



# Meeting the FDA’s Requirements for Electronic Records and Electronic Signatures (21 CFR Part 11)

- Executive Summary..... 3
- Background ..... 4
  - Internet Growth in the Pharmaceutical Industries..... 4
  - The Need for Security..... 4
  - PKI is the Answer ..... 4
- Overview of 21 CFR Part 11..... 5
- Addressing the Requirements of 21 CFR Part 11 ..... 5
  - Subpart B – Electronic Records ..... 5
    - Section 11.10 Controls for Closed Systems ..... 5
    - Section 11.30 Controls for Open Systems ..... 9
    - Section 11.50 Signature Manifestations..... 10
    - Section 11.70 Signature/Record Linking ..... 10
  - Subpart C – Electronic Signatures ..... 11
    - Section 11.100 General Requirements ..... 11
    - Section 11.200 Electronic Signature Components and Controls ..... 12
    - Section 11.300 Controls for Identification Codes/Passwords ..... 13
- Summary..... 14



This white paper provides a brief introduction to 21 CFR Part 11 and discusses the requirements of the rule in the context of Xcert's Sentry PKI solution. Although this paper contains Xcert's views on and interpretation of certain aspects of the rule, this white paper is for general information purposes only. It does not contain or constitute legal or other advice. Xcert expressly disclaims any and all liability for the statements set forth in this white paper and any reliance thereon. Xcert encourages all readers and persons interested in the legal aspects of 21 CFR Part 11 to seek competent legal counsel for advice regarding compliance with this rule. For further information about Xcert's PKI solution as it relates to 21 CFR Part 11, please contact Xcert at 800-721-9191 or 925-274-9300.



## Executive Summary

Companies in the pharmaceutical industries are increasingly using the Internet to create new on-line services, reduce paper-handling costs, and provide more efficient access to data.

Pharmaceutical companies that rely on the Internet for electronic information exchange need robust security to maintain trust, to protect an organization from liability, and to comply with regulations such as the U.S. Food and Drug (FDA) Administration's 21 Code of Federal Regulations (CFR), Part 11, concerning electronic records and electronic signatures. Public Key Infrastructure (PKI) meets market and regulatory requirements for securing electronic information in the pharmaceutical industry.

21 Code of Federal Regulations Part 11 has been in effect since August 1997 and establishes the FDA's requirements for electronic records and electronic signatures to be trustworthy, reliable, and essentially equivalent to paper records and handwritten signatures. The driving force in its creation was to prevent fraud while permitting the widest possible use of electronic technology to reduce costs incurred from paper processes.

Xcert's PKI solution addresses the FDA's requirements for electronic records and electronic signatures (21 CFR Part 11) including the controls for closed and open systems, signature manifestations, signature/record linking, electronic signatures in general, electronic signature components and controls, and controls for identification codes/passwords.



## Background

### Internet Growth in the Pharmaceutical Industries

Companies in the pharmaceutical industries are increasingly using the Internet to create new on-line services, reduce paper-handling costs, and provide more efficient access to data.

Internet applications in these industries are wide ranging and include using e-mail for research collaboration projects or for communication during clinical trials. Web servers are also used to store and access information like test and lab results. More and more prescription fulfillment is moving on-line. Important tele-health applications are also beginning to emerge, including remote monitoring of patients via medical devices connected to the Internet.

These types of applications reduce cost, time, and complexity over traditional processes. Competitive pharmaceutical companies are moving quickly to harness these benefits. At the same time, these companies need to ensure this sensitive data is secure to meet market and regulatory requirements.

### The Need for Security

The Internet is a public network and, as such, needs higher security measures to ensure that only authorized users are able to access or receive the information that was intended for them. Pharmaceutical companies that rely on the Internet for electronic information exchange need robust security for several important reasons:

- To maintain the trust of customers and business partners while building the competitive advantage that the Internet brings,
- To mitigate the risk of litigation from accidental or unauthorized information disclosure, and to protect an organization from liability, and
- To comply with regulations such as the U.S. Food and Drug Administration's 21 Code of Federal Regulations (CFR), Part 11, concerning electronic records and electronic signatures.

### PKI is the Answer

Public Key Infrastructure meets market and regulatory requirements for securing electronic information in the pharmaceutical industry.

PKI is a system that uses digital key pairs, digital certificates and digital signatures to identify and trust users on a network. Digital key pairs (public and private) are used for encrypting and decrypting information. Private keys are used to generate and attach a digital signature. Public keys are used to verify that signature. Digital certificates are used as proof of identity.



