21 CFR Part 11

Meeting the FDA's requirements for electronic records and electronic signatures used in the pharmaceutical industry

This white paper provides a brief introduction to 21 CFR Part 11 and discusses the requirements of the rule in the context of RSA Security's solutions. Although this paper contains RSA Security'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. RSA Security expressly disclaims any and all liability for the statements set forth in this white paper and any reliance thereon. RSA Security 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 RSA Security's solutions as they relate to 21 CFR Part 11, please contact RSA Security at 781.515.5000.

RSA SECURITY®

Table of Contents

I. Executive Summary

The pharmaceutical industry is increasingly using electronic information systems to improve efficiency of operations. One of the major initiatives is to move to a paperless environment and thereby significantly reduce costs. At the same time, major forces based on market demands and regulations, are calling for developing enhanced security policies and practices in order to protect electronic information.

21 Code of Federal Regulations (CFR) Part 11 establishes the U.S. Food and Drug Administration's (FDA) requirements for electronic records and electronic signatures to be trustworthy, reliable and essentially equivalent to paper records and handwritten signatures.

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. Under 21 CFR Part 11, electronic signatures are broadly defined and therefore can be based on various authentication technologies including everything from user ID and password to cryptographically based digital signatures, as long as the specific requirements and controls for electronic signatures are met.

Under the sections covering electronic records, there are requirements for closed systems (where access is controlled by the persons that are responsible for the content of the electronic records) including authenticity, integrity, confidentiality and non-repudiation. The requirements for open systems (like the Internet) cover electronic records from the point of their creation to the point of receipt and also call for authenticity, integrity and confidentiality, as well as additional measures such as encryption and digital signatures (defined as cryptographically-based).

For electronic signatures, the central tenet of the requirements is that a signature should uniquely identify an individual. There are requirements for signature manifestations (what information must be contained in the signature), signature/record linking, signature components, usage in a series of signings and collaboration in obtaining another's signature. As well, there are specific controls for using electronic signatures based on identification codes and passwords.

To meet the various needs of different pharmaceutical firms, RSA Security offers a range of products and services that support the use of electronic records and electronic signatures, including RSA Keon® certificate management, RSA SecurID® two-factor authentication, RSA ClearTrust® Web access management and RSA BSAFE® software development kits. RSA Professional Services provides a comprehensive set of services to align e-security investments with business requirements.

To be compliant with 21 CFR Part 11, an organization must develop, implement and enforce policies and procedures that specifically meet the requirements, including training and monitoring employees and deploying the appropriate technical infrastructure. The general approach of the agency is to provide a baseline standard and allow organizations to determine the appropriate security measures and technologies.

RSA Security's solutions address many of the central requirements of 21 CFR Part 11. The products are designed to enable authentication, protect data integrity and confidentiality, provide audit trails, establish non-repudiation, control access to information and deliver unique electronic signatures. RSA Security solutions also address the specific security and signature controls required by the regulation. (The list of specific controls and how RSA Security addresses these is described in a table in the appendix.)
RSA Professional Services can work with an organization to develop the corresponding policies and procedures.
For building custom applications that integrate security, RSA Security provides tools for developers.

II. Background

Electronic Information Systems

The pharmaceutical industry is increasingly using electronic information systems to improve efficiency of operations. One of the major initiatives is to move to a paperless environment and thereby significantly reduce costs. Part of this trend, in recent years, has been the increased use of the Internet. Applications such as e-mail communications, Web-based clinical trials, supply chain management and interactive Web sites are used for delivering information regarding drugs and treatments.

At the same time that pharmaceutical companies are increasing their use of computer systems and networking technology, major forces based on market demands and regulations are calling for developing enhanced security policies and practices in order to protect electronic information.

The Need for Security and Electronic Signatures

Pharmaceutical companies need robust security and e-signatures for several important reasons:

- To "e-enable" and therefore improve business processes.
- To protect intellectual property.
- To maintain the trust of customers and business partners and remain competitive.
- To mitigate the risk of litigation and protect an organization from liability and
- To comply with regulations such as the U.S. Food and Drug Administration's (FDA) 21 Code of Federal Regulations (CFR) Part 11 covering electronic records and electronic signatures.

III. Overview of 21 CFR Part 11

21 Code of Federal Regulations (CFR) Part 11 has been in effect since August 1997 and establishes the U.S. Food and Drug (FDA) Administration'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.

Both the pharmaceutical industry and the agency have much to gain by using electronic records and electronic signatures, such as accelerated information exchange, reduced storage space requirements, decreased errors, more extensive data analysis, faster and more advanced information search techniques, streamlined manufacturing and better process control.

The rule covers two main areas, requirements for electronic records and 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 rule applies 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."

Under 21 CFR Part 11, electronic signatures are broadly defined and therefore can be based on various authentication technologies, including everything from user ID and password to cryptographically based digital signatures, as long as the specific requirements and controls for electronic signatures are met.

The regulations do not require the use of electronic records and electronic signatures, but rather permit their use when the requirements are met. It is important to note that the regulations represent the minimum requirements for implementation, such that organizations can choose to make their systems even more secure.

In developing the regulations, the agency's intention was to allow a lot of flexibility while providing a baseline standard. Accordingly, the regulations permit the use of a variety of electronic record and electronic signature technologies. As well, the regulations give organizations flexibility in determining the appropriate level and suitable methods of security for their particular situation.

IV. Requirements of 21 CFR Part 11

Electronic Records

Controls for closed systems

This section outlines the 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.

