Digital Signatures

R.D. McDowall, McDowall Consulting, Bromley, Kent, UK.

When signing the US E-commerce bill, Bill Clinton used the latest digital gadgetry and his dog's name as a password. Are we ready for the technology?

In recent "Pharmaceutical Files" we discussed first electronic signatures and logical security (1) and then biometrics (2) within the context of the *Electronic Signatures and Electronic Records Final Rule* (21 CFR Part 11) (3).

Electronic signatures consist of a unique combination of user identity and password and we discussed some of the issues surrounding the security of passwords and the access control needed for an application or system. Biometrics use biological traits and characteristics for the verification of an individual's identity and to sign electronic records.

The 21 CFR Part 11 regulations also mention the term *digital signature* as a type of electronic signature when used with open systems (not controlled by those who are responsible for generating the electronic records). A digital signature is defined by the Food and Drug Administration (FDA) (3) as:

…an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

To help decipher what this means in practice, we'll be discussing digital signatures and how they can be used within the context of 21 CFR Part 11. This method of signing records is intended for use within open systems (3) but as the e-commerce and biometric systems become more cost-effective and reliable, they will be used routinely for closed systems as they will eliminate many of the problems caused by misuse of passwords.

Paper and Electronic Security

Over time the means of ensuring the security of paper signatures and handwritten signatures has evolved in four main areas:

- Non-repudiation: the certainty of knowing that the sender or signer of the message cannot later deny sending or signing a document.
- Authentication: a guarantee that a message has come from the person whose name is on the bottom of it.
- Confidentiality: evidence that the contents of the message have not been seen by anyone not authorized to see it.
- Integrity: knowing that the message contents have not been modified during transmission either accidentally or deliberately.

Take a simple paper message: you can write it on your organization's headed notepaper, sign it and then send it in a sealed envelope to a recipient. Using this low technology approach you'll meet the four security requirements outlined above. I'll ignore your thoughts of an industrial spy steaming letters open and reading the contents, as you should be able to see the envelope has been modified.

This is the situation for paper, but what is the equivalent situation for the electronic world? To understand digital signatures fully, we need to understand public key infrastructure (PKI) and its wider role in e-commerce, and how it can be applied within the pharmaceutical industry for open systems.

Public Key Infrastructure

There are several elements essential to an effective PKI, these are:

Certificate Authority (CA): The CA system is the trust centre of a PKI as it manages the public key certificates for their whole life cycle. Although an organization can set up its own CA, it is easier to use the services of a commercial CA or Trusted Third Party. The CA issues certificates by binding the identity of a user or a system to a public key with a digital signature. All certificates have an expiry date but if problems occur then specific certificates can be revoked and these are highlighted in Certificate Revocation Lists (CRLs) published by the CA.

Certificate Practice Statement (CPS): PKI systems operated by commercial CAs require a CPS. This is a document detailing the operational procedures on how the security policy will be enforced and supported in practice. It typically includes how the CA is constructed and operated; how certificates are issued, accepted and revoked; and how keys will be generated, registered and certified; where they will be stored; and how they will be made available to users.

Registration Authority (RA): An RA provides the interface between the user and the CA. It captures and authenticates the identity of the users and his or her certificate request to the CA. The quality of this authentication process determines the level of trust that can be placed in the certificates.

The key issue is that users of PKI place their trust in the CA and the RA. Therefore, the individuals don't need to trust each other because the process of registration should guarantee that individuals are who they say they are.

Certificate Distribution System: Certificates can be distributed in several ways depending on the structure of the PKI environment; for example, by the users

themselves, or through a directory service. A directory server may already exist within an organization or one may be supplied as part of the PKI solution from a certification authority.

Security Policy: When an organization wants to use PKI it should have a security policy with appropriate procedures under it. The policy will define an organization's high-level requirements for information security including cryptography, and the procedures will present how it will handle the public and private keys, its intellectual property and training of staff to use the technology effectively (these are the procedures required under 21 CFR Part 11). Thought needs to go into this process and you'll have to have a good understanding of how the technology will be used; ideally a pilot scheme would help you evolve this.

