Authors : C.Flachard – P.Rinaudo
Document reference : COM-0794 v1.00
Update date : 2015 May 23th

21 CFR 11 COMPLIANCE for Qubes software

1. Executive Summary

a. 21 CFR Part 11: Electronic Record; Electronic Signatures

Life Sciences companies in the GMP regulated environment that are using a Manufacturing Execution System need robust security administration to comply with U.S. Food and Drug (FDA) Administration's 21 Code of Federal Regulations (CFR), Part 11, concerning electronic records and electronic signatures. The 21 CFR Part 11 is a comprehensive piece of legislation that outlines the controls necessary for the regulated industry to utilize electronic records and electronic signatures.

References:
Guidance for Industry, Part 11, electronic Records; Electronic Signatures – Scope and Application (Part 11 Final Guidance Issued)
TITLE 21—Food and Drugs, Chapter I—Food and Drug Administration, Department of Health and Human Services – General, Part 11 Electronic Records; Electronic Signatures (21CFR11)

b. 1.2 Compliance with part 11

From the very start of Qubes software, Creative IT development team has taken into account the 21 CFR 11 requirements. But, it is not possible for any vendor of software systems to offer a turnkey 'Part 11 compliant system'. Part 11 requires both procedural controls (i.e. notification, training, SOPs, administration) and administrative controls to be put in place by the user in addition to the technical controls that Qubes can offer. Creative IT believes that Qubes gives all the functionalities and technical tools needed for a System Owner to set up an application compliant with the 21 CFR 11 and other international GMP guidelines.

2. Part 11 Clause Comments

11.10

The business practices of the user have to be taken into account in determining whether part 11 applies. During an implementation project, there should be a step, where the System Owner qualifies the records whether these are Part 11 records or not. This analysis should be documented. System Owner should identify and define the high impact GxP electronic records and focus of effort should be on records that have a high impact, i.e. those records upon which quality decisions are based.

(a) Validation of the system is a responsibility of the System Owner since the identification of part 11 records and the configuration of Qubes is made under is responsibility and will evolve on its own will. However, Creative IT performs tests on Qubes software to ensure that all the data are accurately and reliably stored and retrieved in all the functional modules. For each new major release of Qubes software, Creative IT performs documented tests of all the main functionalities. The complete records with the results of the tests, with name of the tester, date and signature are available in Creative IT office. These records are confidential but System Owner can consult this document at Creative IT's headquarters and Creative IT can provide it to the Food and Drug Administration under non-disclosure agreement. These records do not replace any validation action or document that the System Owner should make to validate its own application.

(b) The records can be exported in html or pdf by Qubes. This generates accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.

(c) The records are stored in a database with no access in the application to modify it. Qubes doesn't modify or erase any record. Qubes ensures an upward compatibility and so even when System Owner upgrades the software, the records remain accurate and readable. It is the responsibility of the System Owner Administrators to define the retention periods and to configure or launch any purge in compliance with the records retention period.

(d) Qubes provides an advanced user rights management system in order to limit system access to authorized people. It is the responsibility of System Owner to configure it according to its organization rules and to limit the access to the database server. However, Qubes stores the record in a proprietary binary compress format, making them unchangeable by ordinary means at the database level.

(e) All records are date and time stamped, and include the user ID of the individual who is logged on to the system and who performed the action. The actions that create, modify, or delete electronic records are performed within a workflow where previous and new values are displayed and where each screen validation is date and time stamped. These audit trails are never modified by Qubes, it is the responsibility of the System Owner Administrators to define the retention periods and to configure or launch any purge in compliance with the records retention period.

(f) The workflow that the System Owner can configure with Qubes will ensure the proper sequencing of steps and events required by the application.

(g) Qubes provides an advanced security and authorization profiles module. It allows to precisely define the access rights needed in the application and the profiles that can

access data, register records or perform signature in Qubes standard screens and in the customized workflow screens. Authority checks are then performed by Qubes at each connection and action.

(h) Qubes can perform device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. Due to its web technology, it requires a proper network configuration with static IP address for the devices to be checked.

(i) Creative IT ensures that the persons who develop and maintain Qubes, have the education, training, and experience to perform their assigned tasks. Creative IT provides the proper training on technologies and also on the 21 CFR 11 requirements.

(j) This clause covers a procedural requirement for organizations and is not related to the functions of Qubes.

(k) The Qubes software package includes a module for document management, which provides controls over the distribution of, access to the documentation that the System Owner can use for the the system operation and maintenance documents. It also provides versioning and life cycle management of the documents. It maintains an audit trail that documents time-sequenced development and modification of documentation. The System Owner can use it for systems documentation.

11.30

Qubes is a closed system, so §11.30, which specifies controls for open systems, does not apply. Access to Qubes is controlled by System Owner (i.e. people who are responsible for the content of electronic records that are in the system).

11.50(a)

For each signature of an electronic record, Qubes display the following information:

- The user name of the signer
- The date and time when the approval was executed
- The meaning (such as review, approval, responsibility, or reason for approval) associated with the approval

Qubes automatically records the meaning associated with the signature with details of the activity the signature performed. In addition, users can enter a comment to expand or clarify the meaning of the approval.

11.70

In Qubes, signed electronic records are maintained in the same manner as all electronic records, and System Owner can display or print them in a human-readable format. The verification password of user is encrypted and cannot be displayed or printed in a human-readable format.

In Qubes, electronic signatures are linked to their respective electronic records directly in the database and there is no mean to excised, copy, or transfer it by ordinary means.

11.100(a)

The user identification code, called the login, is unique in Qubes and therefore the signature consisting of the login plus a password, is unique. It is the responsibility of the System Owner not to reassign an existing login to another individual.

11.100(b)

This clause covers a procedural requirement for organizations and is not related to the functions of Qubes.

11.100(c)

This clause covers a procedural requirement for organizations and is not related to the functions of Qubes.

11.200(a)(1)

Qubes requires two distinct components – a user identification code and a password – to perform each and every record. Depending of the configuration chosen by the System Owner, Qubes can oblige to use identification code and password for each signing or only the password for a connected user. The automatic disconnection of the user after a configurable idle time ensures that the user have to use identification code and password at the beginning of a continuous period of system access before signing.

11.200(a)(2)

Qubes requires the user identification code and the corresponding password to authenticate the identity of each user. The Qubes password is only managed by the genuine owner of an account and cannot be seen or copied in the software. The System Owner must have procedural controls to check that login and password are issued to the genuine owner.

11.200(a)(3)

In Qubes, the only function that would allow to use of the electronic signature by someone else than it genuine owner, is the reset of a password. This function is necessary since users often forget their password but it is protected in Qubes since two administrators have to sign in order to reset a password.

11.200(b)

Qubes does not provide biometric signature.

11.300(a)

Each individual has a unique identification code in Qubes therefore two individuals can’t have the same combination of identification code and password .

11.300(b)

System Owner can configure Qubes to force users to change passwords at a configurable interval. System Owner can invalidate Qubes user account.

11.300(c)

This clause covers a procedural requirement for organizations and is not related to the functions of Qubes. System Owner can invalidate Qubes user account.

11.300(d)

Qubes provides the following features to satisfy 11.300(d):

- When the number of failed attempts (for either logon or signature) is exceeded, Qubes prevents the user from further access without intervention from the security administration. System Owner can configure the number of failed attempts allowed.
- Failed attempts are recorded

11.300(e)

This clause covers a procedural requirement for organizations and is not related to the functions of Qubes.