The controls should be "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 specific controls required, including access controls and audit trails, are listed in the appendix.

Controls for open systems

This section outlines the 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. An example of an open system is the Internet.

The controls should be "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 [for closed systems], and as needed, additional measures such as document encryption and appropriate digital signature standards."

In general, for open systems, the controls for closed systems still apply and additional measures should be taken such as encryption and digital signatures. Encryption and digital signatures are not restricted to meeting the requirements for open systems and may be used as part of a robust security system in meeting all of the requirements for electronic records on closed and open systems and for electronic signatures. However, because of the added risks when using

open systems, as indicated above, the FDA specifically references these two proven methods, encryption and digital signatures, as suitable measures to take.

The definition of a digital signature (as per 21 CFR Part 11) is "an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such the identity of the signer and the integrity of the data can be verified."

Signature Manifestations

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

Signature/Record Linking

This section specifies that signatures be linked with records: "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."

Electronic Signatures

General requirements

This section specifies general requirements for electronic signatures including uniqueness, previous verification of identity and certification of intent. The complete requirements are listed in the appendix.

Electronic signature components and controls

This section outlines the requirements for electronic signature components and controls including the requirement for two distinct identification components, the usage in a series of signings and the need for collaborative methods in obtaining another's signature. The detailed requirements are listed in the appendix.

Controls for identification codes/passwords

This section covers controls that must be in place when using electronic signatures based on identification codes and passwords: "Persons who use electronic signatures based upon identification codes and passwords should employ controls to ensure their security and integrity." The specific controls under this section are listed in the appendix.

V. Range of Products and Services

To meet the various needs of different pharmaceutical firms, RSA Security offers a range of products and services that support the use of electronic records and electronic signatures as described below. In addition, RSA Secured® Partners can offer a wide range of complementary technology including e-forms, workflow and document solutions. The RSA Secured Partner Program works with software and hardware vendors to integrate or establish interoperability between partner products and RSA Keon certificate management, RSA SecurID authentication, RSA ClearTrust access management and RSA BSAFE encryption.

RSA Keon Certificate Management

RSA Keon software is a family of interoperable modules for managing digital certificates and creating an environment for authenticated, private and legally binding electronic communications and transactions. RSA Keon Certificate Authority (CA) issues, manages and validates digital certificates. RSA Keon Registration Authority (RA) helps streamline the enrollment process. RSA Keon Key Recovery Module (KRM) provides a way to securely archive and recover users' private encryption keys. RSA Keon Web PassPort is a browser-compatible applet used to download and secure on-line credentials. RSA e-Sign provides the ability to digitally sign Web-based forms.

A digital certificate is a data file used as form of electronic identification that follows a rigid format (RSA Security conforms to the IETF's X.509 standard for certificates) and contains information on the holder of the certificate and the organization that issued the certificate.

With RSA Keon certificate management, each end-user is issued a private/public key pair (pair of numbers with a unique mathematical relationship). The public key is embedded in the digital certificate and available to others for communicating, conducting transactions or exchanging data with the owner of the key pair. The corresponding private key is securely held by the owner, for example in software (i.e. secure desktop) or in hardware (i.e. downloaded to a smart card). RSA Keon certificate management software provides policy-based access for securing the software- or hardware-based credential store, designed to ensure the protection of the private key.

Keys are used for encryption/decryption and digital signing. Data that is encrypted with a public key can only be decrypted with the corresponding private key. Private keys are used to generate and attach a digital signature to a file, document or message, and the corresponding public key to verify that signature.

RSA SecurID Authentication

RSA SecurID authentication system is a solution designed to provide centrally managed, strong, two-factor user authentication services for enterprise networks, operating systems, e-commerce and other IT infrastructure. It is intended to ensure that only authorized users access data, applications and communications. RSA SecurID authentication is used in applications such as Virtual Private Networks (VPN) and Web access in wired or wireless environments.

The RSA SecurID system consists of three components; RSA ACE/Server® authentication server; RSA ACE/Agent,® software — intermediary agents built into the device or application that proxy the authentication request to the server; and the RSA SecurID authenticator (token or smart card) that is held by the end-user. The product line also includes a comprehensive smart card solution including the RSA SecurID Passage, a stand-alone smart card client that combines the security of a certificate enabled smart card with the flexibility of a multi-application Java Card, and RSA SecurID 5100 Smart Card, a Java Card that combines digital certificate credential storage with other applications such as building access, corporate ID and e-purse.

RSA ACE/Server software and each RSA SecurID authenticator are time synchronized and both have the user's unique seed value and the RSA SecurID algorithm. Every sixty seconds the authenticator's chip performs a calculation using the RSA SecurID algorithm. This combines the unique seed value with the current GMT time to create a unique and pseudorandom number called a token code.

The end user enters a one-time passcode, which is a combination of a personal PIN plus the unique token code. Using the user's unique seed record, RSA ACE/Server software performs the same calculation as the RSA SecurID authenticator. If the user's passcode matches the server passcode, RSA ACE/Server software grants that user access.

RSA ClearTrust Web Access Management

The RSA ClearTrust Web access management solution is a unified, Web-centric user access and privilege management system for e-business that allows or denies access based on definable user attributes. RSA ClearTrust access management is designed to allow organizations to secure Web applications via intranets, extranets, portals and exchange infrastructures. RSA ClearTrust access management software is designed to enable transparent Single Sign-on (SSO) within or across multiple Web sites or domains.

