Thermo Scientific Qtegra Intelligent Scientific Data Solution (ISDS) Software for 21 CFR Part 11 Compliant Laboratories

Key Words

Compliance, Electronic Records, 21 CFR Part 11

Goal

Demonstrate the tool set provided in Qtegra ISDS for operation in 21 CFR Part 11 compliant laboratories.

Introduction

Part 11 of Title 21 of the "Code of Federal Regulations; Electronic Records; Electronic Signatures" (21 CFR Part 11) includes the United States federal guidelines for storage and protection of electronically stored data and the application of electronic signatures. These guidelines have been developed to ensure that electronic records are reliable, authentic and comprehensible.

This document examines all sections of the code and describes how the Thermo Scientific™ Qtegra™ Intelligent Scientific Data Solution™ (ISDS) Software supports 21 CFR Part 11 compliant environments. The new Qtegra ISDS Software platform provides a wide range of features, which enable laboratories to operate within total FDA compliance. These features include audit trails, support for electronic signatures and tools for integrated data managements.

Part 11 Electronic Records; Electronic Signatures

Subpart B - Electronic Records

21 CFR Sec. 11.10 Description		Comment
Sec. 11.10	**Controls for Closed Systems**	**Part B of Electronic Records**
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Thermo Scientific products are developed in accordance to an established New Product Development and Introduction process (NPDI). This provides a continuous phase/gate review. All documents are stored in Microsoft™ SharePoint™ and therefore subject to a complete history. All development items are tracked in a fully auditable database. Each item is linked to a test case and outcome. Qtegra ISDS Software is subjected to automated testing procedures including regression testing, followed by installation, functional, alpha and beta testing. All software releases are subject to full validation processes.
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 a review and copying of the electronic records.	Qtegra ISDS Software stores records in both native format and human, readable format. Electronic records can be printed.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Qtegra ISDS Software has all the necessary functionality to provide safe and secure processing. The software ensures total compliance with regulations and includes a compliance expert system with rules for password creation and user rights management.
11.10 (d)	Limiting system access to authorized individuals.	Each user must be assigned to a group with defined privileges. The user has only access permission to that group to which they have been assigned.

Thermo SCIENTIFIC

21 CFR Sec. 11.10	Description	Comment
Sec. 11.10	**Controls for Closed Systems**	**Part B of Electronic Records**
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.	Complete histories of changes in records are available and can be compared at any time, from version to version. Comments on the changes can also be manually inserted. In addition, all deletions, amendments or moving of the record will be documented. Complete trails can be inspected and exported (see Figure 2).
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Qtegra ISDS Software follows a clear, structured sequence of process, which ensures that the workflow is performed in the correct order. For example, it is not possible to store a document without user authentication and a reason entered for any amendments to the document. Another example is the forced protocol fidelity in the Sample List where the user must follow a defined number of sample for standardization of quality checks.
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.	All users must log in into the system prior to accessing it with a unique name and password combination. All subsequent changes in the system are marked with unique name.
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.	Qtegra ISDS Software operates in remote mode via Windows message queues. This component is not subject to the same safety criteria as a direct log in to the system. It is expected to establish such a link in the same credentials.
11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems has the education, training, and experience to perform their assigned tasks.	This is the responsibility of the user and should be controlled by user created procedures and documentation.
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.	This is the responsibility of the user and should be controlled by user created procedures and documentation.
Sec. 11.30	**Controls for Open Systems**	**Comment**
11.30	Person 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.	Records are subject to a 256-bit AES encryption and can only be decrypted with Qtegra ISDS Software.

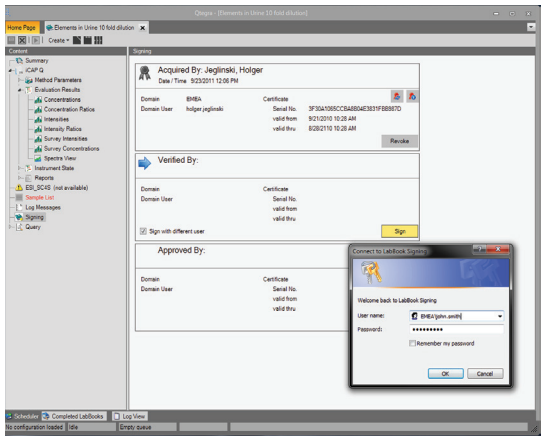

Figure 1. Example of electronic signature and verification process.

Sec. 11.50	Signature Forms	Comment
11.50 (a)	Signed electronic records shall contain information associated with 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; (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Users have the option to sign records electronically. The electric signature is encrypted with a time stamp embedded in the record. See Figures 1 and 2.
11.50 (b)	The conditions in paragraph (a) (1-3) concepts described in this section shall be subject to the same controls as electronic records and as part of any human readable form of electronic recording should be included.	Electronic signatures are subject to the same version control as the record itself. Electronic signatures will be displayed on screen and in print.

