Use Case

21 CFR Part 11 electronic signatures

v 0.4, 8 March 2020, Lemoene Smit

1. Background

Though Bika passed ISO 17025 as recently as 2018, it is now being upgraded for the 2017 version, firstly with more information on COAs. See the first discussed at COA for 2017 ISO 17025. Single Sample.

In some regions, it is already expected that users re-authorise themselves to do important functions, submitting, verifying and publishing results, and configuring critical objects, as stipulated by Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration (FDA) regulations on electronic records and electronic signatures (ERES).

1.1. Not in the Scope. Signing page views

NB Bika Health and Patient privacy requirements are not scoped here. It is understood that for CLIA requirements, page views have to be logged. These are available in the server logs from where they can be mined by authorised staff when required.

1.2. Not in the Scope. Login failures

Ditto for retrieving failed login attempts, available from the server logs. This is the simplest use case:

2. Use Case. Signing Results *Verification*

Role players

Users - *labmanagers, verifiers, analysts, publishers* as required by the LIMS for each function, signed in at the beginning of their sessions. The LIMS.

Use Case

1. The user navigates to the Analyses to be *verified*, on their parent Samples or Worksheets
2. He/she selects *To be Verified* Analyses, an presses [Verify]
3. **Note.** The signing via this procedure does not affect any user rights per se, those stay the same, and the extra signing procedure only add for those critical actions where it is required
4. The system pops up an authorisation form, much like the the Plone login portlet, for the user to be reauthorized

One signature for all the data that has changed on the screen before moving to the next screen is required

In Bika/Senaite, moving between multiple tabs on the same screen before submitting the changes, only requires 1 signature as long as all of the records within all of the tabs get associated with the single signature.

5. It displays the user's Full name
6. The reason for signing is displayed clearly and shows the guarded action to be taken in user friendly texts sourced from the new setup tabs described below
7. The system supplies the reason from the action taken, e.g. *Results Verification* if the signing is requested after the *[Verify]* button was pressed
8. The user may also capture additional comment in a free text field - useful in cases when results are retracted for re-testing, and with reasons for editing the configuration, e.g. as in the mockup below
9. The reason for the signature request, is used in the popup's header
10. Other information required

    Full name - not username. Firstname, middle name, surname

User roles - plural. It is possible for say a senior clerk to have both *labclerk* and *publisher* roles

System **Date and Time**

Results Verification	
Name	Vera Verifier
Role	Lab manager
Date	yyyy/mm/dd hh:mm
Comment	
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer nec odio. Praesent libero. Sed cursus ante dapibus diam. Sed nisi	
Password	********

Sign Cancel

11. Ditto for editing the Configuration

Edits to Maldi Biotyper Instrument	
Name	Vera Verifier
Role	Lab manager
Date	yyyy/mm/dd hh:mm
Comment	
Nulla quis sem at nibh elementum imperdiet. Duis sagittis ipsum. Praesent mauris. Fusce nec tellus sed augue semper porta. Mauris massa.i	
Password	**********

Sign Cancel

12. The user captures his/her password (eventually biometrically), and presses *[Sign]*
13. He/she lands on the next page, as in the current workflow sans the interruption
14. ... or *[Cancels]*, and goes back to the previous page

15. The system displays a confirmation, *Results Verification successfully signed,* alternatively *Signing cancelled*
16. Should the password entry fail, the form is refreshed for another attempt, displaying *Incorrect password, please try again*
17. When successfully authorised, the LIMS writes the autorisation and its comment to the objects' audit logs
18. The standard LIMS workflow proceeds hereafter

Similar workflows play out when the results are not verified but retracted for retesting.

The same for other functions considered critical for traceability purposes, as well as edits to the important configuration items listed below.

3. Configuration

The system stays flexible with regards to which functions are safeguarded like this, interpretations differ between regions.

3.1 Signatures On/Off

On a 'Signatures' tab in the LIMS setup, authorised users may activate / deactivate the '21 CFR Part 11' electronic signatures.

Not all labs will require it.

3.2 Critical functions

Further down on the signature tab in the LIMS setup, *labmanagers* maintain a table of actions for this purpose, e.g.

These are coded in the system core, and the user may select them individually for inclusion:

1. Creating new Batches
2. Cancelling new Batches
3. Closing Batches
4. Registering new Samples
5. Bulk Sample import (when valid imports are committed to the DB)
6. Cancelling Samples

7. Edit previously created Samples, add or remove analyses
8. Creating Reference Samples
9. Creating Worksheets
10. Assigning Analyses to Worksheets
11. Exporting Worksheets to Instruments
12. Saving results on Samples or Worksheets
13. Submitting results for Verification on Samples or Worksheets
14. Manually importing results from Instruments
15. Auto Import of results
16. Retracting Analysis Results, on Samples or Worksheets
17. Verifying Analysis Results, on Samples or Worksheets
18. Publishing, pre publishing and republishing COAs
19. Results Invalidation

3.2 Critical Configuration items

Configuration Items to be subjected to the 21 CFR regime are maintained in the same way, e.g. every time an item is created or modification made to any of these objects, the user has to identify him/herself before proceeding, and the modifications logged

For the signature procedure to display the reason for signing, the pop-up for the setup modifications, is only displayed when the user pushes [Save]

At that point the system will be able to determine what type object is being modified and display a corresponding *Reason,* e.g. *Analysis Service modified.*

These configuration objects have to be guarded in this way:

1. Users
2. Groups
3. Analysis Services
4. Methods
5. Instruments

6. Calculations
7. Specifications
8. Reference Definitions
9. Clients
10. Suppliers
11. Sample Points