Electronic Signatures and Logical Security

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

Welcome to "Pharmaceutical File." This is a new column that I'm writing specifically for readers working in the pharmaceutical industry and organizations that supply support services to it, such as contract research organizations. However, the contents should also be of interest to the rest of the readership. You may ask why the name "Pharmaceutical File" was chosen; the simple answer is that the editor and I couldn't think up anything better…

The writing style will be the same as my existing column, "Questions of Quality," and similarly it is intended to make you either agree or disagree with my views. The aim is not to have to sit on the fence but to stimulate your thinking or challenge established practices. As always, I would encourage your feedback and welcome comments regardless of whether you agree or disagree with my views.

What's Hot Today?

The first two columns will be about electronic signatures as this is today's hot topic in the pharmaceutical industry: Electronic Records and Electronic Signatures legislation (1). I discussed an overview of the regulations in the last "Questions of Quality" column (2).

So what are we going to cover in this column? I want to focus more on electronic signatures and give you more information to help you understand, select and implement systems in your organizations. Therefore, we'll discuss the following topics:

- What are electronic signatures?
- Differences between electronic and digital signatures
- Electronic signatures and the link with logical security
- Digital signatures including biometrics (this will be covered in the next column).

In essence, we are looking at the replacement of traditional handwritten signatures by an electronic version for authoring, reviewing and releasing data and information. Therefore, to start our discussion we'll look briefly at over 3000 years of experience and tradition with cellulose (mainly) and a variety of materials used for writing.

Pen and Ink Rule OK?

Back to basics: Normal (traditional?) writing materials are well understood. Take for example the laboratory notebook; it is a relatively robust medium. It is bound, the pages are individually numbered and are relatively robust. For example, you can throw a notebook around the room with little impact on the integrity of the data contained within it (provided you've glued in the additional pages and chromatograms, of course). Don't even think about throwing a computer around the room: from personal experience, I can tell you that dropping a PC onto a concrete floor does not improve its performance significantly (don't even ask). Furthermore, it's easier to remove a drink spilt on a laboratory notebook than one poured onto a computer keyboard (ditto). Also, it's relatively easy to see whether pages have been torn from a numbered laboratory notebook. So much so, that even a lay person can detect this type of tampering.

When you look at a handwritten signature in the laboratory notebook, it is visible and tangible; you may not be able to read it but it's there. The definition of a handwritten signature is shown below and is taken from the Final Rule §11.3 (1).

Handwritten signature: means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

So looking at the latter part of the definition, you'll see that the signature is not necessarily limited to paper. If you have ever signed for a letter sent via some couriers you may have been presented with a stylus and asked to sign on a screen. You'll also find a similar situation with the newer credit card transactions in some stores. Although the act of signing is computerized, the signature is still classified as handwritten and is NOT classed as an electronic signature.

Hybrid Systems

As you may remember from the last "Questions of Quality" column, I mentioned hybrid systems briefly; these systems have a mixture of electronic and paper elements. You could see a situation where an existing chromatography data system incorporated the stylus signing method above to review and authorize results. However, there are drawbacks with this approach as there would be few controls to check the identity of the individual signing the records unless the act was linked with functionality within the chromatography data system software.

Going Electronic?

With the transfer to electronic media, we are moving from an easily understood medium to one that requires a technical background to comprehend fully. Electronic media are less robust (hence the need for back-up and disaster recovery schemes) and the ways to commit fraud are greater with a lower chance of detection (audit trails are one way to monitor changes to monitored data fields and are mandatory under 21 CFR 11).

Therefore, when discussing electronic signatures we need to consider logical security as well. Not convinced? The reason being that controls required for implementation of electronic signatures are derived from the logical security of the operating system, network and/or the application, and failing to understand this area can leave you open to non-compliance issues. Read on and discover….

Electronic and Digital Signatures

Within the *Final Rule* there are two types of signatures defined: electronic signatures and digital signatures. We'll start by looking at the simplest of these, electronic signatures, and then move on to discuss digital signatures in the next column. The use of these two types of signature is usually predicated by the type of computer system used: electronic signatures are the minimum for closed systems and digital signatures are required for open systems (1, 2); although there is nothing in the regulations to stop an organization from implementing digital signatures on a closed system.

