

orders. If the certificate holder left the computer while the signing system was open, another person could sign orders because the signing software generally does not require reauthentication of the user for each order once the private key has been accessed. The automatic closure of the system if unused for 10 minutes will lessen this threat.

Item six would ensure that the private key cannot be retrieved from the certificate holder's computer memory following its use. Software systems may not automatically clear items from memory when the application is shut down. Therefore, it is necessary to specify that the software clear the private key from the system's memory whenever the signing application is closed to ensure that someone cannot recover the key.

Items seven and eight are the basic requirements for a digital signature system, the ability to sign a document digitally and communicate with the CA.

Item nine requires the system to have a time system within five minutes of the official National Institute of Standards and Technology time source. It is important that all users of the CSOS system be synchronized to a single, consistent time source.

Items 10 and 11 are necessary for the system to function as a substitute for a Form 222. Item 11 requires the creation of an order that includes all of the Form 222 information. Item 10 ensures that the system automatically stores and retains the orders.

What Systems Are Required To Be Able To Process a Digital Signature?

Any system may be used to process an electronic order provided it has been enabled to handle digital signatures and that it meets the following requirements:

1. The digital signature system must be FIPS 186-2 validated and use the RSA algorithm.
2. The hash function must be FIPS 180-1 validated.
3. The system must check the purchaser certificate extension data to determine that the controlled substances ordered are on schedules the purchaser is eligible to order and that the certificate had not expired at the time the order was signed.
4. The system must decrypt the digital signature using the purchaser's public key and determine that an order has not been altered in transmission.
5. The system must check the certificate revocation list and the CA's directory automatically and invalidate any order signed with a certificate listed on the CRL or not included in the CA directory.

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

7. The system must archive the order and include the digital certificate linked to the order in the record of each order.

8. The system must require that all authentication and validation steps are carried out prior to allowing the processing of the order to be completed. Further, the system will not allow orders that have failed to pass any authentication or validation step to be processed.

9. If the supplier intends to file a summary report of orders rather than copies of the actual orders, the system must create a report that includes, for each Schedule I and II order, all data fields listed in proposed § 1305.28(a) in a format that DEA specifies. This provision would allow for compliance with the current paper requirement that suppliers forward copy 2 of the DEA Form 222 to the nearest DEA office on a monthly basis.

Items 1 and 2, the three FIPS standards (discussed in more detail below), are needed to ensure the integrity of the key and hash generating systems. Items 3, 4, 5, and 6 are needed to ensure that the system can and does validate each order by checking that the order was signed by the certificate holder, that the order has not been altered, that the registrant is eligible to order the substances, and that the certificate has not expired or been revoked. Item 7 ensures that the system automatically stores and retains the orders. Item 9 requires the creation of a report that includes all of the Form 222 information.

What Are the FIPS Standards and Why Are They Needed?

FIPS means Federal Information Processing Standard. FIPS 140-2 is a standard entitled "Security Requirements for Cryptographic Modules." The standard is produced by the National Institute of Standards and Technology (NIST) to lay out general requirements for cryptographic modules for computer and telecommunications systems. FIPS 186-2 specifies algorithms for applications used to generate digital signatures. FIPS 180-1 is the Secure Hash Standard. The standards have been adopted by the U.S. government and are required for all cryptographic-based security systems and digital signature systems that are used by or approved by Federal agencies to protect unclassified information. DEA, therefore, must require that the software modules used for digital signatures comply with these standards.

A list of vendors whose cryptographic modules have been validated as FIPS 140-2 compliant may be obtained from the NIST web site at <http://csrc.nist.gov/cryptval/140-2/1402vend.htm>.

Information on FIPS 186-2 and FIPS 180-1 can be obtained from <http://csrc.nist.gov>.

The modules that have been validated as compliant with these standards can be used to enable software to handle digital signatures. As long as the code in the compliant module is not altered, adding it to the software would not alter its validation.

How Is It Possible To Determine Whether a Specific System Meets These Criteria?

Before implementing an electronic system for Schedule I and II controlled substances orders, the software system must be certified by means of a third-party audit that determines the system performs the required functions. Registrants must ensure that any software/system that they use for electronic Schedule I and II orders has been certified. Certification from the software developer/vendor that the product being acquired has received the required audit is sufficient.

After the initial audit, the developer or vendor would be required to have third-party audits whenever the signing or verifying functionality is changed to ensure that the software continues to function as required. Registrants who implement order systems developed by third-party vendors would obtain a certification from the vendor. In instances where suppliers provide their customers with ordering software for use in this system, it would be the supplier's responsibility to ensure this auditing requirement has been satisfied. Individual customers of that supplier would not be required to maintain a copy of the audit report.

DEA recognizes that software systems are modified frequently, as vendors add services and improve functions. Modifications would need to be audited when the modification affects the digital signature or validation part of the system. If the modifications relate to other functions and do not change the digital signature functions or validation functions, modifications would not trigger a need for a third-party audit.

What Are the Requirements for Safeguarding Private Keys?

DEA regulations require that each registrant provide effective controls and procedures to guard against theft and diversion of controlled substances. This requirement applies to both physical and procedural safeguards; a registrant