The main components are a Certificate Authority (CA), Registration Authority (RA), and PKI-aware applications. Establishing a PKI also involves developing a Certificate Policy and Certificate Practices Statement. For more detailed information, please reference Xcert's "A Practical Guide to PKI" which can be obtained at [www.xcert.com](http://www.xcert.com).

## Overview of 21 CFR Part 11

21 Code of Federal Regulations Part 11 has been in effect since August 1997 and establishes the FDA's requirements for electronic records and electronic signatures to be trustworthy, reliable, and essentially equivalent to paper records and handwritten signatures. The driving force in its creation was to prevent fraud while permitting the widest possible use of electronic technology to reduce costs incurred from paper processes.

The rule contains two major sections: one that addresses requirements for electronic records and one for electronic signatures. Electronic records are defined as "any combination of text, graphics, data, audio, pictorial, or other information in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system." The rules apply to any records covered by FDA regulations that exist in an electronic form – including records that are required to be maintained whether they are submitted to the FDA or not. Electronic signatures are defined as "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." The determination of whether to use an electronic signature is up to an individual organization.

The use of electronic records and their submission to the FDA is voluntary. Also, if there is no FDA requirement that a document or record be created or maintained, then 21 CFR Part 11 does not apply. It is important to note that the regulations represent minimum requirements for implementation, but organizations can choose to make their systems more secure if they choose.

## Addressing the Requirements of 21 CFR Part 11

Xcert Sentry addresses the requirements of 21 Code of Federal Regulations Part 11. The following sections outline the FDA's requirements and how Sentry addresses each requirement.

### Subpart B – Electronic Records

#### Section 11.10 Controls for Closed Systems

This section outlines controls that must be in place for "closed systems," or an environment in which system access is controlled by the persons that are



responsible for the content of the electronic records that are on the system. An example of a closed system would be an information system that is contained within an organization's local area network or Intranet.

These controls require that "Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine."

The following are the specific requirements of Section 11.10 and how Xcert addresses the requirements:

(a) **Requirement:** Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

- Xcert Sentry is a system for issuing, managing, and verifying digital certificates and provides for the use of authorized digital certificates and digital signatures with applications such as e-mail, web access and electronic records management. In deploying Xcert's PKI solution, an organization implements policies and procedures that include a periodic audit to ensure accuracy, reliability and consistent intended performance. Xcert can assist in the development of the policies and procedures. Xcert Sentry provides logging of all PKI events to be used for auditing purposes. The use of a cryptographically based digital signature guarantees the integrity of data. For the user, signing a record may be as simple as selecting an "attach signature" option within an application; the technical process uses the user's private key to encrypt a hash (electronic fingerprint) of the record and the resulting digital signature is attached. The reader or recipient of the data verifies the signature, determining immediately if the data has been altered. PKI-aware applications will return a message regarding the verification of the signature. For verification, the technical process uses the originator's public key to decrypt the hash of the record, and then a hash of the record is compared to the decrypted hash to ensure that it is the same. This provides the ability to discern invalid or altered records.

(b) **Requirement:** The ability to generate accurate and complete copies of records in both human readable and electronic form.

- This is again related to the use of cryptographically based digital signatures that provide assurance that signed records are accurate and complete. A digital signature involves using a private key to encrypt a hash (electronic fingerprint) of the data. The resulting digital signature is attached to the data. The reader or recipient of the data uses the originator's public key to decrypt the data and can determine immediately if the data is accurate and complete by verifying the signature. Verification ensures that a hash of the data is the same as the decrypted hash of the data. In other words, it ensures that the record being viewed is the exact record that was signed.