PKI-enabled Applications and Hardware: You don't just go down to the local computer supermarket and pick up a PKI-enabled application. You will need to have the additional hardware such as smart cards and readers in place within your organization for the sender and the recipient before you can roll this out. This is not a trivial operation. Again, I'll stress the need for an evalution of the technology here as well as working out the policies.

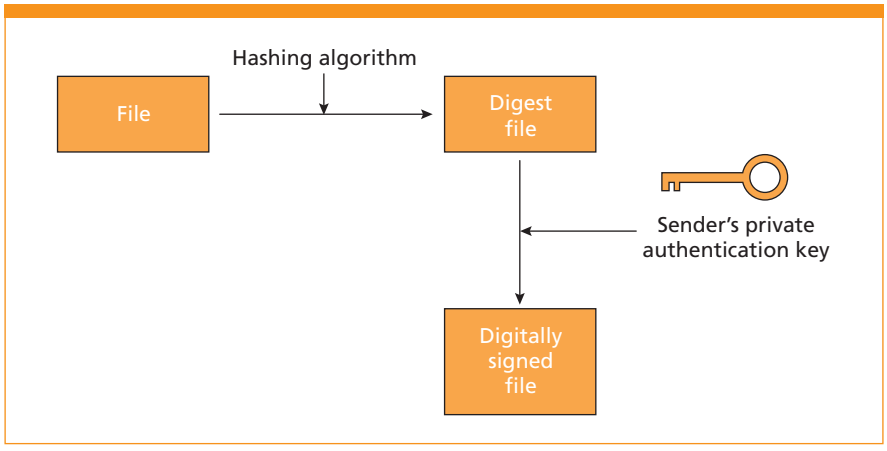

Figure 1: *Digitally signing a document.*

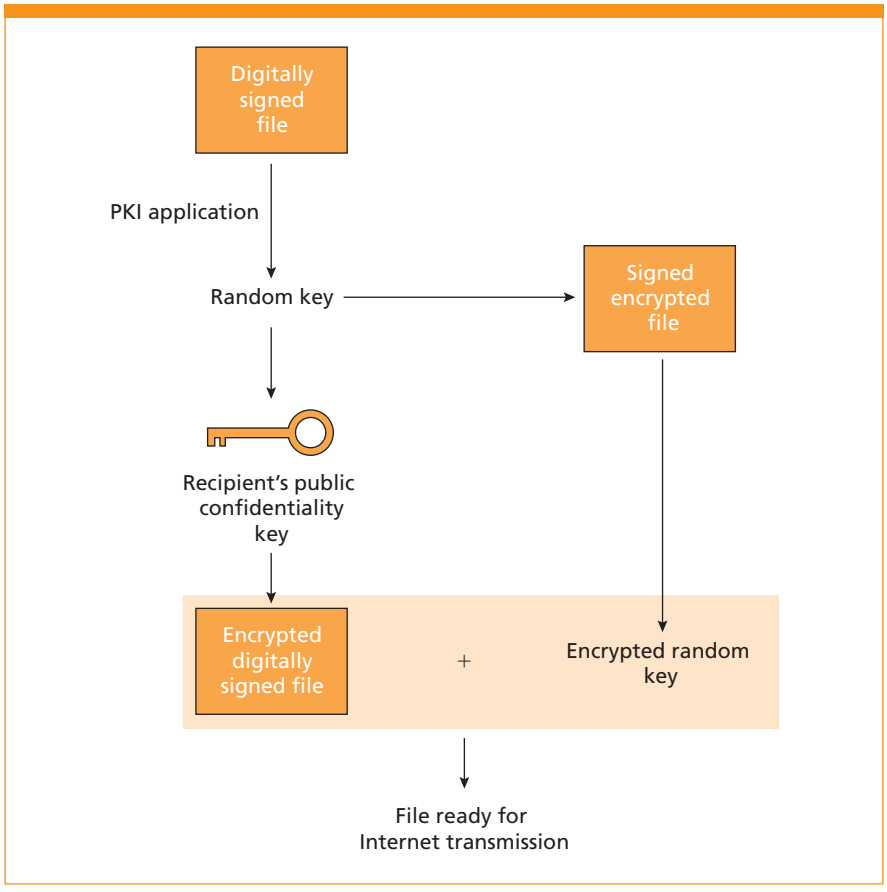

Figure 2: *Encrypting the file for transmission over the Internet.*

Security of the CA/RA

The CA/RA systems are at the heart of any PKI; therefore, the security of these systems is of primary importance. If they are compromised, the whole PKI solution is useless. In particular, the PKI must ensure that the following occur:

- The CA's private key should be held in a tamper-resistant security module with back-up copies available for disaster recovery purposes.
- Access to the CA and RA should be tightly controlled; for example, using smart cards to ensure good user authentication. It should also be possible to configure the certificate management process so that more than one operator is required to authorize certification requests.
- Identification of individuals is also a key security point: what level of identification is required to obtain a key as this is a potential weak point of the whole process?

All certificate requests should be digitally signed by strong cryptographic authentication to detect and prevent hackers from deliberately generating bogus certificates. All significant events performed by the CA/RA system should be recorded in a secure audit trail, whereby each entry is time/date stamped and signed, to ensure that entries cannot be falsified.

Digital Signatures

Digital signatures consist of at least two keys:

- a public key that is made available to all other users
- a private key that must be kept secret.

Dependent on the mode of implementation some applications can give you two public keys and two private ones, other implementations of PKI can involve only a single pair of keys.

For example, Baltimore Technologies' MailSecure is a product that provides four keys, one pair for digital signing and one pair for encrypting documents.

This works as follows for a digital signature:

- a Private Authentication key for generating digital signatures
- a Public Authentication key that other people use to verify the correctness of a digital signature.

Similarly, to ensure confidentiality the following key pair is used:

- a Public Confidentiality key that other

people use to encrypt files they send to other people
- a Private Confidentiality key used to decrypt messages sent to them that have been encrypted.

Creating a Secure File with a Digital Signature

Let's assume that you'd like to send a document or analytical report to a recipient and don't want a third party to have access to it. We'll assume that you have registered with a CA and have the requisites for digital signatures and the appropriate hardware for the operation.

The process is as follows. It is equivalent to signing a letter and provides authentication, message integrity and non-repudiation of the sender:

1. You pass the document through a hashing algorithm; this creates a digest file that is essentially a unique number for this file. If you change anything in the file, the hashing file creates a totally different number. The hashing algorithm will be used to decrypt the file and confirm that nothing has changed since the original encryption and provides the data integrity check.
2. Then you'll encrypt the digest with your private authentication key and this is the equivalent of a digital signature (Figure 1).

Encrypting the File for Internet Transmission

If you want to send the digitally signed file to the recipient over the Internet, you'll follow the procedure outlined in Figure 2.

1. Starting from the digitally signed file, the PKI application generates a random key that is used to encrypt the digitally signed file.
2. The random key is also encrypted using the recipients' public confidentiality key and attached to the file. The file is now ready to send over the Internet to the recipient by e-mail.

Decrypting a Secure File

When the recipient receives your secure, file, they use a similar process (Figure 3):

1. Using their private confidentiality key, the recipient deciphers the file to obtain the signed and encrypted file with the random key. Confidentiality is ensured as only the recipient can receive and decode the file, hence the need to ensure that your private keys remain so.
2. Then, if the random key has been successfully decrypted, the PKI application uses this key to decrypt the file to obtain the file with the digital signature.

Confirming the Signature

After the file has been decrypted, the recipient should check that the signature is correct, this process is shown in Figure 4.

1. The file is passed through the same hashing algorithm used to create the digest originally.
2. The electronic signature is passed through the sender's public authentication key to obtain another digest.
3. The recipient's application should check the digest results; if they don't match then the message has changed since it was sent or it has been forged.
4. When the two digests match exactly then the message is authentic and has the required integrity and the signature is genuine.

The key issue with digital signatures is that to send a secure message using PKI:

1. The sender must have the recipient's public confidentially key so they can encrypt the file.
2. The recipient must have the sender's public authentication key to check the author's digital signature.

This issue must be supported by user verification and infrastructure that provides trust to use the overall approach.