Digital signatures have an increased level of security and include additional security elements such as encryption or biometrics.

What are Electronic Signatures?

The definition of an electronic signature in the regulations is presented below (1):

Electronic signature: a computer data compilation of any symbol or series of symbols executed, adopted or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Duh? Fish through the sections of the Final Rule and find §11.200; here all is revealed about what constitutes an electronic signature: a minimum combination of a password and user identity. Note again the use of the word minimum, as the Food and Drug Administration (FDA) considers the requirements in the Final Rule to be a minimum set of requirements.

For the majority of systems used in the laboratory, electronic signatures will be implemented using a combination of user identity and password. There are two reasons for this; first, it is a known technology that can be easily implemented, and second, it is relatively inexpensive compared with digital signatures to implement.

Now we hit an issue — user identities and passwords. You can now see the relationship between electronic signatures and logical security. User identities will usually be derived externally from the computer system; passwords will be generated and guarded within the application, network or operating system. The whole issue of electronic signatures hinges around passwords and their control. Frightening thought eh?

Let's look at logical security in a little more detail…

Logical Security

Logical security deals with the security provided either by an application and/or the operating system software that enables a user to gain access to the application or by a computer system respectively. Within logical security, there is also the issue of access by an individual to some or all functions of an application and the associated data.

Therefore, we'll be able to look further at, and the impact of:

- access to individual systems and/or networks
- access to individual functions
- access to data.

So, if the electronic signature is a unique combination of a user identity and a password, what can go wrong? Come on, if you've been reading and understanding this far, you'll have a good idea!

User Registration

Before obtaining access to a network or application, a user is usually required to register with an administrator. This should be a formal process; usually when an individual first joins an organization. However, how many organizations perform checks on potential employees before they join the company? Normally the references asked for concern the applicant's ability to perform in the new position; however, one or two questions on computer security would be useful to ask at the same time. This is especially important if the individual is to have access to sensitive information during the course of their work with the new employer or is to run a major application or network as the administrator. Commercial information is valuable to the organization that owns it. Unfortunately it is also as valuable to unscrupulous competitors.

A specific requirement of the Final Rule is that the identities of individuals are checked before they can use electronic signatures (§11.100 (b)). So we'll assume that any identity, security and background checks are OK. A new user will then usually complete a form that is countersigned by a line manager before an account and password is issued by a network administrator. Some managers think that this is just a waste of time and consider this as just pushing paper around an organization. Think again. What you are doing is allowing a new user access to your network and you have to comply with the 21 CFR 11 regulations: do you have a policy that everyone has access to all functions and data or are these restricted to a need-to-know basis? Tailoring access to the individual is the best approach to use. This will be an area that you will be inspected on from now on.

For most users there may be the need for training before access to the system can be allowed. This may include the security policies of the organization and password policies. It may also cover the use of floppy disks for working at home and the process of increasing or decreasing the access to applications, functions and data. When an upgrade is installed resulting in the network operating system undergoing a major change, follow-up training may be required, as there may be an impact on security and usability.

A network administrator will need to have a list of current and retired registered users and their levels of security clearance. As an employee leaves or retires, the old account must be removed and retired as well. Similarly, if a user changes or moves positions within the organization should the access levels be changed as well? There must be a list of all user identities so that they are not reused. This is important as the electronic signature must be a unique combination of user identity and password: how can you ensure that passwords are unique without informing somebody that there is another use of the same password on the network?

Some organizations reuse old account numbers after a certain time. Don't. Best practice should ensure that old account identities are never reissued. For example, some organizations use the employee number as the account number, others input a user's name providing that they are unique and others use the official company initials of an individual. This is a good and logical approach for the user name, but someone from the outside who wants to gain access to the organization's files can easily understand it. Thus, this places more importance on the password and the measures necessary to keep it confidential and secure. We'll discuss passwords and their role in logical computer (in)security now.

Passwords and Their Management

Currently, passwords are the main way of checking that you are who you say you are when you log on to a computer system. However, there are several issues that can make this difficult to operate.

