Evidian

Evidian Enterprise Access Management and 21 CFR Part 11

What is 21 CFR Part 11?

In their dealings with the US Food and Drugs Administration (FDA), some organizations, including pharmaceutical companies, are required to provide documents to the FDA, and to keep documents internally for archiving purposes.

Using physical documents exclusively (paper, films etc.) would impose an unnecessary regulatory burden to these organizations in terms of productivity and efficiency.

More and more, documents are available in electronic format, either natively or after scanning.

Therefore, title 21, part 11 of the Code of Federal Regulations (21 CFR Part 11) details the conditions required for:

- Archiving and providing to the FDA certain documents in electronic format in place of physical format.
- Using electronic signatures in place of regular signatures.

Not all documents required by the FDA may be submitted in electronic format. The list of documents for which electronic format is considered official can be consulted on-line in public docket 92s-0251.

Current status of 21 CFR Part 11

21 CFR Part 11 is effective since August 20th 1997. As its content generated many comments in the industry, the FDA issued a compliance policy guide and draft guidance documents over the next years, which were later rescinded.

In August 2003, the FDA issued a "Guidance for Industry". In that document, the FDA announced its intention to revise specific aspects of the regulation. Since the 21 CFR Part 11 remains valid and enforceable, we will include in this document the necessary caveats when we comment the parts that will probably change in the next months.

Identity and Access Management (IAM) and 21 CFR Part 11

IAM software can help an organization achieve the requirements of 21 CFR Part 11. However, compliance requires a large number of other factors, of which IAM software is but one element. A compliance project entails, among others:

- Specifically designed Standard Operating Procedures
- Conformant applications, including document management systems
- Internal awareness, checks and training

A large number of 21 CFR Part 11 requirements concern the software and databases used to store and sign electronic records.

IAM software can help compliance projects significantly by making access to electronic records databases more secure. Such software can also make it easier for users to access compliant systems, using applications to manage electronic records and signing documents. It thus makes compliance less intrusive and helps organizations achieve a better return on investment.

Using IAM software, organizations can make user authentication actions both **easier to perform** (through single sign-on) and **more secure** (through strong authentication). This may apply to all user authentication actions such as system access, application access and record signature. In addition, **centralized audit trails** make it easier to analyze the sequence of multi-applications user actions.

Lastly, centralized **user management** and sophisticated provisioning helps ensure that authorized users obtain their access and signature rights on an as-needed basis.

Single Sign-On and 21 CFR Part 11

A Single Sign-On (SSO) tool can be part of an environment compliant with 21 CFR Part 11.

SSO provides end-user ease-of-use and boots productivity. This can be of considerable help in managing the proliferation of application-specific IDs, passwords and hardware-based authentication.

In that case, all authentications will be performed under the control of the SSO system, and the user just needs one key pair in his or her daily work. For instance:

- Initial login to the workstation is performed with the primary key pair (e.g. Windows login and password or USB token and PIN code).
- Login to non-sensitive applications is done transparently by the SSO system.
- To log in to sensitive applications, the user needs to re-authenticate with his or her primary credential.
- To sign documents, the application will request re-authentication. The SSO system will notice that window and just ask the user to re-authenticate using the primary credential.

With such a system, administration is made easier by the centralization of management concerning resources, access rights and password management.

An additional advantage of using an SSO tool in that environment is that, as it logs each secondary re-authentication login required by a signature action, this provides a second, centralized audit trail for signatures.

Some definitions

According to 21 CFR Part 11, the following definitions apply:

- An **electronic record** meeting the FDA requirements outlined in 21 CFR Part 11 "may be used in lieu of paper records". It can be made of any type of information in digital format handled with a computer.
- A **closed system** is an environment "in which system access is controlled by persons who are responsible for the content of electronic records that are on the system."
- An **open system** is an environment "in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system."