The RSA ClearTrust software is engineered to be an easy-to-deploy, rules-based solution that integrates the required services for centrally controlling and managing user privilege for access to Web applications based on user profiles, business rules and security policies. It enables organizations to build Web access management policies based on existing data and automatic updates and to quickly translate "business rules" into online Web access management policy using native language and Boolean constructs.

With RSA ClearTrust software, administrators can monitor both the resources accessed as well as what function users perform within those resources. This granular authorization can even be external from the Web application, so that a developer can simply "drop-in" any level of protection to an existing application.

RSA BSAFE Software Development Kits

RSA BSAFE security software is designed for building state-of-the-art privacy, authentication and digital certificate management features into any application. Securing almost a billion applications worldwide, RSA BSAFE software is the developer's tool of choice for secure, rapid application development.

Designed to meet the needs of secure application development, RSA BSAFE software provides security technology at three different levels:

1. Protocol level support: A comprehensive solution for developers who need to securely enable applications and products to send encrypted data according to industry standard protocols like:
    - IPSec – used to protect data streams by encrypting and authenticating network traffic at the level of Internet Protocol (IP) packets,
    - SSL – built to secure client/server applications,
    - WTLS – used to secure wireless client and wireless gateway applications, and
    - S/MIME – designed to secure electronic messaging applications for secure e-mail.
2. Digital certificate enablement: certificate enablement capabilities for applications or products, including digital certificates, digital signing capabilities and digital certificate handling including revocation or management capabilities. RSA BSAFE products allow applications to co-exist in a multiple CA environment and enable applications to understand a user's digital credentials whether stored in a digital certificate or smart card.
3. Core crypto functionality: Cryptography is the basis for establishing data integrity, authentication and non-repudiation in the electronic world. Providing time-tested and trusted encryption technology to securely protect confidential information stored in a number of databases, Web servers and data storage products, RSA BSAFE Crypto products allow developers to pick and choose the algorithms they need based on the security requirements of the application.

RSA Professional Services

RSA Security has been working with clients in a broad range of industries, including pharmaceuticals, for almost 20 years. RSA Professional Services can complement in-house resources, providing assistance in everything from installation and training to deployment and maintenance.

Drawing on years of knowledge and expertise in security systems, RSA Security is able to provide a clear understanding of the strengths and weaknesses of an organization's current network and application security capabilities, along with concise recommendations for improvement.

Also, RSA Security delivers services through strategic partnerships with leading technology firms and in conjunction with some of the industry's most experienced network security consultants, providing custom and industry-specific solutions to e-business challenges.

VI. Addressing the requirements with RSA Security solutions

To be compliant with 21 CFR Part 11, an organization must develop, implement and enforce policies and procedures that specifically meet the requirements, including training and monitoring employees, and deploying the appropriate technical infrastructure. The general approach of the agency is to provide a baseline standard and allow organizations to determine the appropriate security measures and technologies.

RSA Security's solutions address many of the central requirements of 21 CFR Part 11. They are designed to enable authentication, protect data integrity and confidentiality, provide audit trails, establish non-repudiation, control access to information, as well as deliver unique electronic signatures that identify an individual. The following sections describe how RSA Security solutions address these central requirements. RSA Professional Services will work with an organization to develop corresponding security policies and procedures. For building custom applications that integrate security, RSA Security provides tools for developers. RSA Security solutions also address the regulations' specific controls as outlined in the appendix.

Authentication

Authentication protects resources and applications by requiring that users validate who they claim to be. It is the process of verifying the identity of users before they are allowed to gain access to critical data assets, perform electronic transactions or manipulate electronic records.

The three most common factors used to verify identities are: something the user knows (e.g., password), something the user has (e.g., RSA SecurID hardware token or smart card) and something the user is (e.g., biometric data such as fingerprint). Authentication is based on a single factor or multiple factors. Single factor authentication (i.e., a password) has consistently been proven to be a weak method of authenticating a user's identity. Strong user authentication only results from using at least two factors of authentication, such as a secret a user knows (e.g., a PIN) and a device that a user holds (e.g., an RSA SecurID token).

Passwords are the weakest, although most widely used, form of authentication. This method is perceived to be easy to deploy and inexpensive. However, history has proven that these codes are easily guessed, stolen or otherwise compromised and difficult and expensive to maintain. Surprisingly, passwords are one of the most ineffective forms of authentication.

In the context of the regulation, the FDA cautions that: "...records are less trustworthy and reliable if it is relatively easy for someone to deduce or execute by chance a person's electronic signature where the ID is not confidential and the password is easily guessed." Therefore using a user ID which would be commonly known (e.g., some form of the person's name) with a weak password would likely not provide a high assurance system in which records are trustworthy and reliable. For a high assurance system, RSA Security recommends strong two-factor authentication using a digital certificate and/or RSA SecurID authentication.

Digital Certificates

With RSA Keon certificate management system, a user's certificate is digitally signed by a Certificate Authority that has approved the individual, stands behind their certificate and corroborates their identity, providing a high level of assurance that the individual is who they say they are. An RSA Keon digital certificate provides a unique identifier; each certificate has a unique serial number and DN (distinguished name).

The relative strength of digital certificates as an authentication method depends on how securely the corresponding private key is protected. RSA Keon certificate management provides ways to protect private keys including passwords, smart cards, biometrics and/or RSA SecurID authentication.

Digital certificates gain strength when they are accompanied by a password governed by a controlled password policy. Here, a trusted certificate authority has a certificate policy statement that establishes password requirements (e.g., every password has to be 9 alphanumeric characters in length and be periodically revised.)