Passwords in practice: Let's introduce ourselves to the password paradox. This simply states that a short name used as a password is easier to remember and use, but can be guessed by others. The corollary is a long nonsensical word, especially when it has been computer generated, which is easily forgotten so a user writes it down to avoid forgetting it.

So, what can we do about using passwords? First, individuals must each have their own password. In other words passwords must not be shared. Of course, this never occurs in your organization does it, as this compromises security immediately. Passwords must be kept confidential: no record must be made of the password outside of the computer. The classic story of the password written down on a Post It Note placed next to the PC was exceeded in one organization I visited where the screen had a printed label on the top which said PASSWORD = XXXXXX.

Passwords must be changed regularly and an operating system or application can enforce this every 30, 60 or 90 days if required. Whenever security has been compromised, a password change should be triggered. The problem with this approach is that infrequent users will have the problem of remembering the current password and all users will have problems remembering a new password in the first few days after a change.

I was standing next to a user logging on to a computerized system during one audit I was involved with; out of the corner of my eye, one key was depressed three times to log on to the software. After discussion it turned out that the password entered was AAA, which was the default password delivered with the system over 10 years previously.

Ideally, a good operating system should remember all passwords used by an individual and prevent their reuse. Personally, I used to have two passwords that I alternated with until the operating system decided that this was a bad idea.

So now we turn to the password itself. The length of it should be a minimum of six characters. The next advice is very sound and will probably be ignored by many readers, but you should NOT use as passwords

- days of the week
- months or any other aspect of dates
- family or pet names
- car registration numbers
- birthdays
- telephone numbers.

The rationale for this is that if you know a person you'll be able to access their account by reasoned deduction. Investigations of password security can be depressing reading: in one instance a password-breaking program obtained access to over 60% of accounts in one organization (3). To help the situation, some operating systems have a function preventing a user entering some common variations such as days of the week etc.

A password consisting of either all numbers or all letters should not be used, as one covering both letters and numbers increases the permutations that could be available making it harder to enter a system.

To help increase the number of combinations possible for a password:

- The alphabet can be made case sensitive thus increasing the number of available characters from 26 to 52. This increases by several orders of magnitude the number of different password combinations.
- Adding numbers and special characters can further increase the number of keys used for a password.
- More complexity can be added by linking words to make them longer and therefore more difficult to identify.

This is counterbalanced by the ease of remembering the password as human nature now snatches defeat out of the jaws of victory: we are lazy. Having devised a reasonable password that we can remember, we now lengthen it by adding 1 for January, 2 for February etc. to make it easy to remember. Of course, this never happens in your organization does it?

Further password protection: Having typed your password into the workstation you may be forgiven for thinking that it is now protected. Well, you'd be wrong! The weak link with passwords and any security system is that the password must be stored in the computer for comparison with the entered string. Therefore, the password must never be displayed in human readable format either on the screen or within the system to avoid the password being compromised. As a result, passwords must be encrypted if stored and hidden carefully within the system. The encryption algorithm will still, however, be stored on the computer.

You may think that this is basic stuff and common practice, but during qualification of a computer-controlled system, a colleague found that the password was stored as a text string in the WIN.INI file of the PC. The manufacturer expressed surprise that this was an unacceptable practice.

Application designers must use echo inhibition when entering the password at a terminal or workstation. This is where a keystroke is entered into the PC but not echoed back to the workstation.

This must extend to remote access, especially via the Internet, to ensure the password is protected as securely as a normal network.

Network Access Control

So, you've entered your account identification and you've remembered and typed in your password; now you are in. Welcome to Windows or UNIX or whatever operating system you use. Can we do anything and everything or is there access control to various functions? Here's where the network administrator or the Information Technology (IT) department can help by tailoring the access control.

Limit Network Access

Increasingly, network administrators are restricting access rights of users to all functions available in a network. For example, one organization eliminates the Microsoft games from the portable PCs for employees. Another organization only allows users to have access to common office applications and those business functions directly needed to perform their job function. Moreover, the use of the Windows Explorer function is restricted to their shared and application drives.