- Generating a copy of the record in human-readable form is application-dependent and would involve the displaying the record in a user-friendly format on the screen or printing the record.
- (c) **Requirement:** Protection of records to enable their accurate and ready retrieval throughout the records retention period.
- Using Xcert's PKI solution, organizations can protect records using access control or encryption. For example, in order to gain access to a record on a web site, the user must present a valid digital certificate and have access rights to that particular record. Access rights are defined using Sentry's Access Control Lists (ACLs). With encryption, a user uses the recipients' public key to encrypt the data, so that only the intended user will be able to gain access to the data by using their private encryption key to decrypt the data. In this way, organizations can protect records and enable accurate and ready retrieval only by authorized individuals. For records that are stored in an encrypted format, Xcert provides a way to retrieve these records, even if these records have been in long-term storage. The Sentry Key Recovery Module can securely recover private encryption keys. This permits ready access to data, not only after the original users involved have left an organization, but also if a private encryption key is accidentally destroyed or lost. (For security and to ensure non-repudiation, Sentry's key escrow system does not back-up or recover private keys used for signing, only private keys used for encryption. Signing keys are tightly held by the owner and not accessible by others.)
- (d) **Requirement:** Limiting system access to authorized individuals.
- Related to the above discussion, organizations can limit system access to authorized individuals by using Sentry's digital certificates and ACLs. Digital certificates provided by Sentry uniquely identify the individuals in the system. In order to gain access to a record, the user must present a valid digital certificate and have access rights to that particular record. Access rules are defined using Sentry's Access Control Lists (ACLs) including read and write privileges.
- (e) **Requirement:** Use of secure, computer-generated, time-stamped audit trails.
- Sentry records and securely logs all PKI events including the identity of the individual performing the action. These logs are configurable, time-stamped, and signed by an authority (e.g., with the CA's private key). Access to these logs is strictly limited to system administrators.
- (f) **Requirement:** Use of operational system checks to enforce permitted sequencing of steps and events.
- Operational system checks are generally specific to organizations and application-dependent. In deploying an Xcert PKI solution, an organization must establish and enforce procedures and policies. Xcert can assist in establishing the procedures; it is up to the organization to enforce these.



(g) **Requirement:** Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

- Xcert Sentry supports the use of authority checks to ensure only authorized individuals use the system and sign records, etc. Every time a user presents a digital certificate for authentication or uses a digital signature to sign a record, the system can determine that it is an authorized individual by checking the certificate status and access rights. If the certificate has been revoked or if the rights have not been granted, the individual is denied access or signing privileges.

(h) **Requirement:** Use of device checks to determine the validity of the source of data input or operational instruction.

- For device checks, Xcert Sentry issues certificates to devices. Device certificates are used to authenticate a device to determine the validity of the source of data input (e.g., a Sentry CA server must have a certificate to authenticate itself when making a query to Sentry's database) or operational instruction (e.g., a Sentry CA server must have a certificate to authenticate itself when issuing a certificate to an enrollment server).

(i) **Requirement:** Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned task.

- For education and training, Xcert provides online and printed documentation and comprehensive training courses for administrators and operators on how to develop, maintain and operate a digital certificate/digital signature system. As part of deploying Xcert's PKI solution, Xcert can help organizations develop a Certificate Policy which is made available to all administrators, operators, and users of the system to educate them on security procedures and using their digital certificate and signature. For end users within the PKI, there is no Xcert client software for enrolling or using digital certificates within applications. Xcert solutions do not require proprietary client-side software but instead use PKI-aware software such as web browsers, e-mail, VPN and SSO clients. This design means there is minimal training required for end users, since end users are already familiar with the software on their desktop.

(j) **Requirement:** The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures.

- Written policies regarding digital certificate issuance, use, and management are defined in an organization's Certificate Policy. This document defines appropriate certificate usage as well as liability for any misuse of a certificate. Additionally, to ensure that certificate holders are accountable and responsible for their actions, organizations develop a subscriber's agreement, which outlines the terms and



conditions for acceptable use of a certificate. Xcert can provide assistance in developing these documents.

(k) **Requirement:** Use of appropriate controls over systems documentation.

- Online system documentation for Sentry is restricted to authorized individuals with a valid digital certificate and access privileges. Controlling access to hard copy documentation can be handled by organizational policies that govern access to these resources.

### Section 11.30 Controls for Open Systems

This section outlines controls that must be in place for “open systems,” or an environment that is not controlled by persons who are responsible for the content of electronic records that are on the system. A good example of an open system is the Internet.

**Requirement:** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and confidentiality of electronic records from the point of their creation to the point of receipt, including those identified in section 11.10, and as appropriate, additional measures such as encryption and digital signature standards.

- A security system built with Xcert Sentry provides user authentication, data integrity and confidentiality, and enables the attachment of digital signatures to messages or records. These requirements are met as follows:

*Authentication:* Sentry issues each user a digital certificate; their identity is bound to their certificate and endorsed by a trusted organization. A digital certificate is used to authenticate users. Any person or application that relies on that certificate, to allow access to information or use of a signature, can verify the identity of the certificate holder, the status and validity of the certificate.