Using smart cards to protect private keys provides one of the strongest levels of authentication. Access to the private keys on the smart card can be protected with a PIN or password. Key pairs can be generated and then stored on the smart card, in this way the private key never leaves the card. RSA Keon software can support storing certificates on smart cards from RSA Secured partners as well as RSA SecurID smart cards. Authentication can also be extended to include methods such as biometrics.

Two-factor authentication

Providing two-factor authentication, the RSA SecurID system requires that users possess their authenticator and know their PIN. Users are authenticated by providing this impossible-to-guess or -duplicate token code / PIN combination. This gives organizations a very high assurance that those persons requesting access to information are in fact who they claim to be. Each individual on the system is uniquely identified since each authenticator (token or smart card) has a unique seed value.

Combining these two methods, digital certificates and two-factor authentication, enhances the strength of authentication. By requiring two-factor authentication to access keys, an organization is able to bind a user's digital identity to his/her physical identity with a higher level of confidence.

Revoking credentials

As per the FDA's guidelines, the security system should include a mechanism for preventing access of users who have been issued credentials but whose credentials are no longer valid. This would prevent for example, the signing of a record with an invalid signature by a former employee. To minimize the opportunity for executing false signatures, as a matter of organizational policy, assigned signatures should be cancelled immediately upon the departure of an employee or in the event of any type of compromise.

RSA Keon certificate revocation functionality is designed to disallow the use of a certificate immediately upon revocation. Unlike other certificate management systems, there is no time lag between the revocation and limiting access to applications. RSA Keon uses a unique real-time implementation of the industry standard on-line certificate status protocol (OCSP). The RSA SecurID authentication system provides a mechanism to deactivate authenticators, immediately disallowing access to applications.

Centralized Authentication Management

RSA ClearTrust software centralizes the management of authentication services as well as Web access management. It supports resource-based authentication (i.e., authentication that is linked to the resource not the user) to provide more consistent security and more flexibility in user authentication. This means that an administrator can assign authentication methods based on the value of the resource. RSA ClearTrust access management supports multiple methods of authentication including user name & password, certificates, tokens, smart cards, LDAP authentication and custom methods. (Note: RSA ClearTrust software is both RSA SecurID Ready and RSA Keon Ready.)

Data Integrity

RSA Keon certificate management addresses this requirement through the use of digital signatures. Digital signatures protect data integrity. For the user, signing a document can be as simple as selecting an "attach signature" option within an application. The underlying technical process uses the signer's private key to encrypt a hash (digest) of the document. The resulting bit string is attached to the document as a digital signature. Applications using digital signatures automatically verify the signature, and can immediately determine if the data has been altered. For verification, the process uses the signer's public key to decrypt the hash of the document and then independently creates a hash of the document and compares the two. If they match, the signed document is proven to be unaltered. Also, the identity of the signer is proven since only the private key of the signer could have been used to encrypt the digest that was decrypted by the signer's corresponding public key.

RSA Secure e-Forms Signing solution provides the ability to digitally sign Web-based forms. It verifies the signature on the form and thereby detects if any modifications have been made to the form after it has been digitally signed. RSA Secure e-Mail solution provides for the signing of e-mail messages to ensure messages are delivered intact. For protecting data integrity by digitally signing other types of e-forms, e-mail messages, or documents, RSA Keon CA works with a range of electronic document, workflow, office automation, and mail applications from RSA Secured partners.

RSA SecurID authentication and RSA ClearTrust Web access management solutions support data integrity so that in logging changes to the record, the application would have access to an audit trail, enabling individual accountability for invalid or altered records.

Confidentiality

Encryption can be used to ensure the confidentiality of documents or communications. RSA Security solutions support strong encryption up to 2048 bits (asymmetric) and 128 bits (symmetric). For encryption of documents or e-mail messages, RSA Keon digital certificate technology provides a system employing private/public key pairs. The originator of the document / message uses the intended recipients' or viewers' public key to encrypt the data, so that only this intended user will be able to view the data by using their corresponding private key to decrypt it.

RSA Secure e-Mail solution enables users to encrypt (and digitally sign) e-mail communications — including attachments — so messages in transit remain confidential and cannot be easily intercepted. RSA Secure e-Mail capabilities are included as a standard feature of RSA Keon CA software and require no additional client-side software other than the standard MS e-mail client. RSA Secure e-Forms Signing solution enables the user to encrypt a Web-based form before it is signed to protect it in storage and transport. For encrypting other electronic forms, documents, or files on a desktop, RSA Keon CA works with a range of e-document, workflow and office automation applications from RSA Secured partners.

For documents/messages that are stored in an encrypted format, there must be a means to enable their retrieval, in the event that encryption keys are lost, damaged or otherwise not available. The RSA Keon Key Recovery Module is an archival system that is designed to securely recover private encryption keys. (For security and to ensure non-repudiation, the RSA Keon key escrow system does not back-up or recover private keys used for signing, only private keys used for encryption. Signing keys are securely held by the owner and not accessible by others.)

For encrypting information exchanged between a client and Web site, an SSL session (i.e. a secure channel) can be established using an SSL server certificate. The RSA Keon Web Server SSL solution allows organizations to issue and manage trusted SSL certificates. The solution includes the RSA Keon CA, which provides for the issuance and installation of an SSL server certificate (as well as the end user's client certificate), and the RSA Keon Root Signing Service which chains an organization's CA to the trusted RSA Root.