As a user gains access to the network, there is, therefore, an enforced path that reflects the privileges requested during the user registration process. This approach means that there is a lower risk associated with a user having unrestricted access to all functions. It also avoids the situation

Table 1: Continuum of User Privileges.

Access privilege	Access rights
Zero-level	No access rights or access denied
Execute only	User can execute functions accessed but nothing else
Read only	User can only read the data accessed but cannot write or append anything
Write only	User can overwrite data
Read–write	User can read or write as required
Append only	User cannot change any data but can add additional information
Administrator	Full access rights to create, read, write, copy and delete data

whereby an authorized user may blunder into an area and cause disruption to applications and/or data.

At a lower level in the network design, this approach may be enforced by the physical components of the network. The use of network segmentation, where a department or user community only has access to its own, is one way to enforce limited network access.

There are other approaches to logical security of the network:

- Identification of terminals: where a function must be performed in a specific place and the terminal has a network address that confirms that the task is completed in the correct location.
- Use of time-outs for logging users off their workstation if no activity has been detected for a predefined period. The user then has to log in again to continue their work.
- User re-authentication where at key stages of work a user is prompted to re-enter their password (see after). This is not to be confused with the use of electronic signatures.

Re-authentication of User ID

Part of making computer environments secure is the re-authentication of user identity, whereby the user is prompted to re-enter their password at key stages, such as:

- when attempting to use a function not usually privileged to all users
- when requesting to access a highly classified program or file
- when requesting a service deemed excessive in a particular environment (e.g., heavy download of files from an intranet over a long period of time).

This feature would be used in addition to some of the other logical security features discussed above.

Monitoring Unauthorized Access

Usually an operating system will allow a user three attempts to gain access; three being a balance between a non-tolerant (one attempt only) and a hacker's paradise (unlimited attempts) system. To be effective the person should be logged off the system after three attempts. There is then a delay before the user can log on. If the user fails again there will be a longer delay before a new attempt can be made again. If this happens to a specific user several times, it may be a symptom that more training is required or a possible security breach.

Note there are specific requirements under the 21 CFR 11 regulations, where unauthorized attempts to log on to a system must be reported immediately to an administrator or system owner (§11.300(d)). This requirement may be difficult to comply with if the system is a stand-alone workstation!

Most operating systems have the ability to monitor and record all attempted log-ins including failures. Thus, the attempts described above will be monitored and recorded in a log. These logs, ideally permanent ones made on CD write-only disks to prevent unauthorized tampering, should be monitored regularly to see whether discontinued accounts and user identities have been used or unusual events have occurred on the network. Unusual events on a network are typified as:

- abnormal termination of an application
- abnormal system failure
- failure of a software security mechanism
- unsuccessful attempts to log on to the system or network
- attempts at unauthorized access to files or applications
- attempts to use privileged instructions improperly.

Again these events need to be investigated to detect any potential breaches of security and to make the appropriate changes.

Application Security

OK, you've got into the network and now require access to the necessary application (at last!); this may require a second user identification and password, or the enforced path from the network will direct you to the appropriate application and you'll enter directly. Accessing the application you'll find another level of access control features that will allow the application administrator to define access of classes of users or individuals to different functions. Access to all systems but especially business critical ones must be defined in writing.

There are three main areas of security we'll discuss about applications, these are

- access privileges
- access by function
- security models.

Each will be discussed below; however, the principles described are also applicable to network security as well.

User Privileges

Any discussion on logical security of an application should first consider what each user could do when they use any function. These are the privileges associated with the user of a function within an application. This has a continuum that ranges from the ability to undertake any function to being denied access. These privileges are shown in Table 1 and are intended to be general. This continuum may need to be tailored to any application in practice. For instance you may decide that an execute-only function and a read-and-write function are so similar that in practice combining them makes sense. Alternatively, the privilege may not be implemented in the application you have purchased or developed.

Mapping User Privilege to Application Function

Once the user privilege continuum has been decided upon it must be mapped to job functions. In this example we'll use just four levels:

- zero-level (denied)
- read only
- read–write
- administrator (create, read, write, copy and delete).

Again in our example we'll have four jobs that will be considered within the application:

- trainee
- user
- supervisor
- system administrator.