*Integrity:* Xcert's PKI solution supports the use of digital signatures – the technical process of signing uses the signer's private signing key to encrypt a hash (electronic fingerprint) of a record. By verifying the signature, another user can validate that the record originated from a specific user (since only their unique public key could decrypt the signature) and that the record has not been altered (since the hash of the data must be exactly the same as the hash of the decrypted data).

*Confidentiality:* Xcert's PKI solution employs a public/private key pair for encryption so that Sentry can assure that only intended recipients or viewers are able to read a specific record or message. The record is encrypted by the originator with recipient's public key and decrypted by the recipient with the recipient's private key.



*Digital Signatures:* Sentry gives each user a unique private signing key that allows them to create and apply a digital signature. Not only is the signature unique to the user, it is unique to that instance of the record since the digital signature encompasses the record itself.

## Section 11.50 Signature Manifestations

This section requires signature manifestations to contain information associated with the signing of electronic records.

**Requirement:** Signed electronic records must contain information associated with the signing that indicates the printed name of the signer, the date and time of the signing, and the meaning associated with the signature (such as review, approval, responsibility or authorship).

- In accordance with the X.509 industry standard, Sentry issues digital certificates that contain the name of the certificate owner. Encapsulating the date and time of a signing event is application-dependent. By conforming to the industry standards for the Internet and PKI technology, Sentry is compatible with applications that support the use of a digital signatures containing the date and time of the signing, such as email programs like Microsoft Outlook and Netscape Messenger. Xcert can also provide tools and expertise to integrate this functionality with custom applications. Encompassing the meaning of the signature for each signing event would be application-specific and event-dependent; Xcert can provide tools and expertise to build in this functionality. Depending on the organizations' requirements however, it may issue multiple digital certificates to an individual user and each certificate can be associated with a different role, such as review or approval. With each signing, a particular certificate could be used to indicate the meaning.

## Section 11.70 Signature/Record Linking

This section specifies a requirement that signatures be linked with records and that the signature cannot be removed from the record.

**Requirement:** Electronic signatures and handwritten signatures applied to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be removed, copied, or transferred to falsify an electronic record.

- Xcert's PKI solution uses cryptographically based digital signatures which link a digital signature to the electronic record by incorporating that instance of the record into the signature itself. This protects data integrity and is a safeguard to prevent falsification of a record. Another safeguard is to develop strict access control rules so that only the users with a real business need can access a record, so the risk of falsification is reduced. Technical measures alone will not prevent falsification of records. In deploying a digital certificate/digital signature



system for use with electronic records an organization must develop policies and procedures to prevent falsification of the records. Xcert can provide assistance in developing the policy and procedures.

## Subpart C – Electronic Signatures

### Section 11.100 General Requirements

The section specifies general requirements for digital signatures.

(a) **Requirement:** Each electronic signature will be unique to an individual and should not be reused by, or assigned to, another individual.

Each digital certificate created by Sentry contains a unique serial number and DN (distinguished name) as specified by the X.509 certificate and X.500 directory standards. The private key used to generate the digital signature associated with a user's certificate is known only to the user, and no one else can create a signature using this key. This private key can be password-protected or stored on a smart card to provide greater assurance that no one else has access to it.

(b) **Requirement:** Before an organization establishes, assigns or certifies an individual's electronic signature, the organization shall verify the identity of the individual.

- Sentry provides an enrollment process whereby users request a certificate; administrators vet their requests and issue a digital certificate only after approval. Sentry can support any vetting policy. For example, the process could be automated whereby the user's name is checked against a pre-authorized employee database, or an "out-of-band" mechanism could be used whereby a telephone call is made to verify the identity. The chosen method is determined by an organization to fit its own policies and procedures.

**Requirement:** Persons using electronic signatures shall certify to the FDA that they are using electronic signatures intended to be the legally binding equivalent of a traditional handwritten signatures, and may be required to provide additional certification that a given electronic signature is the equivalent of the signer's handwritten signature.

- With Xcert Sentry, a list of all digital certificate holders can be generated. This provides a method for providing the FDA with a list of the population of users at an organization that will be using digital signatures.



## Section 11.200 Electronic Signature Components and Controls

This section outlines requirements for electronic signatures not based on the use of biometrics, which would include cryptographically based signatures created by Xcert Sentry.

(1) **Requirement:** Electronic signatures not based upon biometrics should employ two distinct identification components such as an identification code and password.

- The digital certificate created by Sentry represents a unique identification component for each user. This certificate is password-protected to ensure that no one but its owner can access it and create an electronic signature. For higher assurance Xcert recommends storing the digital certificate on a hardware token or smart card.