The RSA BSAFE encryption product line allows software and hardware developers to incorporate encryption technologies into their applications and products. RSA BSAFE SDKs provide fully implemented protocols and core cryptographic components. Protocols include SSL for securing Web communications, WTLS for securing wireless devices and applications, S/MIME for securing e-mail messaging applications, and IPSec for encrypting and authenticating network traffic. RSA BSAFE cryptography provides a full library of popular cryptographic algorithms.

Non-repudiation

Non-repudiation means that a user cannot later disavow an action (e.g., modifying or signing a record). RSA Keon certificate management provides non-repudiation through the use of digital signatures — the identity of the signer is verified by using the signer's public key, i.e., only the holder of the corresponding private key could have signed the document. RSA SecurID authentication supports non-repudiation through strong two-factor authentication coupled with audit logs; the audit trail provides a link to the identity of the signer. With RSA ClearTrust Web access management, audit logs serve as proof so users are not able to repudiate actions.

Access Control

Access control takes business rules and security profiles into consideration to establish and enforce policy around which users are granted the privilege to access which resources. Several levels of access management are possible:

- Course-grained authorization involves limiting access at the URL-level to protect Web-based resources. This will authorize where a user can go, i.e., to what domains, directories, data stores, departments, Web servers, or individual pages on a Web server.
- Medium-grained authorization provides a more granular level of access management than course-grained. It provides the ability to allow/restrict access to values associated with fields within application records, specific files, objects on a Web page, subsets of Web pages, etc.
- Fine-grained authorization involves elaborate rule-based access control. It requires the application of business policies and the administration of complex "if-then" business rules.

RSA ClearTrust Web access management solution provides a single, unified framework that is designed to enable an organization to manage users' access privileges, ensure that only legitimate users get access to specific resources and provide fine-grained control over who can access what. Access control is a general requirement of 21 CFR Part 11; specifically the regulation calls for organizations to limit system access to authorized individuals.

As pharmaceutical companies increasingly use Web applications to improve the efficiency of operations, Web access management will be a critical element to a security strategy. To provide access management in a Web environment, administrators must be able to manage a large number of user accounts and the privileges associated with their accounts, create centralized access control, validate the user and then permit access to resources based on user privileges. With RSA ClearTrust Web access management solution, access is granted or denied based on whether a user's privilege profile meets certain criteria. The criteria can be static (job responsibility or department) or dynamic (account status).

Auditing

RSA Keon certificate management, RSA, RSA SecurID authentication, and RSA Clear Trust Web access management can provide extensive logging, to be used for auditing purposes. Logs are configurable, time-stamped and strictly limited to system administrators.

Application and network activity is traceable to the user, not just a device. This allows organizations to effectively implement security policies that hold individuals responsible for their actions. Policies should include the procedures to follow in the event of audit alarms or discrepancies. RSA Professional Services can assist in the development of policies and procedures.

RSA Keon software can record and securely log all certificate management events (e.g., certificate issuance/denial) including the identity of the individual performing the action. RSA Keon software can also log each certificate status query; these logs can be used in detecting and reporting any attempted misuse of a certificate. For added security, RSA Keon logs can be digitally signed by an authority (e.g., with the CA's private key).

With RSA SecurID authentication, the RSA ACE/Server software can provide comprehensive reporting of all access to protected resources. Reports can be easily tailored to an organization's own security requirements. Reporting is highly granular: at the user, group, system or agent level. Reports can be designed to view an activity, exception or incident, as well as usage summaries. RSA ACE/Server software also supports notification based on events, so that the administrator can be alerted to a failed logon attempt while in progress. Select messages from the RSA ACE/Server audit log can be forwarded to the UNIX syslog or Windows NT event log, calling attention to the most important events from the system's extensive log data.

With RSA ACE/Server software, an audit trail of each login attempt and operation performed is automatically generated. The automated log maintenance feature lets administrators create settings for archiving log files. This "set and forget" feature is designed to ensure that usage logs are safely preserved without intervention.

RSA ClearTrust Web access management provides for end-to-end auditing of all transactions with full reporting of all security events. The audit trail begins with detailed logs that serve as proof of activity so users are not able to repudiate a transaction. Similarly, audit logs can be used by the administrator to prove that specific user activity occurred. For reporting, data can be sorted and filtered by a variety of attributes.

Electronic Signatures

RSA Keon certificate management provides a solution to meet the requirements for electronic signatures. RSA SecurID authentication supports electronic signatures by providing strong two-factor authentication. Both support the general requirement that a signature be unique and identify an individual.

Each digital certificate created by RSA Keon software contains a unique serial number and DN (distinguished name). The private key used to generate the digital signature associated with a user's certificate is held only by the user. No one else can create a signature using this key. Private keys can be protected by a password (governed by a password policy) or RSA SecurID authentication and/or stored on a smart card to provide greater assurance that no one else has access to it.

Each RSA SecurID token is unique. With strong two-factor authentication, even if someone attempts to use a token belonging to another individual, they would not have that user's PIN, which provides greater assurance that no one else has access to a user's electronic signature. RSA ACE/Server software tracks all user IDs and prevents the issuance of duplicates, so each user ID would be unique.

Also each passcode consisting of a token code and PIN is unique not only to the user but is unique with each authentication, since an RSA SecurID token generates a new token code every 60 seconds. The FDA specifically acknowledges this mechanism for developing unique passwords: "The agency is aware, however, of identification devices that generate new passwords on a continuous basis in synchronization with a "host" computer. This results in unique passwords for each system access."