Table 2: Access by User Types to Individual Functions within an Application.

User type	Function 1	Function 2	Function 3	Function 4
Trainee	Denied	Read	Read	Read
User	Denied	Read/write	Read/write	Read/write
Supervisor	Read only	Read/write	Create/read/copy write/delete	Read/write
System administrator	Create/read/copy write/delete	Create/read/copy write/delete	Create/read/copy write/delete	Create/read/copy write/delete

The approach taken here is that we will implement the minimal privileges required consistent with being able to perform the job effectively. In our application there are four functions: it's a simple application!

The mapping of user privilege to application function is shown in Table 2. The trainee has read-only access to three functions, thus reducing the possibility of accidental data corruption. This can wait until the user is 'competent'! As a user becomes more experienced they will gain access to more functions, together with greater access privileges. However, if you look at function 1, only the system administrator has full access to this function as it may be associated with data security or access rights.

The system administrator should review access rights of individuals regularly especially as they are trained or are promoted. This should be reflected in a change of user privilege. However, this may be difficult to implement in some applications because the security system may not allow this approach.

Security Models

There are two main types of security models possible in applications. Legacy systems tend to have a hierarchical security model and newer applications have a class model. Regardless of approach, the security profiles of each user will be kept by the system; best practice is also to document this outside of the system.

The hierarchical security approach is based on a tier of users whereby individuals can see everything that peers can see as well as those functions in the tiers below them, but do not have access to the functions in the tiers above them. Thus, the system administrator can see everything. This is shown in Figure 1 and is similar to an organizational chart. Each user will be able to see what the other users may be doing and have access to their data as well as their own. From this perspective it is not ideal but is better than no application security.

The class approach is more flexible and can be tailored to individual users. You'll have the same user types but each profile can be different. Again using Figure 1 and considering the two trainees; both will have the same profile as shown in Table 2. However, during their training one user is seen to be more proficient compared with the second. Under a class security system, the access profile of the more proficient trainee can be updated so that he or she can have read–write access to, say, function 2 without altering the access profile of the second trainee. This approach allows a dynamic modification of a user profile relatively easily.

Role of Management

Although this topic has been left until last, it is essential that the role of management in computer security be discussed because of its importance.

In short, senior management must take the lead in computer security. They are responsible for running the business and thus must also be responsible for ensuring the business is protected from loss of confidential or important data and computer services. This is not just an information technology issue. It affects everyone in the organization. Unfortunately, you can see the eyes of too many managers glaze over when you mention the word "computers" and they pretend not to understand. "It's not my responsibility," is the common view, "go and see IT." This is an appalling viewpoint and a total abdication of responsibility.

There are responsibilities that management should undertake with respect to computer security:

- To understand the problems associated with computer security. This provides the basis for the other roles of management.
- To provide visible and vocal support for computer security. This provides the environment in which computer security can be sold to the user community and guidance given effectively. Without this there is little point in IT trying to provide security as local management will override their efforts.
- To plan for appropriate computer security responses based on business drivers and an evaluation of risks facing the business. For instance, if you are responsible for a stand-alone computer application that is not networked and is not linked to other applications in the organization, then the security requirements are a lot less compared with an application that runs partly over the Internet.

Training of Users

For computer security measures to be effective, the users involved in implementing them must be trained. This training will need to cover full-time, temporary/part-time and contract staff that use computers in your organization. It may also need to cover service and maintenance engineers undertaking repairs to computerized equipment or applications. Furthermore, as technology provides the means to access applications remotely via modem, special arrangements may be necessary to minimize the impact that it can have, especially in a regulated environment.

The training will involve using the security measures, such as passwords and their maintenance, but also general awareness of computer security issues. For example:

- users authorized to access systems and networks
- the need for users to report problems with software: both bugs and errors, and possible breaches of security
- documented ways of working.