On-line information

The FDA's 21 CFR Part 11 on-line information center:
http://www.fda.gov/ora/compliance_ref/part11/

Public docket 92s-0251:
http://www.fda.gov/ohrms/dockets/dockets/92s0251/92s0251.htm

FDA's August 2003 "Guidance for Industry - Part 11, Electronic Records; Electronic Signatures - Scope and Application":
http://www.fda.gov/cder/guidance/5667fnl.htm

Audit Data Content with Enterprise Access Management

The data made available by Enterprise Access Management is extremely detailed. It covers the following domains, among others:

Audit of user activity

- Access to an application authorized
- Access refused because of password/ identifier
- Access refused because of time and date requirements (configurable)
- Account blocked because of too many refused attempts, etc.

Audit of user rights allocation activity (early 2007)

- Allocation of access rights (to a resource or group of resources) for a user or group of users
- Creation and modification of profiles
- Allocation of rights specific to a security administrator (based on roles).
- Password change operations, etc.

Note: Enterprise Access Management uses the enterprise's existing user and organization data located in an existing LDAP directory. This feature allows you to keep in place your user management procedures. Therefore, information on users can be obtained by using standard directory tools.

Audit on status of user access rights

- Number of users, groups, access granted
- Suspended accounts, etc.

Detailed requirements

Evidian's Enterprise Access Management provides Identity and Access Management to existing applications (open or closed systems). It can help organizations achieve compliance for their processes. This is explained in the following table.

Unless otherwise noted, the content of the "Evidian Enterprise Access Management feature" column concern the Evidian Enterprise Access Management product. In addition, some answers require the use of the Evidian WAM (Web Access Manager) product.

21 CFR Part 11 paragraph	Requirement	Evidian Enterprise Access Management feature
Subpart B – Electronic records		
11.10	Controls for closed systems. 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. Such procedures and controls shall include the following:	
11.10.a	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	This area will be revised by the FDA, as announced in the August 2003 "Guidance for Industry" document. The FDA states that it does not intend to "impose any additional requirements" in addition to those that already apply outside 21 CFR Part 11. In any case, it is strongly suggested to evaluate if systems validation is useful, even if "there is no predicate rule requirement" for doing so. Systems validation processes typically require auditing in order to trace whether procedures were satisfactorily completed. Enterprise Access Management provides comprehensive audit data on user and administrator activity – see: Audit Data Content with Enterprise Access Management.

11.10.b	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. (...)	Not relevant.
11.10.c	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Enterprise Access Management protects access to the applications that manage the electronic records. Authorized administrators, using role-based methods, may grant access rights that enable retrieval at any time.
11.10.d	Limiting system access to authorized individuals.	Enterprise Access Management limits application and system access to authorized users. Enterprise Access Management is compatible with strong authentication mechanisms, among a variety of authentication mechanisms. Alternatively, Enterprise Access Management can delegate workstation access control to existing procedures (e.g. standard Windows login with Active Directory). With applications written using J2EE, the SAM J2EE module can apply access control to inter-application communications as well.
11.10.e	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	This area will be revised by the FDA, as announced in the August 2003 "Guidance for Industry" document. In particular, the FDA suggests that organizations evaluate which areas to apply audit trails to, based on risk assessments. System and application access and document signing are actions that potentially impact electronic records. Enterprise Access Management records such security and access events in audit files (see Appendix A: Audit Data Content with). The audit entries record the time of the event as well as other information (user identity used, resource etc.) Enterprise Access Management authentication encompasses all record-management applications, both for application access and document signing. This means that a centralized audit trail can be analyzed for these events, even for multi-systems and multi-applications activities. In particular, sequencing of event is much easier to analyze. Enterprise Access Management audit records can be stored for long-term archiving.
11.10.f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Not relevant.
11.10.g	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.	Access control to the system, resources and steps requiring re-authentication is performed through Enterprise Access Management and enforced through centralized rules-based management. Alternatively, Enterprise Access Management can delegate workstation access control to existing procedures (e.g. standard Windows login with Active Directory).
11.10.h	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Users can be restricted to a particular terminal, a set of terminals, or terminals in specific locations. It is possible to enforce rules such as "User A can access application B, but only from workstation C".
11.10.i	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Evidian and its partners provide training classes on Enterprise Access Management. They can also organize on-site training to provide developers and administrators with hands-on experience.
11.10.j	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Not relevant.
11.10.k	Use of appropriate controls over systems documentation including:	
11.10.k.1	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	Not relevant.
11.10.k.2	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Not relevant.