Applicability to the Chromatography Laboratory

Not much in the short term is the easy answer. Most, if not all systems, working in chromatography laboratories today are closed, therefore there is no need to

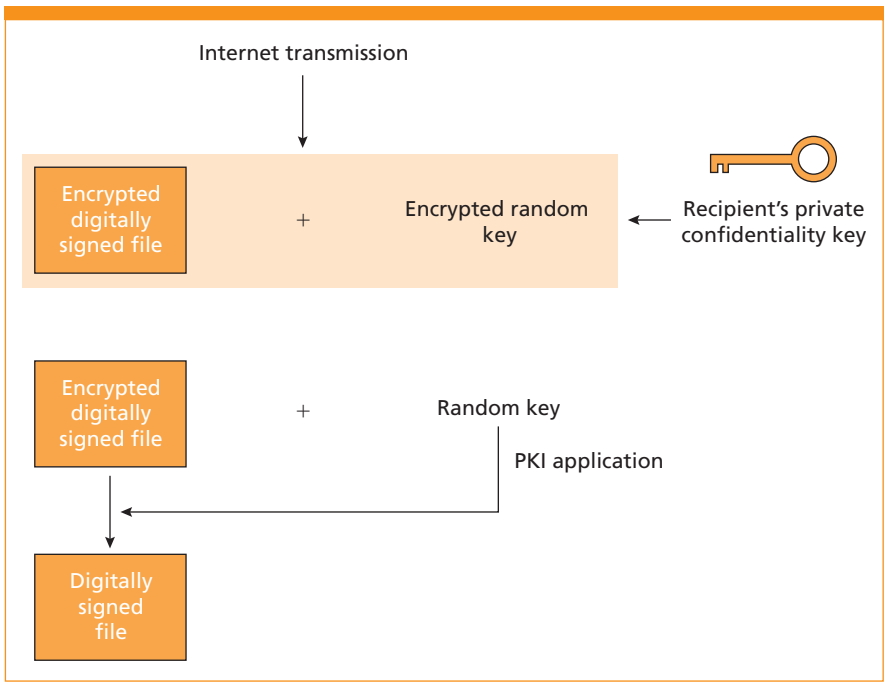

Figure 3: *Decrypting a secure file.*

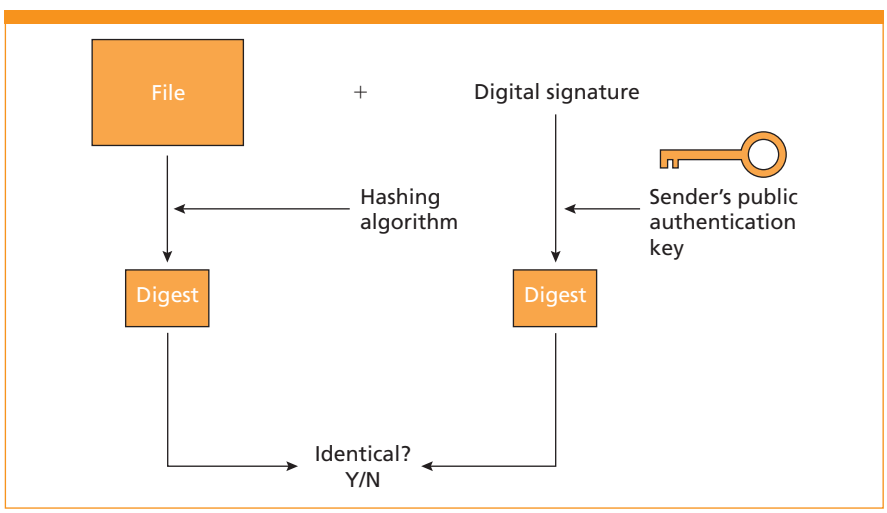

Figure 4: *Verifying the signature.*

employ digital signatures. The situation may change but don't use your dog's name as your password. If you do, don't reveal the fact to reporters — as Bill Clinton did.

References

(1) R.D. McDowall, *LC•GC Europe*, **13**(5), 331–339 (2000).
(2) R.D. McDowall, *LC•GC Europe*, **13**(10), 734–742 (2000).
(3) 21 CFR Part 11, *Electronic Records, Electronic Signatures Final Rule*, Federal Register 62, 13430–13466 (1997).

Bob McDowall is Visiting Research Fellow in the department of Chemistry at the University of Surrey, and Principal of McDowall Consulting, Bromley, Kent, UK. He is also a member of the Editorial Advisory Board of LC•GC Europe.