Regulatory Sticks

Of course some of you reading this may be thinking that this is over the top and is far too much work. Let me assure you that it's not, as this is where the FDA inspectors are looking closely. For example, 483 Observations of a client/server chromatography data system in a bulk pharmaceutical manufacturer in December 1999 (3) stated:

Access control issues: "Programmable switches, which could be turned on or off

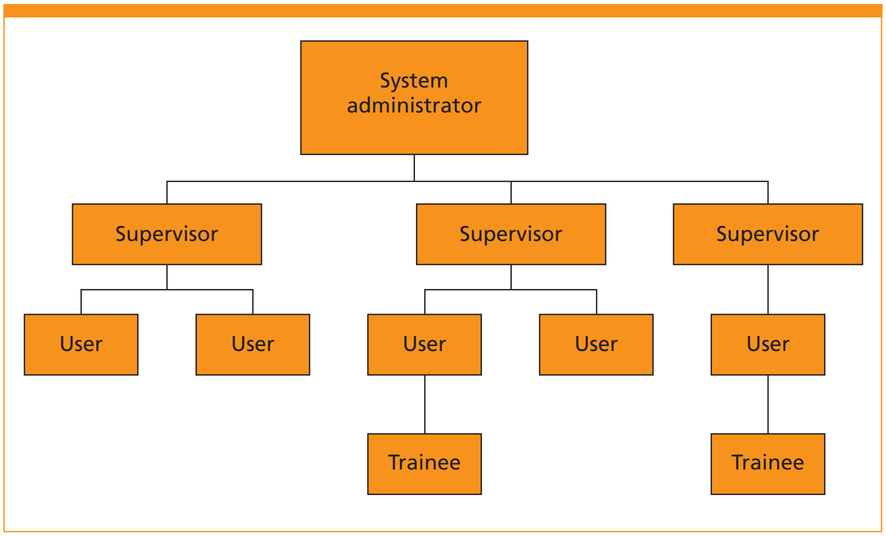

Figure 1: *Hierarchical and class security.*

without record or documentation was available in the QC network system, which could circumvent system and data integrity. The system administrator and each analyst had access privileges that enabled or disabled switches for the system configuration editor, editing permissions for fields and commands, and system menu functions. The firm did not have sufficient security controls in place to prevent analysts from submitting edited or modified data."

More access control issues: "Programmable functions which could be chosen without record or documentation was available in the QC network system that could circumvent system and data integrity. These functions were not only available to the system administrator but also to each analyst and included read–write access, delete and purge data, modify and rename a data file, overwrite a data file, and copy and rename files. The File Menu was also available to users and allowed each analyst to open, replace, close and copy one or more chromatograms for use in new or renamed applications. Analyst had access to all database files on the server."

Third time unlucky: "The operating system was not configured to prevent analysts from accessing the "Permissions" that control which directories and files a user or group can access. Analyst could bypass the menu security features in the Windows environment and access all programs, including DOS prompt, autoexec.bat and config.sys, through the taskbar. There were no restrictions on who could create, rename or delete data."

And the icing on the password cake: "The client/server password system failed to adequately ensure system and data integrity in that passwords never expired and could consist of four characters. Once an analyst initiated data acquisition, anyone could access the system. System configuration did not allow for the unattended operation of an instrument in a secure mode during processing and collection of chromatographic and electrophoretic data."

Still not convinced?

Mutual Recognition Agreements (MRA)

Those readers working in the pharmaceutical industry who are not subject to inspections by FDA are probably having a good laugh at the other poor souls who will have to jump through hoops to implement this regulation. Hold on a minute, there is MRA coming your way. Part of the harmonization work that has been going on for the past 10 years is the acceptance of one regulatory agency of inspections by another; for example, FDA would accept an inspection report by the UK Medicines Control Agency (MCA) inspectors.

We are currently about halfway though the three-year MRA evaluation period during which observers from the US and Japanese authorities are looking at approaches of inspectors in the various European countries. Given that there is no corresponding electronic signatures and electronic records regulation in Europe, guess which way the European agencies will go if they want to sign an MRA with FDA?

References

(1) Electronic Records, Electronic Signatures Final Rule, Federal Register, (available on www.fda.gov).

(2) R.D. McDowall, *LC•GC Europe*, **13**(2), 79–86.

(3) 483 Observations, Ganes Chemical Company, December 1999; (available from FDA under the Freedom of Information Act).

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.