Both RSA Keon certificate management and RSA SecurID authentication also support the use of the required two distinct identification components for an electronic signature, such as identification code and password. An RSA Keon electronic signature could be comprised of a digital certificate (i.e., representing an ID code) and a policy-controlled password or RSA SecurID passcode. With RSA SecurID technology, the electronic signature technique could be based on the two components of user ID and passcode.

For open networks (i.e., Internet) the FDA recommends digital signatures and defines these as cryptographically based. RSA Security digital signatures fulfill this definition and conform to the appropriate standards. The FDA specifically acknowledges the American National Standards Institute (ANSI) and the Federal Information Processing Systems (FIPS) standard for digital signatures (which uses the RSA Security digital signature cryptographic algorithm) as appropriate standards.

Many pharmaceutical companies are looking to improve efficiencies by replacing paper-based forms with electronic forms and implementing e-business processes. For electronically signed Web-based forms, RSA Secure e-Forms Signing solution provides digital signatures. This solution will enable trusted and secure end-to-end electronic processes. It utilizes a zero footprint, signing applet that works within standard Web browsers and does not require any client software to be installed or configured by the user. It also supports multiple signings per form.

Pharmaceutical companies are also implementing trusted and secure mail communications through the use of signatures on e-mail messages. RSA Secure e-Mail solution can provide the required digital signatures. This solution verifies the signature and validates the source and integrity of messages. In addition, RSA Secured partners can offer other e-form, work flow and document solutions that work with RSA Keon digital signatures or RSA SecurID authentication for implementing electronic signatures.

To develop a custom signing application that would use RSA Keon digital signatures or RSA SecurID authentication services, RSA Security provides high-level APIs. RSA Professional Services can also provide programming expertise for the development of custom applications.

Policies and Procedures

In complying with 21 CFR Part 11, an organization must establish and enforce procedures and policies. RSA Security can assist in establishing the policies and procedures, it is up to the organization to enforce them.

For example, in developing certificate management policy, RSA Professional Services can assist with the Certificate Policy and Certificate Practices Statements — policy and procedure documents that include digital certificate issuance and management. These documents also define appropriate certificate usage as well as liability for any misuse of a certificate. As well, to ensure that certificate holders are accountable and responsible for their actions, organizations must develop a subscriber's agreement, which outlines the terms and conditions for acceptable use of a certificate.

Solutions for Developers

Meeting the FDA's requirements for securing electronic records and using electronic signatures includes ensuring security at the application level. For building solutions that meet the FDA requirements, developers can turn to RSA BSAFE Software Development Kits to integrate authentication, data integrity and non-repudiation components into applications for secure rapid application development.

These products include:

RSA BSAFE SSL-C and SSL-J implement the SSL protocol in C and Java languages to secure data flowing between two points (server to server, client to server, client to client for FTP, Telnet and Web sessions.)

RSA BSAFE S/MIME-C implements the S/MIME protocol for developers who need to build security into messaging applications to secure data that is stored and forwarded. The S/MIME protocol was written by RSA Security and accepted as an international standard, used worldwide to secure electronic messaging applications.

RSA BSAFE WTLS implements the WTLS protocol within WAP for developers building security into wireless devices and applications. The WTLS protocol secures information transferred between wireless clients and Internet gateway devices.

RSA BSAFE Cert-C & Cert-J are certificate-enablement products which are designed to allow developers to implement certificate management and digital signature capabilities into applications and devices. These products allow developers to make their applications certificate-aware so that applications know how to retrieve, store and validate a user's digital credentials whether stored in a smart card or digital certificate.

RSA BSAFE Crypto-C & Crypto-J are designed to allow developers to embed encryption technologies into products and applications to achieve privacy and integrity of data, as well as establish authentication and non-repudiation techniques.

APPENDIX: Meeting the Specific Controls Listed in 21 CFR Part 11

The following table lists the specific controls and requirements and includes the rule's section numbers to enable easy cross referencing. Each requirement has a brief description of how it is addressed by RSA Security solutions. In meeting these specific controls, an organization must not only deploy technology but must also develop policies and procedures. That is, technical measures alone will not meet the requirements. RSA Professional Services can assist an organization in developing policies and procedures.

Subpart B — Electronic Records

11.10 Controls for Closed Systems

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records.	Organizations must validate systems (internally or externally) Organizational policy should include auditing Need mechanism to check data integrity	Provides extensive logging for auditing purposes Digital signature verifies data integrity	Provides extensive logging for auditing purposes Supports data integrity by providing an audit trail to the user	Auditing and reporting create a complete log Supports data integrity by providing audit trail to the user	Integrates data integrity functionality into applications
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form.	Application-dependent Accurate and complete records supported by data integrity and audit trails	Supports through data integrity and audit trails	Supports through audit trails	Supports through audit trails	Supports by integrating data integrity into applications
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Protect records with access control and/or encryption Need encryption key recovery Organizations must establish access control policy	Encryption mechanisms restrict access to intended individuals or groups, includes key recovery	Controlling access to networks or applications can be set by user or group	Enforces access control policy Access based on whether user profile meets certain static and dynamic criteria, so throughout retention period, access to records would require valid and active user status	Integrates cryptographic services into applications

