Test report issued under the responsibility of:

EVALUATION REPORT
CFR – Code of Federal Regulations Title 21

Evaluation Report number. .....:	CFR21ODINS180101.00
Approved by (name + signature).....: Technical Director (Document signed by means of electronic signature)	David Latorre
Date of issue .....:	16-10-2019
Total number of pages .....:	10
Applicant's name.....:	Odin Solutions, S.L
address.....:	C/ Perú, 5, 3º, Oficina 12 30820 Alcantarilla (Murcia – Spain)
Evaluating laboratory.....:	TECNOCREA, S.L.
Address .....:	C/ Sèquia de Benàger, 23 Pol. Ind. Alquería de Moret 46210 Picanya (Valencia – Spain)
Evaluation specifications:	
Standard.....:	CFR – Code of Federal Regulations Title 21 (April 1 2018)
Test procedure .....:	Internal verification
Non-standard test method.....:	N/A
Evaluation Report Form No.....:	03CFR2_01
Evalutation Report Form(s) Originator ..:	Tecnocert
Master Evaluation Report Form .....:	Dated 09-2019

The reflected results are property of the applicant and without his/her previous authorisation they will not be communicated to a mediator.

Evaluationg laboratory accepts no responsibility for damages resulting for use or improper interpretation of the information contained in this document.

Evaluating laboratory accepts no responsibility for the information provided by the applicant.

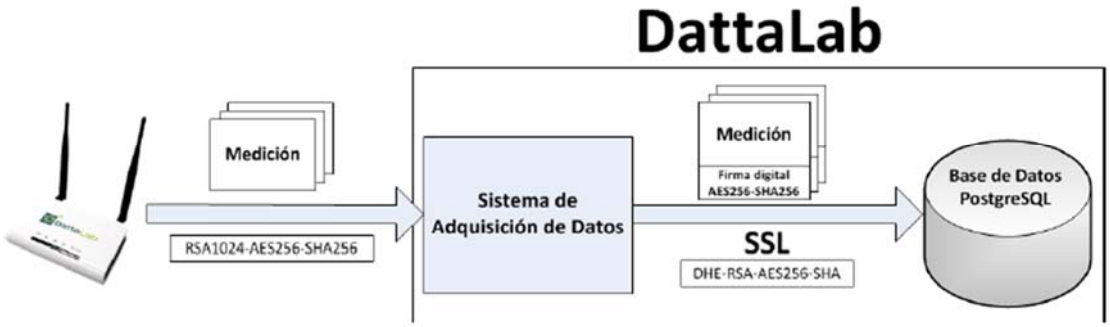
Description.....:	Temperature datalogger continuous in time
Trade mark .....:	DattaLab
Developer .....:	Odin Solutions, S.L.
Software version.....:	2.01
User Manual version .....:	Rev. 5 (Oct. 2019)

Evaluation performed (name of test and clause):	**Evaluation locations:**

- CFR Title 21 evaluation (April 1 2018):
  - Subpart B: Electronic records
  - Subpart C: Electronic signatures
	ODIN SOLUTIONS, S.L.
	Universidad de Murcia
	Campus Universitario de Espinardo, s/n
	Nave de Informática B1.0.006
	30100 - Espinardo (Murcia)
	
	TECNOCREA, S.L.
	C/ Sèquia de Benàger, 23
	Pol. Ind. Alquería de Moret
	46210 Picanya (Valencia – Spain)

Evaluation:	
Date (s) of evaluation .....:	01-10-2019 / 14-10-2019
Possible evaluation case verdicts:	
- evaluation case does not apply to the system .....:	N/A
- evaluation object does meet the requirement.....:	P (Pass)
- evaluation object does not meet the requirement:	F (Fail)
- evaluation object not performed.....:	N/E (Not evaluated)
General remarks:	
The results presented in this report relate only to the version of software tested. This report shall not be reproduced, except in full, without the written approval of the issuing testing laboratory. "(See Enclosure #)" refers to additional information appended to the report. "(See appended table)" refers to a table appended to the report.	
General information:	
Software evaluated .....:	DattaLab
Version .....:	2.01
Hardware acquisition data accessories .....:	Datalogger (CexLab) Radio Receiver (RexLab) Radio module Receiver (Rex Lab) Ethernet module
Acquisition data accessories firmware version .....:	Datalogger (CexLab) Radio: 2.11 Receiver (RexLab) Radio module: 2.11 Receiver (Rex Lab) Ethernet module: 2.11
User manual version .....:	Rev. 5 (Oct. 2019)

DattaLab – Scheme and description:



- Communication between Receiver and Data Acquisition System (DAS) is done by secure connection based on RSA1024_AES256_SHA256 algorithm. This communication is done using an UDP protocol proprietary of Odin Solutions which uses RSA1024 to negotiate the AES256 keys. These symmetric keys are used to encrypt the communication between Receiver and DAS.

- Communication between DAS and Data Base (DB) PostgreSQL is done using a SSL connection encrypted with DHE-RSA-AES256-SHA algorithm.

- DAS store records from Receiver in the DB PostreSQL together with their electronic signature using encryption algorithm AES256-SHA256. Records stored in DB are:
  - Timestamp
  - ID of the measure device
  - Value measured
  - Data regarding configuration

Electronic signature is obtained by calculating a hash SHA256 from the AES256 coding of records. Electronic signature is stored in the DB encrypted in base64.

DattaLab software runs continuously in the Server where it is installed. An USB Unikey Drive license key is necessary to be plugged in the Server to execute Datta Lab software.

DattaLab software runs automatically when Server is switched on if licence key is plugged in without intervention of any user.