(i) **Requirement:** When executing a series of signings during a continuous period, the first signing should be executed using all signature components and subsequent signings at least one signature component.

- When using a password-protected digital certificate at the start of a continuous session, both the certificate (which may be on a smart card) and the password are required. For subsequent signings the system could be set up so that only the password was needed.

(ii) **Requirement:** When an individual executes one or more signings not performed during a continuous period, each signing should be executed using all of the electronic signature components.

- An application that uses a password-protected digital certificate/signature can be configured to “time-out” after a pre-determined length of time of non-activity. Xcert has “forced log-out” capabilities and can provide the tools and expertise to implement this functionality into custom applications. In the case of an application that has “timed-out” the user would be required to present their certificate and enter in their password again to gain access to the system or create a digital signature.

(2) **Requirement:** Electronic signatures shall be used by their genuine owners, and be administered so that attempted use of an individual signature by anyone other than its genuine owner requires collaboration of two or more individuals.

- Sentry is designed so that there is no central storage of the private keys used by individuals to create their unique digital signatures. Private keys are held only by their owner, stored on their own computer hard drive or a smart card. This distributed system ensures that no one has access to a digital signature except the rightful owner.



## Section 11.300 Controls for Identification Codes/Passwords

This section covers controls that must be in place to ensure security and integrity when using electronic signatures based on identification codes and passwords.

**Requirement:** Persons who use electronic signatures based upon identification codes and passwords should employ controls to ensure their security and integrity. These controls should include the following:

- (a) Maintain the uniqueness of each combined identification code and password to avoid duplication of the same combination of identification code and password.
  - (b) Ensure that identification code and password issuance are periodically checked, revoked, or revised.
  - (c) Follow loss management procedures to electronically deauthorize lost, stolen, or compromised tokens, cards, and other devices that bear or generate identification code and password information, and provide for the issuance of temporary or permanent replacements using suitable, rigorous controls.
  - (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report attempts at misuse.
  - (e) Initial and periodic testing of devices that bear or generate identification code or password information to ensure they function properly and have not been altered.
- Sentry addresses the requirements above in the following ways:
    - (a) Each digital certificate issued by Sentry is unique from all others through the use of a distinct serial number, distinguished name, and unique private/public key pair.
    - (b) Certificates can be set to automatically expire after a pre-determined amount of time. Sentry allows for a certificate to be revoked at any time by an authorized system administrator. Certificate status is also checked each time a certificate is presented to ensure it has not been revoked.
    - (c) Sentry allows for a certificate to be revoked at any time by an authorized Sentry system administrator. This revocation can be done in real-time to ensure that reliant applications or users are aware that the certificate is no longer valid. In the event of loss, new certificates can be issued immediately as a replacement.
    - (d) Certificates that have been revoked are no longer valid and cannot be used for authentication or signing. Sentry checks the status of a certificate by reading a Certificate Revocation List (CRL) or by looking it up in the certificate repository directly using Xcert's real-time online certificate status protocol (OCSP). A revoked certificate will be rejected by an application,



preventing unauthorized use. Sentry logs each certificate status query; these logs can be used in detecting and reporting an attempted misuse of a certificate.

- (e) When used with hardware security modules, Sentry meets FIPS 140 certification. This certification guarantees that Sentry's keys and certificates are virtually tamper-proof.

## Summary

The growth of the Internet has brought both opportunities and challenges to the pharmaceutical and medical instruments industries. The opportunity to cut costs and reduce dependency on paper processes is of enormous benefit. However, taking advantage of these efficiencies poses a security challenge as sensitive information is transferred and stored on the public Internet. PKI is a robust and cost-effective security technology to ensure that this information is secure and being accessed only by authorized individuals.

21 CFR Part 11 is a key regulation that pharmaceutical companies need to conform to if they wish to take advantage of electronic records and electronic signatures. The regulations seek to reduce fraud while ensuring that electronic signatures and records are as reliable as their traditional paper versions. Xcert Sentry is a solution that allows companies to closely adhere to these regulations. Sentry can issue unique digital certificates to an organization's users to provide strong authentication and access control and allow users to generate unique digital signatures.

###

Xcert, Xcert Sentry CA, Xcert Sentry RA, Xcert WebSentry, Xcert Sentry Key Recovery Module, Xcert Sentry OCSP++, OpenXchange, Xcertified and the phrase "Enabling Secure E-Business" are trademarks of Xcert International, Inc. All other product names referenced herein are the property of their respective companies.