

identified that meet all of the performance standards, DEA will consider them and determine whether they could satisfy the CSA mandates with respect to order forms.

The proposed rule would not mandate the use of an electronic system, but would provide registrants with an alternative to DEA Form 222. A DEA-issued digital certificate would contain the information that DEA preprints on a Form 222. Each registrant who wants to order Schedule I or II controlled substances electronically would need to apply to the DEA Certification Authority (CA) for a digital certificate.

#### *Why Are Authentication, Nonrepudiation, and Message Integrity Requirements Necessary?*

The CSA requires that Schedule I or II controlled substances be distributed only in response to signed orders submitted by purchasers on a form issued to them by DEA. The paper Form 222 offers a level of authentication because DEA issues the form only to a valid registrant who is authorized to place the order. Further the order form is bound to a specific registrant and location preprinted by DEA on the form. The registrant's manual signature on the form provides the element of nonrepudiation. The existence of multiple copies held by separate parties ensures the integrity of the document.

With electronic transmission, the importance of authentication, nonrepudiation, and message integrity, criteria the current system meets, is magnified. It is not difficult to send electronic messages in other people's names or intercept, duplicate, or alter messages. Image files and read-only files are now relatively easy to copy, alter, and replace. If purchasers and suppliers are to be able to use computer technology for controlled substance orders, it is critical that they be able to trust the system. Suppliers and purchasers must trust that an order has not been altered during transmission. Suppliers must trust that the purchaser who signed the order is who he or she claimed to be. They (and DEA) must be certain that an order they sign or receive has not been altered and that no one other than an authorized, DEA-registered purchaser could have sent it.

None of the three characteristics is sufficient by itself. If a technology provided nonrepudiation and authentication of the signature, but the message could be altered, the nonrepudiation and authentication would be questionable. For example, if the identity of a purchaser was verified and a purchaser used a biometric to electronically sign an order, but the

document could be altered either during transmission or after receipt by the supplier, the purchaser could repudiate the document even though it could be proved that a specific registrant had signed it. If the message could not be altered, but the identity of the signature holder had never been verified or the password or signing key could be used by anyone, the integrity of the message would also be questionable. In this case, you could prove that a specific order had been sent, but not who had actually sent it. To retain the integrity of the diversion control system, it is necessary to establish specific performance criteria with minimum acceptable standards for any technology that is to be used for signing Schedule I and II controlled substance orders.

#### *What Existing Technologies Meet These Proposed Criteria?*

At present, only a digital signature based on a public key infrastructure (PKI) would provide the authentication, nonrepudiation, and message integrity that are necessary to protect these communications and prevent alteration of the documents. In a June 2000 report, "The Evolving Federal Public Key Infrastructure," the Federal Public Key Infrastructure Steering Committee described the benefits PKI provides as follows:

Public key technology provides a mechanism to authenticate users strongly over closed or open networks, ensure integrity of data transmitted over those networks, achieve technical nonrepudiation for transactions, and allow strong encryption of information for privacy/confidentiality or security purposes. Strongly authenticating users is a critical element in securing any infrastructure; if you cannot be certain with whom you are dealing, there is substantial potential for mischief. Ensuring data integrity of data from end-user to end-user makes it more difficult for data substitution attacks aimed at servers or hosts to succeed. Technical nonrepudiation binds a user to a transaction in a fashion that provides important forensic evidence in the event of a later problem. Encryption protects private information from being divulged even over open networks.

PKI systems are based on asymmetric cryptography: the holder of the digital certificate has a private key, which only the certificate holder can access, and a public key, which is available to anyone. What one key encrypts, only the other key can decrypt. It is computationally infeasible for the two keys to be derived from each other. Only one public key will validate signatures made using its corresponding private key. Because the private key is held by only one person, it is that person's responsibility to ensure that it is not

divulged or compromised. The method in which PKI systems ensure the integrity of the message is explained in detail in the section entitled "In simple terms, how does a digital signature work?"

A PKI system is more than cryptographic keys. The infrastructure component (the "I" in PKI) is critical to meeting the criteria for authentication, integrity and nonrepudiation. PKI systems are operated by a Certification Authority (CA), which is responsible for verifying the identity of any applicant for a digital certificate, maintaining security, establishing the responsibilities of certificate holders, and maintaining a public directory of public keys and an up-to-date certificate revocation list. The Certification Authority is a trusted third party. Suppliers and purchasers need only trust the CA, in this case DEA, to be able to trust each other.

#### *Why Do Other Electronic Signature Systems Not Meet the Performance Standards?*

Other technologies create signatures that are generically referred to as electronic signatures. DEA investigated other electronic signature technologies, but determined that none of them met all three performance criteria. Common electronic signature systems include symmetric cryptography technologies and non-cryptographic methods. Any of the systems may provide for authentication if the controlling authority takes steps to verify the identity of the person using a cryptographic key or password, but this verification is not usually a key element of systems based on electronic signature technologies. Electronic signature systems that rely on symmetric cryptography, where both parties to the transaction use the same key, do not meet the standard of nonrepudiation. The Federal Public Key Infrastructure Steering Committee also noted that symmetric cryptography technology is not suitable for systems that have more than a few users.

None of these electronic signature technologies, by themselves, including biometrics, provide for record integrity. With any of the existing electronic signature technologies, there would be no assurance that the record had not been altered during or after transmission.

#### *Why Is a Digital Signature Approach Necessary?*

After reviewing options, DEA determined that a digital certificate issued by DEA is the only "electronic