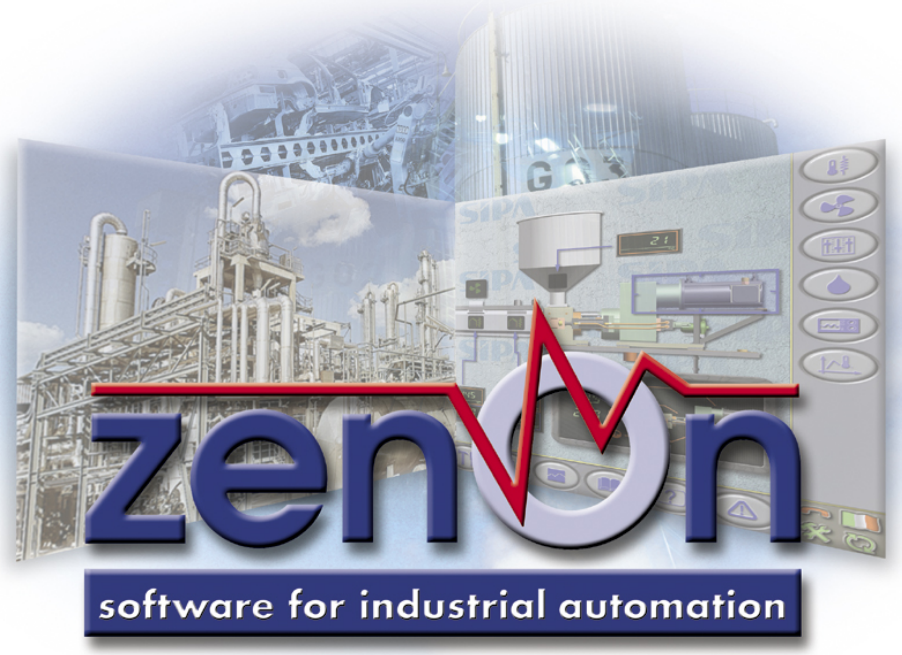

FDA 21 CFR Part 11

History

Date	Comment
January 13th, 2006	Adapted to zenOn version 6.20 (MH)

Contents

Introduction

The American Food and Drug Administration published regulations in 1997 regimenting the electronical storage of data. (Part 11 of the text)

All electronical data recorded in the production of food and drugs have to be in accordance with these regulations.

The audit, if a plant is in accordance with these regulations, is called validitation.

Software products as zenOn cannot be certified or validated themselves. Only the end product (project) of the customer can be validated.

The software product, however, has to offer the functionalities to enable the customer to create a validated project.

In the table below the currently valid text of the regulations (CFR – Code of Federal Regulations) you will also find, which functionalities are offered by the HMI/SCADA system zenOn to realize a project in accordance with 21 CFR Part 11.

If customers stick to these recommendations, their zenOn projects are in accordance with the regulations of the FDA.

We take it as granted that the zenOn projects run in closed systems. Closed systems are systems, which only allow access to qualified personnel responsible for the data. Open systems on the contrary allow access to everybody.

FAQs concerning FDA 21 CFR Part 11

What is 21 CFR Part 11?

Title 21, Code of Federal Regulations, Part 11. Title 21 includes regulations for Food and Drugs. Chapter 1 (parts 1 through 1299) include the U.S. Food and Drug Administration (FDA) part of the U.S. Department of Health and Human Services. Part 11 established the criteria under which electronic records and signatures will be considered equivalent to paper records and handwritten signatures in manufacturing processes regulated by the FDA.

FDA-regulated industries, such as Bio-Pharmaceutical (Human and Veterinary), Personal Care Products, Medical Devices and Food and Beverage, are required to document and acknowledge conditions and events at several points of each manufacturing process to insure exact manufacturing procedures are followed and to produce consistent and repeatable products every time. Signed documents must be reviewed, securely stored and available for review by the FDA. The reviewing of these records was time consuming and required manual searches of the manufacturing information. 21 CFR Part 11 was issued to make this practice more accurate, timely and easier for everyone involved.

What are the benefits of electronic signatures and record keeping?

The benefits of electronic signatures and record keeping are significant. It increases the speed of information exchange and advanced searching capabilities, reduces the cost of record keeping storage space, increases data integration and trending information, improves product quality and consistency, and reduces vulnerability of signature fraud and report misfiling.

When was 21 CFR Part 11 instituted?

The rule was proposed in August, 1994, with a final ruling in March, 1997. It became effective in August, 1997, and the FDA started an aggressive enforcement in January, 2000.

Is packaged software compliant?

