PLA 3.0

21 CFR PART 11 – ELECTRONIC RECORDS, ELECTRONIC SIGNATURES

COMPLIANCE OF PLA 3.0

21.11.2013

PLA 3.0

21 CFR PART 11 – ELECTRONIC RECORDS, ELECTRONIC SIGNATURES
COMPLIANCE OF PLA 3.0

This document describes the compliance of Stegmann Systems software package PLA 3.0 with the FDA regulation 21 CFR Part 11 – Electronic Records; Electronic Signatures.

The document is divided into three parts that are provided by the original document. The first part (Subpart A – General Provisions) is the only part which remains not commented. The following chapters contain the current text of the 21 CFR Part 11 rule along with a corresponding description or comment on how PLA 3.0 meets the appropriate specifications in the regulation.

PLA 3.0 is a 21 CFR part 11 compliant software. However to create a 21 CFR part 11 solution with PLA 3.0, several regulations on the customer side need to be defined.

SUBPART A--GENERAL PROVISIONS

SEC. 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 handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after
(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 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 available for, and subject to, FDA inspection.

SEC. 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 docket 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 intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

SEC. 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 devices 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.

PLA 3.0

SUBPART B--ELECTRONIC RECORDS

SEC. 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:

21 CFR PART 11	YES	NO	N/A	COMMENT
a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	X			Beside the internal development documentation, the optional Validation Package lists more than 2500 pages of printed reference material and procedures (IQ, OQ and PQ) to ensure accuracy and reliability. The ability to discern invalid or altered records is realized by the internal PKI of PLA.
(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.	X			PLA is able to generate complete copies of records in both human readable and electronic form. The software is able to create a complete database backup (electronic form) or to produce reports that contain the whole information in a human readable form (PDF documents).
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	X			PLA has an integrated backup and restore feature for a complete database backup. Alternatively the customer can save the PLA database file on a network attached drive and backup the file with external tools (backup software). PLA is able to restore the database without compromising the data integrity, which is secured by the internal PKI of PLA.
(d) Limiting system access to authorized individuals.	X			PLA has an integrated user account management and controls the access to the PLA system by a unique user ID and a secret password. User groups are implemented to allow a detailed rights management.
(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.	X			PLA provides a secure, computer generated and time-stamped audit trail. All required information and features of the audit trail are supported by PLA. The audit trail information is saved within the PLA database and is therefore retained with the electronic records.

PLA 3.0

21 CFR PART 11	YES	NO	N/A	COMMENT
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	X			PLA does not allow altering the sequence of the analysis steps; therefore this aspect is fulfilled.
(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.	X			With the integrated user account management the access to the PLA system is controlled and only authorized individuals have access to the system.PLA ensures the access to the PLA database through its internal PKI.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	X			Our optional Import Modules, which are intended for the easy and secure transfer of external data into the PLA system, carry out strict checks on the raw data format. If the raw data that should be imported cannot be identified securely, the import process is being stopped.
(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.			X	The implementation of such rules is the administrative responsibility of the customer.
(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.			X	The establishment of such policies is the administrative responsibility of the customer.
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.			X	The implementation of these controls is the administrative responsibility of the customer.

SEC. 11.30 CONTROLS FOR OPEN SYSTEMS

21 CFR PART 11	YES	NO	N/A	COMMENT
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 Sec. 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.			X	As defined in Sec. 11.3 paragraph (4) and (9) PLA is a closed system and this section does not apply. For information on closed systems, see Sec. 11.10.

SEC. 11.50 SIGNATURE MANIFESTATIONS.

21 CFR PART 11	YES	NO	N/A	COMMENT
(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.	X			PLA provides electronic signatures that clearly indicate the username, timestamp and the meaning of the signature. In order to sign an electronic record the user has to enter his password.
(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).	X			If an electronic signature is applied to an electronic record this information will be printed out with the resulting report in a human readable format.

SEC. 11.70 SIGNATURE/RECORD LINKING.

21 CFR PART 11	YES	NO	N/A	COMMENT
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.	X			The electronic signature that is applied to an electronic record is stored as a secured XML document representing the record and is prevented from modification.

PLA 3.0

SUBPART C--ELECTRONIC SIGNATURES

SEC. 11.100 GENERAL REQUIREMENTS.

21 CFR PART 11	YES	NO	N/A	COMMENT
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	X			PLA authenticates individuals by a unique username and a secret password. If the confidentiality of the password is ensured, the authentication of individuals complies with the regulation.
(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.			X	The verification of an individual's identity is the administrative responsibility of the customer.
(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.			X	The implementation of such regulations is the administrative responsibility of the customer.

SEC. 11.200 ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS.

21 CFR PART 11	YES	NO	N/A	COMMENT
(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (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. (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.	X			The PLA user authentication is based on both - an identification code and a password. During the login process both identification components (username and password) are required. The customer can decide by a database security policy, whether the user has to enter his username again or not. For all subsequent operations the password is required in any case.
(2) Be used only by their genuine owners; and	X			If the confidentiality of the password is ensured, the authentication of individuals complies with the regulation.
(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.	X			Each signature in PLA is designed to be executed by its genuine owner only. For any administrative purposes the collaboration of two individuals (PLA administrator and genuine owner) is required.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.			X	PLA does not support electronic signatures based on biometry, therefore this point is not applicable.

PLA 3.0

SEC. 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:

21 CFR PART 11	YES	NO	N/A	COMMENT
(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.	X			It is not possible to generate two PLA user accounts with identical usernames.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	X			PLA supports detailed password aging and complexity rules. The implementation and maintenance of such schedules is the administrative responsibility of the customer.
(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.	X			PLA does not support any devices for the storage and/or generation of identification codes or passwords. All PLA accounts (usernames and respective passwords) can de deauthorized by the PLA system administrator.
(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.	X			All system activities including any security violations are logged within the system audit trail.
(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.			X	PLA does not use any devices for the storage and/or generation of identification codes or passwords.