Sec 11.70	Connection Signature/Document	Comment
	Electronic signatures and handwritten signatures are the electronic record of a running analysis that should to ensure that the signatures do not cut, copied or otherwise transferred to falsify an electronic record by ordinary means.	Electronic signatures are inextricably embedded in the encrypted file. The signature is uniquely qualified with the the document and has no relevance to other documents.

Subpart C - Electronic Signatures

Sec. 11.100	Electronic Signatures	Basic Requirement
	(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. (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. (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, 12420 Parklawn Drive, RM 3007 Rockville, MD 20857.	In priniciple, electronic signatures are validated with digital certificates. The company can build its own infrastructure for assigning digital certificates or commercial vendors such as VeriSign, GlobalSign, Thawte and CAcert.

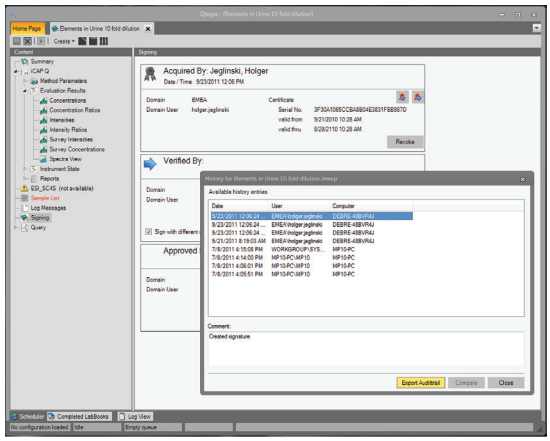

Figure 2. Export of audit trail.

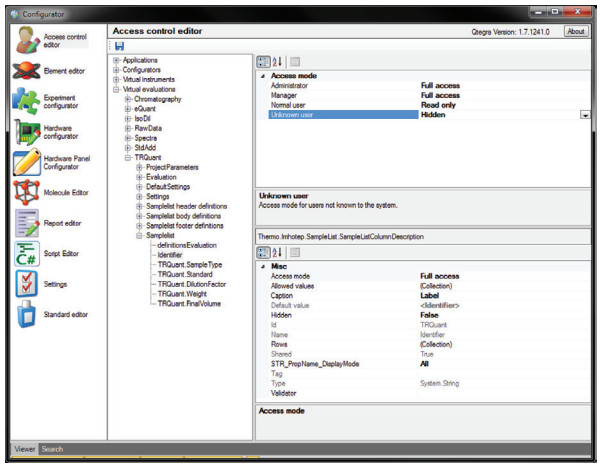

Figure 3. Access control editor.

Sec. 11.200 Components for Electronic Signatures and Controls		
	(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.	A combined user ID and password is required to log in into the system.
	(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.	A combined user ID and password is required to log in into the system. The signature award is presented by the confirmation of the password.
	(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.	After logging out, the user is required to log back into the system with a combination of the user ID and password.
	(2) Be used only by their genuine owners.	
	(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.	The user ID and password must be kept confidential by the owner. User ID must be unique with only one user of each ID allowed on the domain, as per Windows authentication and the system administrator settings. Users are instructed to change their password to one that is known only to them.
	(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Qtegra ISDS Software does not currently support biometric signatures.

Sec. 11.300 Components for Electronic Signatures and Controls	
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:	
(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 user ID and password must be unique. This is ensured by Microsoft Windows and the administrator.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Qtegra ISDS Software uses the Windows domain controller for password control. The network administrator should ensure that the Windows domain controller is configured to ensure that this criteria is met.
(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.	N/A
(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.	All log in and log off attempts are documented. A report is generated if a failed log in attempt is made.

thermofisher.com/Qtegra-ISDS

Africa +43 1 333 50 34 0
Australia +61 3 9757 4300
Austria +43 810 282 206
Belgium +32 53 73 42 41
Canada +1 800 530 8447
China 800 810 5118 (free call domestic)
400 650 5118
Denmark +45 70 23 62 60
Europe-Other +43 1 333 50 34 0
Finland +358 10 3292 200
France +33 1 60 92 48 00
Germany +49 6103 408 1014
India +91 22 6742 9494
Italy +39 02 950 591
Japan +81 45 453 9100
Korea +82 2 3420 8600
Latin America +1 561 688 8700
Middle East +43 1 333 50 34 0
Netherlands +31 76 579 55 55
New Zealand +64 9 980 6700
Norway +46 8 556 468 00
Russia/CIS +43 1 333 50 34 0
Singapore +65 6289 1190
Spain +34 914 845 965
Sweden +46 8 556 468 00
Switzerland +41 61 716 77 00
UK +44 1442 233555
USA +1 800 532 4752

Thermo SCIENTIFIC
A Thermo Fisher Scientific Brand

TN43106-EN 0316S