Packaged software itself cannot be “compliant”; it is the application that one creates with the packaged software that can become Part 11 compliant. Packaged software should be designed with Part 11 in mind, and have built-in tools for capturing electronic signatures and creating secure electronic records.

Is the FDA currently inspecting for 21 CFR Part 11 violations?

Yes; if you choose to use electronic records that are electronically signed in lieu of paper records, then the FDA can audit your process for Part 11 compliancy and may cite you for failure to comply.

Is the FDA forcing me to be 21 CFR Part 11 compliant?

The FDA is not forcing companies to implement electronic signatures and electronic records. Many companies continue to use paper-based signatures and records. The FDA is enforcing requirements for companies choosing to use electronic signatures and electronic records.

Is this going to be another “Y2K” for FDA-regulated industries?

Y2K had a date set in stone, - midnight December 31, 1999. For Part 11, the due date has past and the clock is ticking. Industry analyst reports indicate that companies are applying more resources and budget to become Part 11 compliant than they did to prepare for Y2K.

Does simply capturing the logged-in system user’s name meet the requirement of “capturing an electronic signature”?

No. The currently logged-in user isn’t necessarily the person performing or verifying an operation. Applications should be designed to ensure point verification for each operation.

What are the benefits of “Continuous Use”?

Continuous Use allows for the entry of electronic signatures using only a single token for a short period of time after a signature has been executed with two signatures. Continuous Use requires several controls around its use, and does not remove the need for an operator to execute a signature, to capture the users “Printed Name” and the meaning of that signature. Using the current logged on UserID does not constitute an electronic signature under continuous use.

Where in my manufacturing process does 21 CFR Part 11 compliancy apply?

Part 11 compliancy applies wherever electronic records are used in lieu of paper records.

Can I get by with having my integrator put in a software patch?

No; Part 11 is not merely an integration issue. The regulations require security management beyond the “industry standard”, as well as secured audit trails of alarms and event logs, and point-based verification of the user.

What is 21 CFR Part 11? (http://www.part11.co.uk/)

The pharmaceutical industry has always relied heavily on paper based records, many of which are required by law to be signed by qualified personnel. In fact, regulations with which the industry must comply in order to market drugs in certain countries demanded hand-written signatures on paper records.

In 1991 members of the pharmaceutical industry met with the FDA to discuss how electronic systems could be used within existing Good Manufacturing Practice (GMP) regulations. A FDA task force was formed which, in consultation with the industry, developed a new set of regulations which eventually came into force in August '97.

So why has the industry taken so long to come to terms with this rule? Firstly, there has been some confusion as to the applicability of Part 11 (see below) and the full scope is only just being realized by many companies. In addition, with considerable effort being directed at Year 2000 compliance, 21 CFR Part 11 has, in many environments been neglected.

Where Does Part 11 Apply?

Part 11 applies to all GxP (i.e. GMP, GLP and GCP) IT systems that create, modify, maintain, archive or retrieve electronic records. If your organization is a pharmaceutical, biological or medical device manufacture whose products are for sale within the USA then Part 11 applies to **YOU**!

A **common misconception** is that Part 11 applies only to the use of **electronic signatures** in GxP critical applications, where the hand-written, pen on paper signature is replaced by an electronic equivalent, i.e. entry of a unique ID/password combination.

While Part 11 does indeed cover the use of electronic signatures, it also applies to **electronic records**, i.e. the original data file from which the printed copy was obtained.

Part 11, therefore affects **every** GxP critical computer system producing electronic records (data files) in use since 20 Aug 97, even if the primary output of the system is a printed, hand-signed paper record.

21 CFR Part 11 is a 38 page document, with the **last 4 pages** containing the rule itself and the preceding 34 pages, known as the preamble.

The following is a brief summary and is intended to give an overall impression of the scope of the rule:

Electronic Records

Validation	All computer related systems must be validated to GxP Guidelines.
Retention	Electronic records must be retained and be retrievable for as long as the requirement for the equivalent paper record.
Security	Access to electronic records must be restricted to authorized personnel only.
Audit Trail	All operator entries that create, modify or delete an electronic record must be recorded in a secure, computer generated audit trail identifying who did what and when.

Electronic Signatures

Signature Form	Both biometric (i.e. fingerprint, retinal scan) and non-biometric (ID/password entry) signatures are acceptable. Part 11 lists many specific requirements for ID code/password signatures.
Signature Content	The e-signature should contain the signer's printed name, meaning of

	signature (approved, rejected, etc.) and the date and time of the signature execution.
Signature / Record Link	The e-signature must be linked to the e-record to which it applies. This is to ensure that the e-signature cannot be transferred to other e-records.