11.10 Controls for Closed Systems (cont.)

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(d) Limiting system access to authorized individuals.	Need authentication and access control Multi-factor authentication provides higher assurance	Digital certificates provide authentication and support access control Works with passwords, RSA SecurID technology, smart cards or biometrics	Token code and PIN provide authentication and support access control Strong two-factor authentication	Limits system access to authorized individuals Provides fine-grained access control, limiting not only the resources available to users but also the functions they are able to perform within a given application Works with passwords, RSA SecurID technology, smart cards or biometrics	Integrates certificate handling and trust services into applications, including authentication services
(e) Use of secure, computer-generated, time-stamped audit trails.	Need secure logging Should provide for individual accountability	Logs are digitally signed, time-stamped and accessible only by authorized administrators Activity is traceable to the individual user	Logs are time-stamped, and accessible only by authorized administrators Activity is traceable to the individual user	Logs are time-stamped, and accessible only by authorized administrators Activity is traceable to the individual user	
(f) Use of operational system checks to enforce permitted sequencing of steps and events.	Specific to the application Should be included in organizational policy Relies on security	Provides security services			
(g) Use of authority checks to ensure that only authorized individuals can use the system.	Organizations must have policy defining authorized individuals Relies on authentication	Provides authentication services		Enables authority checks through centralized user privilege management, which provides rule-based and role-based control of access based on definable business rules and user attributes	

11.10 Controls for Closed Systems (cont.)

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(h) Use of device checks to determine the validity of the source of data input or operational instruction	For example, device checks should ensure that it is an authorized workstation and not another device that is issuing a command	Issues certificates to devices such as routers and servers. For example, a RSA Keon CA server must authenticate itself when making a query to the database, to ensure that it is the authorized server issuing the command	Authenticates users who can be using various devices (VPNs, wireless, etc.) and determines that the right user is using the device assigned to them	Enables tight integration with authentication services, to ensure the right user is using the device assigned to them	Integrates digital certificates into applications
(i) Determination that persons who develop, maintain or use electronic record/electronic signature systems have the education, training and experience to perform their assigned task	Specific to the organization Would include documentation and training regarding the security systems	RSA Security solutions are easy to use and many tasks are automated and performed transparently RSA Security provides extensive documentation and comprehensive training courses as well as the RSA Professional Services Certified Security Professional program			
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures	Individual accountability relies on audit trails Organization must establish and enforce policies	Provides for an audit trail to the user. RSA Professional Services can assist in the development of policies.			
(k) Use of appropriate controls over systems documentation	Specific to the organization				

11.30 Controls for Open Systems (additional measures for electronic records on open systems)

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
Encryption	Should support strong encryption up to 2048 bits (asymmetric) and 128 bits (symmetric)	Provides for the encryption of files, documents and messages as well as communications (with SSL session)	Provides strong two-factor authentication to support encryption	Enables tight integration between access control and encryption services	Provides all the core crypto needed to establish data integrity, data protection or non-repudiation at the application level
Digital Signatures	Defined by the FDA as cryptographically-based	Provides digital signatures that conform to the ANSI and FIPS standards	Provides strong two-factor authentication for higher assurance digital signatures	Enables tight integration with digital signatures	Integrates digital signatures into applications

11.50 Signature Manifestations

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(a) Signed records must contain signer's name, signature date, time and meaning	Encapsulating the name can be supported by the electronic signature technique Encapsulating the date and time of a signing event is application-dependent Meaning of the signature includes review, approval, responsibility or authorship	Digital certificates contain the name of the owner (as per X.509 standard) Conformance to industry standards for Internet and digital signatures, allows compatibility with applications such as e-mail programs that use digital signatures with built-in date and time Depending on the requirements, the best solution may be to issue multiple digital certificates to an individual with each certificate associated with a different role. (i.e., For each signing, a particular certificate could be used to indicate the meaning)	Authorized employees are issued individually registered devices that are unique. The user ID information such as their name is contained in the RSA ACE/Server database	Supports the creation of signed records containing name, date, time and meaning by monitoring the resources users access as well as the transactions performed (such as signing a record)	Integrates digital signatures into applications

11.70 Signature Linking

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
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	Link the signature and record Technical measures alone will not prevent falsification of records, an organization must develop policies and procedures to prevent falsification of the records	Uses digital signatures, which automatically link signature and record (i.e., when digitally signing a record, a digest of the record is encrypted with the private key.) Data integrity and audit logs are safeguards to prevent falsification of records. RSA Professional Services can assist in developing policies and procedures	Supports the linking of the electronic signature to the record by providing strong two-factor authentication combined with an audit trail to the user RSA Professional Services can assist in developing policies an procedures	Supports the linking of the electronic signature to the record by monitoring the resources users access as well as the transactions performed and combined with authentication, provides an audit trail to the user. RSA Professional Services can assist in developing policies and procedures	Integrates digital signatures into applications

Subpart C — Electronic Signatures

11.100 General Requirements

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(a) Each electronic signature will be unique to an individual and should not be reused by, or assigned to, another individual	Should uniquely identify individual user and be inaccessible to others Organizational policy should disallow, for example, the sharing of signatures	Each RSA Keon digital certificate is unique. The private key used to generate the digital signature associated with a user's certificate is held only by the user and no one else can create a signature using this key	Each RSA SecurID token is unique. Even if someone attempts to use a token belonging to another individual, they would not have that user's PIN	· Supports unique electronic signatures by enabling tight integration with authentication services	Integrates digital signatures into applications

11.100 General Requirements (cont.)

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(b) Before an organization establishes, assigns or certifies an individual's electronic signature, the organization shall verify the identity of the individual.	Verification and approval is determined by organizational policy	Provides a flexible process whereby a user's identity is approved as per organizational policy before a certificate is issued	Administrators issue individually registered authenticators only after approval as per organizational policy	Enables tight integration with authentication services to support an organization's policies	Integrates digital certificate handling into applications
(c) Persons using electronic signatures shall certify to the FDA that they are using electronic signatures.	Specific to the organization				

11.200 Electronic Signature Components and Controls

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(1) Electronic signatures should employ two distinct identification components such as an identification code and password.	For electronic signatures not based on biometrics	Based on two components for example: a digital certificate and a password/ RSA SecurID passcode	Based on two components: user ID and RSA SecurID passcode	Enables tight integration with authentication methods e.g., digital signatures and RSA SecurID technology, which use two distinct ID components	Integrates digital signatures into applications
(i) When an individual executes one or more signings not performed during a continuous period, each signing should be executed using all of the components.	Application-dependent	With RSA Security's solutions, depending on the organization's requirements, the system could be set up so that each signing required the two components.			

