9. The system must have a time system that is within five minutes of the official National Institute of Standards and Technology (NIST) time source.
10. The system must archive digitally signed files.
11. The system must create an order that includes the data fields listed in proposed § 1305.21(b)—these fields are the same fields that exist on the Form 222 that purchasers complete except for the line numbers, total number of lines and purchaser information, *i.e.*, name, address, DEA registration number, authorized schedules, and business activity, all of which are included in the digital certificate which must accompany the order.

The three FIPS standards (discussed in more detail below) are needed to ensure the integrity of the key and hash generating systems. The fourth item requires that the system control access to the private key through a method of authenticating the user. As discussed below, DEA is proposing that certificate holders use at least a password and user ID combination. If a certificate holder elects to use a biometric authentication method, the single biometric (other than voice recognition) would be sufficient.

Item five is needed to ensure that the digital signing capability cannot be accessed by someone other than the certificate holder. DEA is concerned that a certificate holder authenticate himself or herself to the system, open the signing software, and begin signing