User manual (rev. 5) has been evaluated together with DattaLab software. Some CFR Title 21 requirements must be implemented by final user. For these requirements it has been evaluated that the user manual informs the user about them.

CFR – Title 21 Evaluation			
Clause	Requirement	Result - Remark	Verdict
	SUBPART B- ELECTRONIC RECORDS		—
Sec. 11.10	**Controls for closed systems**		—
	Procedures and controls include:		—
(a)	Validation of system to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records.	Communication between data acquisition system and receiver is encrypted using RSA1024_AES256_SHA256. Communication between data acquisition system and the data base PostgreSQL is also encrypted using DHE-RSA-AES256-SHA. Software does not include any function to modify records.	P
(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.	'.csv' format files of records can be generated.	P
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Software does not include any option for deleting records. Records are stored in the server which runs the software. Records retention period depends on capacity of server where software is installed.	P
(d)	Limiting system access to authorized individuals	Once software is installed it runs automatically when server is switched on. Only authorized individuals can access to checking, copying or download records in '.csv' format.	P

CFR – Title 21 Evaluation			
Clause	Requirement	Result - Remark	Verdict
(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.	Once software is installed it runs automatically when server is switched on. Recording temperature data does not depend on users. Users are only allowed to check, copy or download records. All records are provided with timestamp related with date, time and action. Only 'create' action is possible. Software does not allow to modify or delete records. This information is encrypted and stored together with the recorded data.	P
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	To be implemented by final user. User manual includes information about this requirement.	P
(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.	Only authorized individuals can access the system, each user has a different password. Users does not sign records; they are signed automatically by the system which is continuously acquiring temperature data. Software does not allow the option of record modification. No operations at hand can be made.	P
(h)	Use of device checks to determine, as appropriate, the validity of the source of data input or operational instruction.	To be implemented by final user. User manual includes information about this requirement.	P
(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.	To be implemented by final user. User manual includes information about this requirement.	P

CFR – Title 21 Evaluation			
Clause	Requirement	Result - Remark	Verdict
(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.	To be implemented by final user. User manual includes information about this requirement.	P
(k)	Use of appropriate controls over systems documentation including:	Software is provided with user manual. Controls over system documentation should be implemented by final user. User manual includes information about this requirement.	P
	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	User manual includes information about this requirement.	P
	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	User manual includes information about this requirement.	P
Sec. 11.30	**Controls for open system systems**	System is classified as closed system by the manufacturer.	—
Sec. 11.50	**Signature manifestations**		—
(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:		—
	The printed name of the signer	Signatures are made by the software. Users does not sign records. Software is running and recording temperature registers continuously.	N/A
	The date and time when the signature was executed; and		P
	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.		N/A
(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 records are provided with timestamp related with date, time and action. Software signature is made over records and timestamp information.	P
Sec. 11.70	**Signature/record linking**		—

CFR – Title 21 Evaluation			
Clause	Requirement	Result - Remark	Verdict
	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.	Software electronic signatures are linked to electronic records. Signature is unique for each record because it is based on the information contained in the record and timestamp among others. Signatures cannot be excise, copied or transferred by ordinarily means.	P
	SUBPART C- ELECTRONIC SIGNATURES		—
Sec. 11.100	**Controls for closed systems**		—
(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Software signs each register. Signature for each register is unique. Once software is installed it runs automatically when server is switched on. Recording temperature data does not depend on users. Users are only allowed to check, copy or download records or some uses can also perform administration tasks.	N/A
(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.	Users allowed to access the system and their passwords should be verified by final user. User manual includes information about this requirement.	P
(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.	To be implemented by final user. User manual includes information about this requirement.	P
	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.		P
	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.		P

CFR – Title 21 Evaluation			
Clause	Requirement	Result - Remark	Verdict
Sec. 11.200	**Electronic signature components and controls**	Software signs each register. Signature for each register is unique. Once software is installed it runs automatically when server is switched on. Recording temperature data does not depend on users. Users are only allowed to check, copy or download records or some uses can also perform administration tasks. These tasks and controls are not related with records covered by CFR-21 but some of the requirements of CFR-21 has been applied. They will be evaluated in the following subsections.	—
(a)	Electronic signatures that are not based upon biometrics shall:		—
	Employ at least two distinct identification components such as an identification code and password.	User identification and password are needed to identify each user	P
	(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.	Users do not sign records	N/A
	(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.	Users are automatically logged out after inactivity for 2 minutes. After that, user and password should be provided again	P
	Be used only by their genuine owners; and	To be implemented by final user. User manual includes information about this requirement.	P
	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.		P
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	No biometrics signatures implemented	N/A

CFR – Title 21 Evaluation			
Clause	Requirement	Result - Remark	Verdict
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:	Software signs each register. Signature for each register is unique. Once software is installed it runs automatically when server is switched on. Recording temperature data does not depend on users. Users are only allowed to check, copy or download records or some uses can also perform administration tasks. These tasks and controls are not related with records covered by CFR-21 but some of the requirements of CFR-21 has been applied. They will be evaluated in the following subsections.	—
(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.	To be implemented by final user. User manual includes information about this requirement.	P
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).		P
(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.	To be implemented by final user. User manual includes information about this requirement.	P

CFR – Title 21 Evaluation			
Clause	Requirement	Result - Remark	Verdict
(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.	To be implemented by final user. To prevent unauthorized access if the use of wrong passwords for a user access is detected it is reported to a warning log file with information about user, date and time of the event. The administrator of the system is the responsible for checking this log and inform to the organizational management. User manual includes information about this requirement.	P
(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.		N/A