11.200 Electronic Signature Components and Controls (cont.)

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(ii) When executing a series of signings during a continuous period, the first signing should be executed using all components and subsequent signings at least one component. The FDA provides further guidance on this point: "If the person leaves the workstation, someone else could … impersonate the legitimate signer by entering an ID code or password. It's vital to have stringent controls in place to prevent impersonation, including automatic inactivity disconnect and subsequent signings should be component only known by authorized individuals."	Time limits for continuous periods would be set by the organization Requires inactivity protection Mostly application-dependent, supported by the authentication method	The RSA Keon Web Passport software provides inactivity protection, such that after a set period of time, the workstation is locked and the user must re-authenticate Supports the development of a system which would require the secret component (password or passcode) for subsequent signings	For Web applications, RSA SecurID software has inactivity protection, based on a time-limited cookie. After a set period of time, the user must re-authenticate Supports the development of a system which would require the secret component (password or passcode) for subsequent signings	Enables tight Integration with authentication services	Integrates digital signatures into applications
(2), (3) Be used by their genuine owners. Be administered so attempted use by anyone else requires collaboration of two or more individuals.	Protection of signatures	System can be configured so that keys are stored locally. This prevents access to the digital signature except by the rightful owner. The Key Recovery Module requires the collaboration of multiple (m of n) administrators to access private keys	System can be configured so that it requires more than one administrator to access user information and encrypted token codes that are centrally stored in the RSA ACE/Server database	Enables tight Integration with authentication services	Integrates digital signatures into applications

11.300 Controls for Identification Codes/Passwords (when using electronic signatures based on ID codes/passwords)

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(a) Maintain the uniqueness of each combined identification code and password to avoid duplication of the same combination of identification code and password.	No duplicate ids	Each digital certificate issued has a unique serial number and DN ensuring there will be no duplicates	Each token/PIN combination is unique and the RSA ACE/Server security server tracks all user ids and prevents the issuance of duplicates	Enables tight integration with authentication services	Integrates digital signatures into applications
(b) Ensure that identification code and password issuance are periodically checked, revoked or revised.	Periodic checks	Certificate status can be checked at each authentication and/or signing Certificate can be set to automatically expire after a pre-set time (as per organizational policy)	The token code is revised every 60 seconds	Enables tight integration with authentication services	Integrates digital signatures into applications
(c) Follow loss management procedures to electronically de-authorize lost, stolen or compromised tokens, cards and other devices, and provide for the issuance of temporary or permanent replacements.	Should be included in organizational policy Technology should support loss management	Provides for certificate life cycle management such that when a certificate is compromised (e.g., private key is lost), it is revoked and the database updated so that reliant applications have real-time access to the certificate status information New certificates can be issued immediately as a replacement	Includes a token management system that provides for the deactivation of tokens if lost, stolen or compromised and provides for a replacement	Enables tight integration with authentication services	Integrates digital signatures into applications

11.300 Controls for Identification Codes/Passwords (cont..)

Controls	Key factors	RSA Keon Digital Certificate Management	RSA SecurID Authentication	RSA ClearTrust Web Access Management	RSA BSAFE SDKs
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes and to detect and report attempts at misuse	Should be included in organizational policy Technology should support transaction safeguards	Revoked certificates are no longer valid and cannot be used for authentication or signing Certificate status is checked using real-time on-line certificate status protocol (OCSP) Revoked certificates will immediately be rejected by an application, preventing unauthorized use RSA Keon software logs each certificate status query; these logs can be used in detecting and reporting an attempted misuse of a certificate	Deactivated tokens are no longer valid and cannot be used for authentication or signing Applications will immediately reject the use of an invalid token All failed logon attempts are logged and the system can be configured to alert the administrator while attempted logon is in progress	Auditing and reporting creates a complete log that prevents users from repudiating a transaction	Integrates digital signatures into applications
(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	Should be included in organizational procedures Ensure properly functioning devices	When used with hardware security modules, RSA Keon software meets FIPS 140 certification. This certifies that RSA Keon keys and certificates are difficult to tamper with	RSA SecurID tokens are tested upon manufacture and issuance. Since the tokens are time-synchronized with the authentication server, any deviation from proper functioning would be detected	Enables tight integration with authentication services	Integrates digital signatures into applications

About RSA Security

RSA Security, the most trusted name in e-security,® helps organizations build trusted e-business processes through its RSA SecurID two-factor authentication, RSA ClearTrust Web access management, RSA BSAFE encryption and RSA Keon digital certificate management product families. With approximately one billion RSA BSAFE-enabled applications in use worldwide, more than twelve million RSA SecurID authentication devices deployed and almost 20 years of industry experience, RSA Security has the proven leadership and innovative technology to address the changing security needs of e-business and bring trust to the online economy. RSA Security can be reached at www.rsasecurity.com.

CFR2 WP 0902

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie