

signature" technology that meets the dual requirements:

- The digital certificate provides the message/record integrity, authentication, and nonrepudiation that DEA has determined are necessary to tie these communications to a specific person and prevent alteration of the documents. These standards are substantially related to achieving diversion control.

- The digital certificate would be the functional equivalent of the paper order form, which the CSA requires DEA to issue.

The digital certificate system DEA is proposing would establish an electronic alternative to Form 222 for Schedule I and II controlled substances that will allow registrants to retain their current ordering systems. Instead of an electronic form, the DEA Certification Authority will issue digital certificates, which will serve as an electronic equivalent of the Form 222.

How Is a Digital Certificate an Electronic Equivalent of a Form 222?

The key elements of a Form 222 are that DEA issues them only to registrants authorized to order Schedule I and II controlled substances and preprints the forms with information that ties the form to a specific registrant and location. Only digital certificates issued by DEA under the same circumstances as the Form 222 will be allowed for signing electronic orders for Schedule I and II controlled substances. All of the information currently preprinted on the Form 222 will be part of the digital certificate extension data, which will be included on each order that is digitally signed. The digital certificate attached to an electronic order with the digital signature will create the equivalent of the Form 222. To accept an order, the supplier's software must perform the validation functions, thus confirming that the purchaser is authorized by DEA to order the specified schedules of controlled substances.

This approach will allow registrants to use their current electronic order systems provided the systems can be enabled to accept and validate the DEA-issued digital certificate/signature information and the orders include the information currently required on a Form 222. DEA has been working with industry to develop code to enable existing systems to reduce the cost of implementation.

DEA will not limit digital certificates to those registrants authorized to order Schedule I and II controlled substances. Any DEA registrant eligible to order controlled substances will be able to obtain a DEA-issued digital certificate;

the certificate extension data will inform the supplier which schedules a purchaser is authorized to order. Although the digital certificates would be required for signing and transmitting electronic orders for Schedule I or II controlled substances, DEA will encourage registrants to use the certificates to sign all electronic orders for controlled substances. Using the DEA-issued certificates will reduce the burden on suppliers, who must verify the purchaser's DEA status; the certificate extension data and the validity of the certificate will provide this information.

In Simple Terms, How Does a Digital Signature Work?

This section provides a simplified description of how a digital signature system works. Each certificate holder would have a public key, available to anyone, and a private key, which the certificate holder must keep secure. The two keys are used by an asymmetric encryption algorithm; what one key encrypts, only the other key can decrypt. The two keys are different and cannot be practically derived from each other.

When the certificate holder digitally signs an order, the PKI-enabled software runs the text of the order through a complex algorithm that creates a fixed length digest of the document (called a hash). The hash is a compact representative image of the document that is often referred to as a document "fingerprint." The software then uses the private key to encrypt the hash; the encrypted hash is the digital signature.

The purchaser's software transmits a plain text order with the encrypted hash and the sender's digital certificate to the supplier. When the supplier receives the document, the supplier's software would use the sender's public key, which is part of the certificate, to decrypt the digital signature. If the public key can decrypt the digital signature successfully, the supplier would know that only the holder of the private key could have sent the digitally signed order. The supplier's software would then use the same hashing algorithm the purchaser used to create a second digest (hash) of the plain text document received. If the new hash is identical to the hash the computer has decrypted, the document has not been altered in transmission. If even a single space or letter in the document has been changed, the hashes would not match and the document must be considered invalid.

The power of the digital signature approach is that it provides for authentication, nonrepudiation, and

message/record integrity. The supplier can be certain that only a specific certificate holder could have signed the document (because the Certification Authority verified the identity before issuing the certificate and because the public key decrypted the signature) and that the document has not been altered in transmission (because the hashes match). In addition, the other information included in the digital certificate attached to the order (name, address, DEA registration number, business activity, schedules, and expiration date) provides the supplier an instant source of information to verify the sender's right to issue and sign the order. The system also would automatically check the certificate revocation list to be sure that the certificate is still valid.

For a more complete discussion of the technical details of digital signatures, and a complete list of approved algorithms, see the Federal Information Processing Standard (FIPS) 186-2.

In Simple Terms, How Would This System Work for the User?

Practical implementations of PKI technology are typically simple and transparent for the user, despite the complex technologies involved. The complex parts of the system are automatically handled by the software system.

The steps a user would take are as follows:

- To obtain a digital certificate, a DEA registrant or a person granted power of attorney authority to obtain and sign Schedule I and II orders for a registrant would submit proof of identification and proof of a current DEA registration to the Certification Authority (CA). The applicants would also have to install software to PKI-enable their computers or ensure that their network browsers are PKI-enabled. Most recent versions of Internet browsers are PKI-enabled.

- Once the CA verifies the identification, the CA would send the applicant a one-time use access code and password via separate channels. The applicant would use the PKI software to generate a key pair (public and private keys) and access the Certification Authority electronically using the access code and password to request a certificate. These keys would be stored in the applicant's computer or on a FIPS 140-2 approved secure hardware device. Once generated, the Certification Authority must prove that the user has possession of the key. For signature public keys, the corresponding private key must sign the certificate request. Verification of the signature using the public key in the request