Enforcement

FDA Compliance policy **Guide 7153.17** which provides guidance for the FDA enforcement policy on 21 CFR part 11, states that companies should have a reasonable timetable for promptly modifying any systems not in compliance (including legacy systems) to make them Part 11 compliant and should be able to demonstrate progress in implementing their timetable.

This stresses the importance for a site to have a plan in place for identifying, assessing and ensuring compliance with Part 11for all GxP critical computer systems.

What About Europe?

21 CFR Part 11 applies only to companies whose products are for sale within the USA. However, regulatory bodies in other countries are watching closely and are likely to adopt similar standards.

An **Electronic Signature directive 1999/93/EC** published December 1999, establishes a legal framework for the use of electronic signatures. It was implemented into UK law May 2000 in the Electronic Communication Bill.

21 CFR Part 11 and how zenOn complies

21 CFR PART 11—ELECTRONIC RECORDS;

ELECTRONIC SIGNATURES

Subpart A—General Provisions

Sec.

11.1 Scope.

11.2 Implementation.

11.3 Definitions.

Subpart B—Electronic Records

11.10 Controls for closed systems.

11.30 Controls for open systems.

11.50 Signature manifestations.

11.70 Signature/record linking.

Subpart C—Electronic Signatures

11.100 General requirements.

11.200 Electronic signature components and controls.

11.300 Controls for identification codes/pass-words.

AUTHORITY: 21 U.S.C. 321–393; 42 U.S.C. 262.

SOURCE: 62 FR 13464, Mar. 20, 1997, unless otherwise noted.

Subpart A—General Provisions

§ 11.1 Scope

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full hand-written signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily avail-able for, and subject to, FDA inspection.

§ 11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S–0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public dock-et will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the in-tended agency receiving unit for de-tails on how (e.g., method of trans-mission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

§ 11.3 Definitions

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual’s identity based on measurement of the individual’s physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

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

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means 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.

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

(9) *Open system* means 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.

Regulation Section	Regulation Text	zenOn
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.	Customers must validate the applications. Customers may develop and/or execute the validation plans and protocols themselves or outsource these activities.
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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	All data in zenOn are saved in own proprietary file formats. There are four different ways to access to the data: Integrated tools of zenOn as: Report Generator, Archive revision, Alarm- and CEL adminsitration. Data can be exported into different formats (dBase, Ascii/CSV, XML) and then be processed in external programs. Data can directly be stored in a relational SQL database. External programs can access data there. Data can be printed in PDF format and then be archived.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention pe-	Data are stored in zenOn specific files, which can be secured by the security

	riod.	system of the Windows file system. Customers should establishing policies and procedures to ensure that records are retained for an appropriate duration of time.
11.10 (d)	Limiting system access to authorized individuals.	To limit system access, zenOn should be configured to use Windows NT/2000/XP security. NT/2000/XP account policies should implement password aging, minimum password length, password uniqueness, and account lockout after a reasonable number of unsuccessful login attempts. Internal zenOn security should be used to limit user access to authorized security areas and applications. Also for zenOn users limited password validity and minimal password length should be activated. Each zenOn project should be configured to logout the user after a certain time. The program “Keyblock Runtime Start” should be used to avoid prohibited access to the operating system.
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.	Every user action effecting recorded data is protocolled. All audit trail records include date and time stamp, node of origination, and operator name. zenOn has a built in clock synchronization to ensure that all date and time stamps are accurately recorded in the audit trail.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Sequencing of steps and events can be developed individually by the project engineer as appropriate within zenOn editor.
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.	To limit system access, zenOn should be configured to use Windows NT/2000/XP security. NT/2000/XP account policies should implement password aging, minimum password length, password uniqueness, and account lockout after a reasonable number of unsuccessful login attempts. Internal zenOn security should be used to limit user access to authorized security areas and applications. Also for zenOn users limited password validity and minimal password length should

		be activated. Each zenOn project should be configured to logout the user after a certain time.
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.	Data input can be restricted to defined stations. The station on which an action is executed can be protocolled. zenOn client/server architecture restricts data storage to the server computer, only, ensuring that the audit trail is generated from a single location. All zenOn drivers include statusinformation about the quality of the connection and the quality of each individual value. The same mechanism works also in the zenOn network for Client/Server and Redundancy communication.
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.	It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task.
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.	It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task.
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.	It is the responsibility of the customer to ensure that the controls are in place to limit the distribution of, access to, and use of documentation for system operation and maintenance.
11.10 (k-2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	It is the responsibility of the customer to ensure that revision and change control procedures are in place to maintain an audit trail that documents time-sequenced development and modification of systems documentation.
11.50	**Signature manifestations**	
11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	
11.50 (a-1)	The printed name of the signer;	All audit trail records (AML and CEL) include date and time stamp, node of origination, and operator name.
11.50 (a-2)	The date and time when the signature was executed;	All audit trail records (AML and CEL) include date and time stamp, node of origination, and operator name.
11.50 (a-3)	The meaning (such as review, approval, responsibil-	All audit trail records in the Alarm List include the name of the variable, iden-