11.30	**Controls for open systems**	
	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, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	For systems that can be accessed through web-based means, the Mobile E-SSO module can systematically encrypt all traffic between users and applications. This ensures the integrity of data transfer. Answers given in 11.10 apply.
11.50	**Signature manifestations.**	
11.50.a	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature	The audit trail generated by Enterprise Access Management allows auditors to access, in a central location, information regarding a signature event: identity of the signer, date/time of signature, and type of signature window. This means that the signature actions can be audited, even centrally, even if the application's own audit files have been altered. It complements the audit trails generated by individual record-management applications.
11.50.b	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Enterprise Access Management audit data can be stored for long-term duration. Procedures and tools used to protect electronic records should be applied to this audit trail as well.
11.70	**Signature/record linking.** Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Because Enterprise Access Management stores centrally an audit file listing the instances of electronic signatures, it provides an additional means of verifying whether a digital signature has been tampered with.
Subpart C – Electronic signatures		
11.100	**General requirements.**	
11.100.a	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Enterprise Access Management can be used alongside strong authentication methods, such as smart cards or USB keys.
11.100.b	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	The identity of the individual is verified by Enterprise Access Management's secure single sign-on process.
11.100.c	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Not relevant.
11.200	**Electronic signature components and controls.**	
11.200.a	Electronic signatures that are not based upon biometrics shall:	
11.200.a.1	Employ at least two distinct identification components such as an identification code and password.	Enterprise Access Management supports a variety of identification methods that include two components, such as ID / password or smart card / PIN code.

11.200.a.1.i	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	Supported. Enterprise Access Management's secure single sign-on process detects partial re-authentication windows issued by individual applications. In that case, the user can be asked to enter his or her password or PIN code again.
11.200.a.1.ii	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	Supported. A time-out period can be configured to end a period of system access forcibly if no action has been performed. When accessing the station after the period has ended, the user must perform full primary authentication again.
11.200.a.2	Be used only by their genuine owners; and	No two users can have the same ID, as Enterprise Access Management uses the enterprise's existing LDAP directory environment. Authentication can be reinforced by strong authentication methods, such as smart cards or USB tokens. Single sign-on can be set up in such a way that the users do not know their IDs and passwords on specific applications. Therefore, they cannot give away these IDs and passwords.
11.200.a.3	Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	Passwords are not visible to administrators. Enterprise Access Management can be configured so that whenever the administrator creates a new user (or changes the user's password) the user must change his or her password. The user is therefore the only one to know his or her primary password. Signing in place of a user would therefore require the cooperation of the user as well as the administrator. In addition, Enterprise Access Management can alert a supervisor whenever a password is created (Feature requires integration services). Lastly, workflow solutions can be implemented to require approval for password changes. This necessitates integration services.
11.200.b	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Enterprise Access Management is compatible with biometric authentication solutions.
11.300	**Controls for identification codes/passwords.** Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	
11.300.a	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	By design, no two users can have the same Enterprise Access Management primary ID. With Enterprise Access Management's secure SSO (Enterprise SSO), "shared accounts" can disappear from the IS.
11.300.b	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Enterprise-wide password policies – including password aging – can be defined and implemented centrally with AccessMaster.
11.300.c	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	The authentication device management features of Enterprise Access Management (Authentication Manager) make it possible to de-authorize and issue replacement of such devices. This requires the Token Manager component of Enterprise Access Management. In addition, Enterprise Access Management's central management capabilities make it possible to quickly remove all authorizations from compromised accounts.
11.300.d	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Detection of an unauthorized attempt at accessing a resource can generate an alert sent to a supervisor. Such security alerts are also logged for later auditing. (Feature requires integration services)
11.300.e	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	Not relevant.

Position Paper

About Evidian

Evidian is the Identity and Access Management (IAM) software suite of Eviden.

Evidian IAM is the European leader in identity and access management with a presence which is growing rapidly beyond Europe, particularly in Japan and the US.

More than 5,000,000 users in more than 900 organizations throughout the world connect to their companies every day and manage their access rights with Evidian identity and access management solutions.

For more information: **www.evidian.com**

CT_J2352_190423_RY_PP_EVIDIANENT