	ity, or authorship) associated with the signature.	tification, limit violation text, and a commentary field that can be used to ascertain the meaning of the activity. All sytem messages are self-explaining. (For example, an operator message is interpreted as an operator action, while an alarm record results from an operator acknowledgement.)
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).	All data in zenOn are saved in own proprietary file formats. There are four different ways to access to the data: Integrated tools of zenOn as: Report Generator, Archive revision, Alarm- and CEL adminsitration. Data can be exported into different formats (dBase, Ascii/CSV, XML) and then be processed in external programs. Data can directly be stored in a relational SQL database. External programs can access data there. Data can be printed in non changeable formats like PDF Reports.
11.70	**Signature/record linking.** Electronic signatures and hand-written 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.	Each audit trail record includes the name of the operator linked to the specific activity. Customers should also establish policies and procedures to prevent unauthorized access to audit trail files (AML, CEL), which can be done with the security system of the Windows file system.
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.	Windows NT/2000/XP security and the zenOn internal security do not permit the creation of duplicate user IDs. Customers using zenOn applications in FDA-regulated environments must be responsible for ensuring that electronic signatures are unique to one individual and not reused by or reassigned to any other individual.
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.	Customers using zenOn applications in FDA-regulated environments must be responsible for verifying the identities of individuals using electronic signatures.
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	Customers using zenOn applications in FDA-regulated environments must be responsible for verifying the identities of individuals using electronic signa-

	binding equivalent of traditional handwritten signatures.	tures.
11.100 (c-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.	Customers using zenOn applications in FDA-regulated environments must be responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.
11.100 (c-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.	It is the responsibility of the customer to, upon agency request provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.
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. prevent unauthorized use of passwords and/or identification codes, and to detect	The zenOn user adminsitration as well as the NT/2000/XP user adminsitration demand the input of user-id (name) and password. Additionally logging in with an electronical ident system can be integrated (e.g. chipcard).
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.	To indicate the start of a continuous period of controlled system access, the user must use User-Id and Password to log into zenOn. For subsequent signatures during this period the zenOn security requires the user to enter all signature components. The zenOn User Login Timeout period should be configured to limit the extent of a continuous period of controlled system access. Customers should also implement policies and procedures requiring users to log out of the application during periods of non-use.
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.	The zenOn User Login Timeout period should be configured to limit the extent of a continuous period of controlled system access. Customers should also implement policies and procedures requiring users to log out of the application during periods of non-use. The user has to enter all signature components for all signings by default.
11.200 (a-2)	Be used only by their genuine owners;	Customers using the zenOn applications in FDA-regulated environments

		must be responsible for ensuring that non-biometric electronic signatures are used only by their genuine owners.
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.	Customers using the zenOn applications in FDA-regulated environments must be responsible for ensuring that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. For example, user organizations may require that system administrators enable the Windows NT security function "User Must Change Password at Next Logon" in order to prevent the system administrators from knowing both the user's user ID and password. If the administrator reset the password, zenOn security demands a new password the next time the user logs in.
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. issuance amendment, or revocation of an order.	Biometric devices are readily available from 3rd party vendors. However, Customers using the zenOn applications in FDA-regulated environments, or any organization that may develop biometric devices for interfacing with the audited applications, must be responsible for ensuring that electronic signatures based upon biometrics are designed to ensure that they cannot be used by anyone other than their genuine owners.
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.	The zenOn and the Windows security maintain the uniqueness of each user ID and password combination.
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).	The zenOn and the Windows security shall be configured to use the functionality for password aging and uniqueness.
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.	Customers using the zenOn applications in FDA-regulated environments must be responsible for employing controls to ensure the security and integrity of identification codes and passwords.
11.300 (d)	Use of transaction safeguards to prevent unauthor-	Each successful and unsuccessful login

	ized 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.	attempt in zenOn is recorded to the CEL. zenOn has to be configured in a way, that after a certain number of wrong password inputs the user resp. after a certain number of wrong user ID inputs the system is locked.
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.	Customers using the zenOn applications in FDA-regulated environments, or any organization that may develop devices that bear or generate identification code or password information to interface with the audited applications, must be responsible for ensuring that devices that bear or generate identification code or password information be tested to ensure that they function properly and have not been altered in an unauthorized manner.