APPLICATION NOTE

PB610 PANEL BUILDER 600 V2.8 SUPPORT OF 21 CFR PART 11 COMPLIANT APPLICATIONS

BENEFITS, FEATURES AND DEMONSTRATION

Contents

1 Introduction

1.1 Scope of the document

One of the biggest benefits of new version 2.8 is the support of creating projects which comply with 21 CFR part 11 standard of the American Food and Drug Administration.

The new chapter 22 in the PB610 manual, „21 CFR Part 11 Compliance“ informs about the design of relevant applications. CP600-Pro panels from CP6607 to CP6621 are already prepared for supporting these new features. For CP6605 and all other CP600-eCo and CP600 control panels new BSPs have to be introduced into production.

21 CFR part 11 are regulations of United States Food & Drug Administration (FDA) on electronic records and electronic signatures. These regulations are mandatory for example for applications in pharmaceutical industry, medical device manufacturing, biotechnology development and production or biopharmaceutical production. Of course, also users in many other installations can benefit from these features for achieving increased operation security for their applications.

1.2 Compatibility

The application Note explained in this document have been used with the below engineering system versions. They should also work with other versions, nevertheless some small adaptations may be necessary, for future versions.

- Panel Builder 600 V2.8
- Supported by CP600-eCo, CP600, CP600-Pro
- CP600-eCo - C1
- CP620…CP635 - K1
- CP635-Fx, CP651…CP676 - D1
- CP6605 - B1
- CP6607…CP6621 - A0

2 Benefits & Features

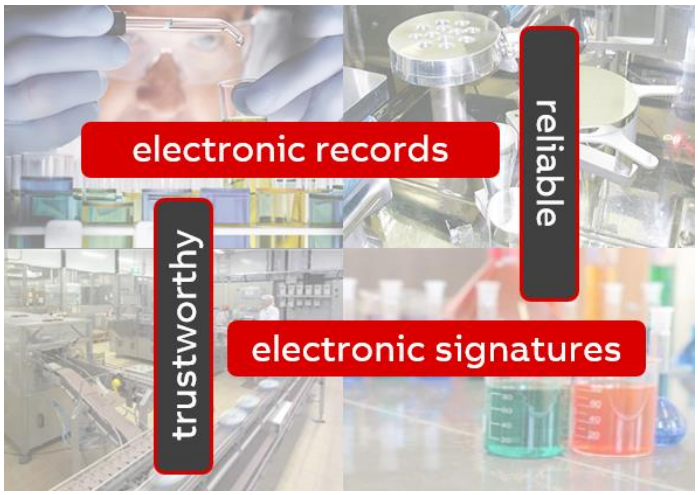
2.1 Applications

- Electronic records
- Electronic signatures Applications
- Pharmaceutical industry,
- Medical device manufacturing
- Biotechnology development & production
- Biopharmaceutical production
- Installations requiring security features (independent of FDA)

2.2 Requirements for electronic records and signatures

Control panels and relevant HMI applications complying with the American standard 21 CFR part 11 must ensure, that electronic records and signatures are trustworthy and reliable. They have to be equivalent substitutes for paper records and handwritten signatures.

PB610 V2.8 is the tool for the design of applications complying with 21 CFR part 11. This capability does not relieve customers from applying for the approval from relevant authorities.

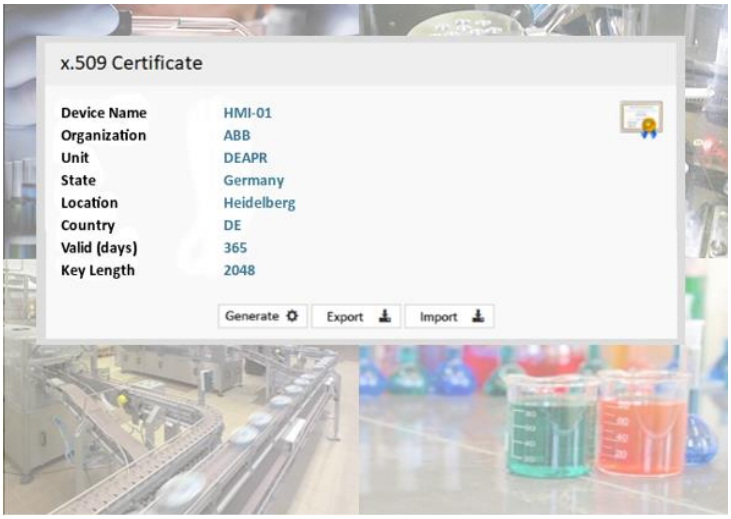


2.3 Realization

We got to know, that digital signatures shall be equivalent substitutes for handwritten ones. Panel Builder therefor works with strong asymmetric cryptography, uses X.509 standard for certificates and OpenSSL library.

As mentioned, for most of the panels from CP600 platform a new BSP, which supports this „21 CFR part 11 feature“ has to be introduced into production.

In case, that customers want to make use of this but products with required BSP are not available in stock yet, relevant BSPs can be made available via PLC support.



2.4 Part 11

Most important for the design of a 21 CFR part 11 compliant HMI application are subparts B „electronic records“ and subpart C „electronic signatures. Therefor the following slides will focus on these requirements and how they can be fulfilled by means of PB610 V2.8.

Subpart A – General provisions

- 11.1 Scope
- 11.2 Implementation
- 11.3 Definitions

Subpart B – Electronic records

- 11.10 Controls for closed systems
- 11.30 Controls for open systems
- 11.50 Signature manifestations
- 11.70 Signature/record linking

Subpart C – Electronic signatures

- 11.100 General requirements
- 11.200 Electronic signature components and controls
- 11.300 Controls for identification codes/passwords

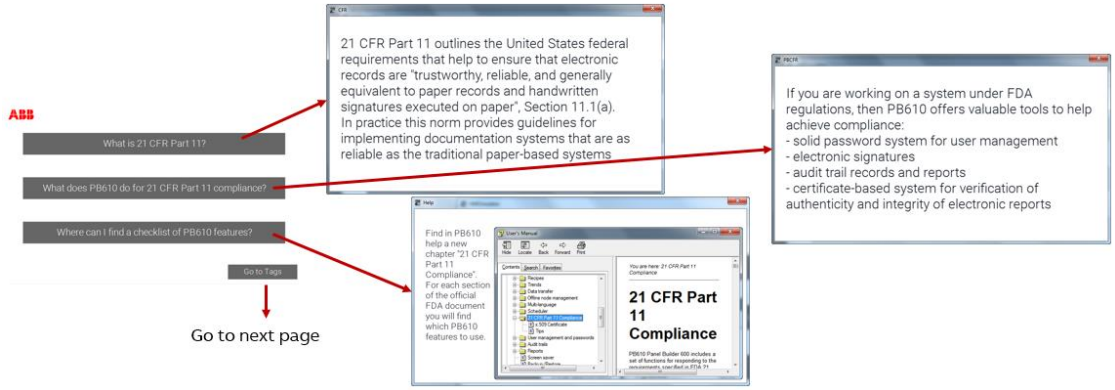
21 CFR part 11 Requirements	PB610 V2.8 Features for Realization
11.10 (a) Ensurance of accuracy, reliability, con-sistent intended performance, ability to discern invalid or altered records.	Signature of reports by means of x.509 certificates Export of reports in combination with - certificate (including the public key) - electronic signature of reports
11.10 (b) Generation of accurate and complete copies of records in both human readable and elec-tronic form suitable for inspection, review, and copying by the agency.	- individual selection of data - records of each change of the selected data - including the operator´s name doing the change - audit trail reports are readable on the HMI and - exportable to csv-files
11.10 (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Definition of self-generated signed reports - to external memory or network folders - at predefined intervals (e.g. daily).
11.10 (d) Limiting system access to authorized individuals.	Individual user management with clear definition of autorizations: Up to 50 users/ user groups
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.	Audit trail records - cannot be modified by operators, - are stored in circulare memory - have sequ. numbers for check of completeness - can be saved/exported on regular basis
11.10 (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Configuration of sequences in PB610 application: - macros and/or - JavaScript
11.10 (g) Use of authority checks to ensure that only authorized individuals can use the system, elec-tronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	User dependant access, rights, permissions: - access user name/password protected - user depentant availability of objects - user depentant availability of resources
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.	- Accessibility of resources for defined user groups only - limitation of access by means of IP addresses

11.10 (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.	PB610 user management: - define and - assign the appropriate user rights
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.	Written policies from management can be - displayed on the HMI. - provided on user dependant home page with appropriate information - displayed prior to execution of actions
11.10 (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of docu-mentation 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.	Appropriate systems documentation can be - displayed on the HMI. - provided on user dependant home page with appropriate information - displayed prior to execution of actions
11.30 Controls for open systems. Persons who use open systems …	PB610 Panel Builder 600 has been designed for operation in closed systems.
11.50 Signature manifestations. (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.	All records will be added to the audit trail with 1. name of the user as logged in 2. date and time when the signature was executed 3. additional comments as entered by the user during signature.
11.50 (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 will be added to the audit trail with 1. name of the user as logged in 2. date and time when the signature was executed 3. additional comments as entered by the user during signature. These data are integrated part of the audit trail records and therefor are subject to the same controls.
11.70 Signature/record linking.	Electronic signatures are exported with the same process step. Application developer is

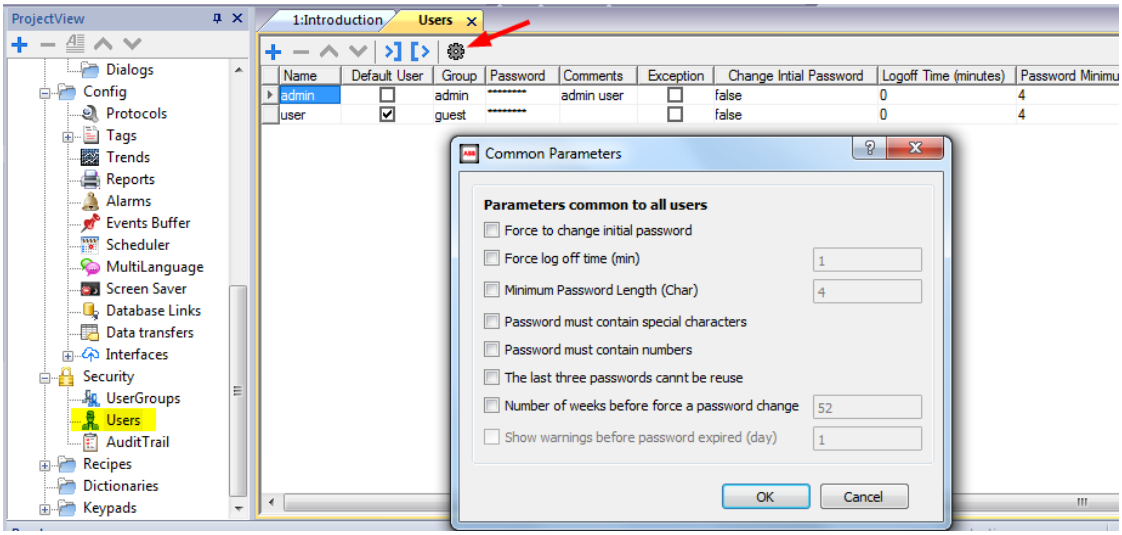
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or other-wise transferred to falsify an electronic record by ordinary means.	responsible not to implement procedures for import/export of user passwords.
11.100 General requirements (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	PB610 ensures that two users with the same id cannot be defined. It is administrator´s responsibility to avoid removal and reassignment of the same user id to a different user.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, …	Responsibility of the organizantion
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agencythat the electronic signatures …	Responsibility of the organizantion
11.200 Electronic sign. components 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.	PB610 Panel Builder 600 security functions are based on the combination username/ password
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, … (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, …	- System access: username and password must be entered - For critical actions: Entering password again can be configured - After configurable time out: username and password must be entered
(2) Be used only by their genuine owners; and (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.	Each user is responsible not to divulge own password. Passwords defined by administrator for first access can be forced to be redefined at first use.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	PB610 Panel Builder 600 does not support biometrics.
11.300 Controls f. identification codes/passwords.	

… Such controls shall include:	
(a) Maintaining the uniqueness of each combined identification code and password, …	PB610 ensures that two users with the same id cannot be defined.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or re-vised (e.g., to cover such events as passw. aging).	System can be configured to force each users to define a new and different password after a configurable number of days.
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, …	Users can change their password at any time. Administration can redefine each user's password and force them to redefine at the first login.
(d) Use of transaction safeguards to prevent un-authorized use of passwords and/or identification codes, and to detect and report …	Failed logging attempts are logged to 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.	Responsibility of the organizantion/administration

3 Demonstration



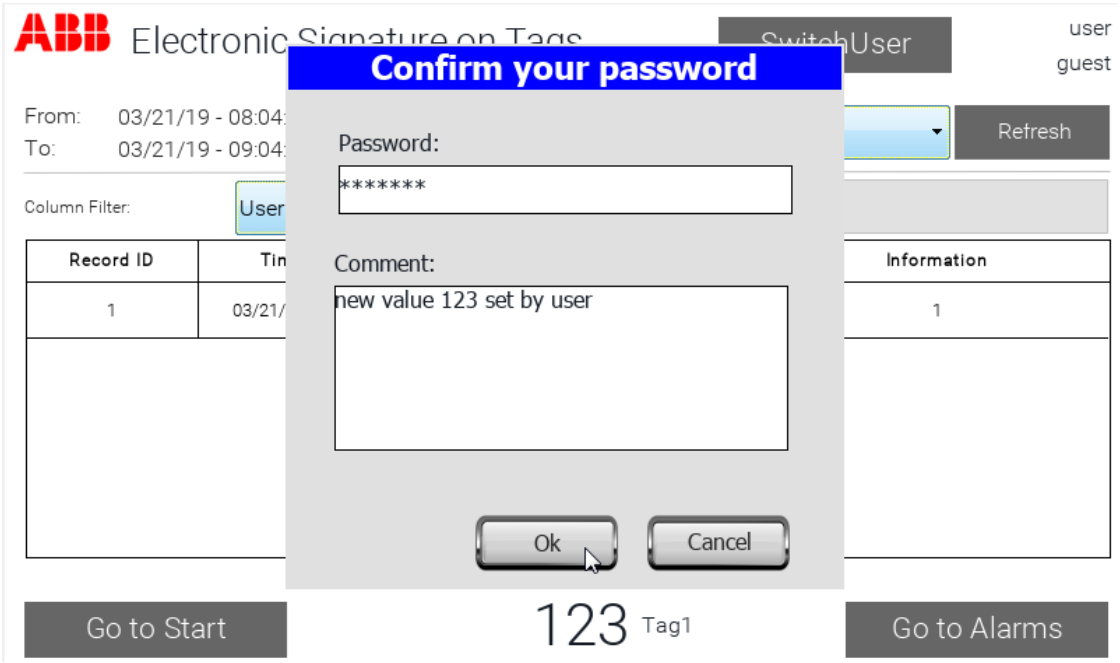
3.1 User Management



In comparison with former PB610 versions “audit trail” in PB610 V2.8 has been moved under security headline. For each set of items like tags, alarms, recipes and miscellaneous audit trail can be enabled by checking relevant check box and then for each tag for example check boxes “audit” and “signature” can be checked individually. If electronic signature is enabled for a tag, operator is asked for entering his password, if he wants to change the value of this tag.

By means of “settings” in the upper right corner of the menu the period (seconds) of the signature´s validity can be defined. Within the defined period operator can do additional modifications for other items and will not be asked again for his password, even if in general those items are checked with signature.

3.2 Setting new tag Value

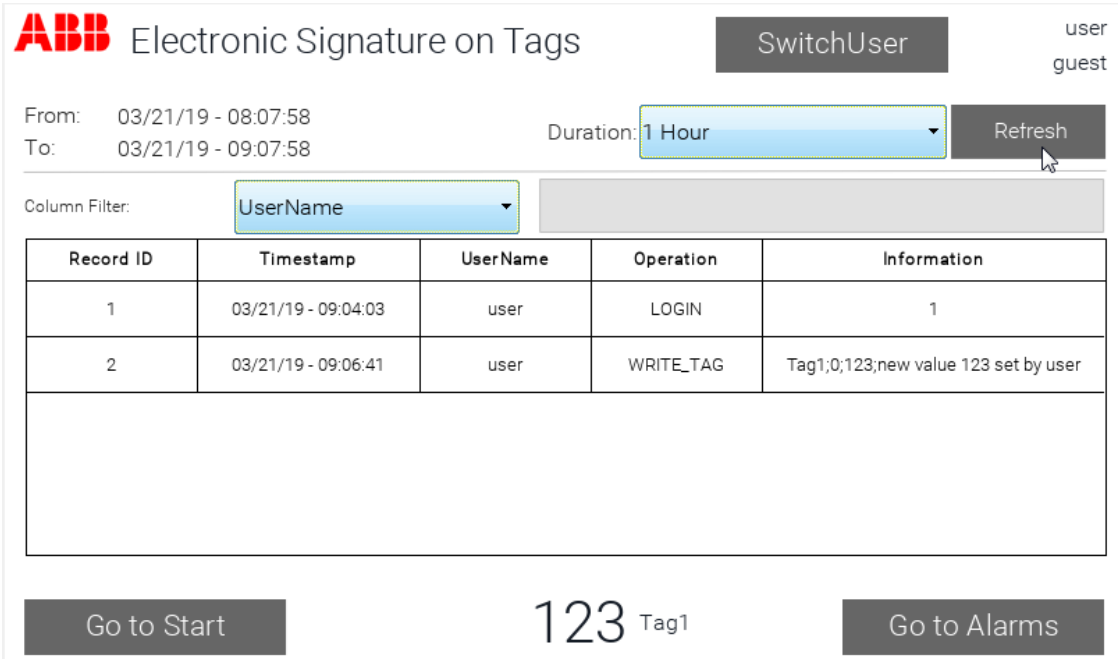


This is the audit trail widget in the demonstration project.

In the upper right part you see the logged user´s name ‘user’ and his user group ‘guest’

In the lower part in the middle Tag1 is available for operator´s settings. After entering the new value – in this example 123 – operator is asked for his password and can add a comment for his new setting.

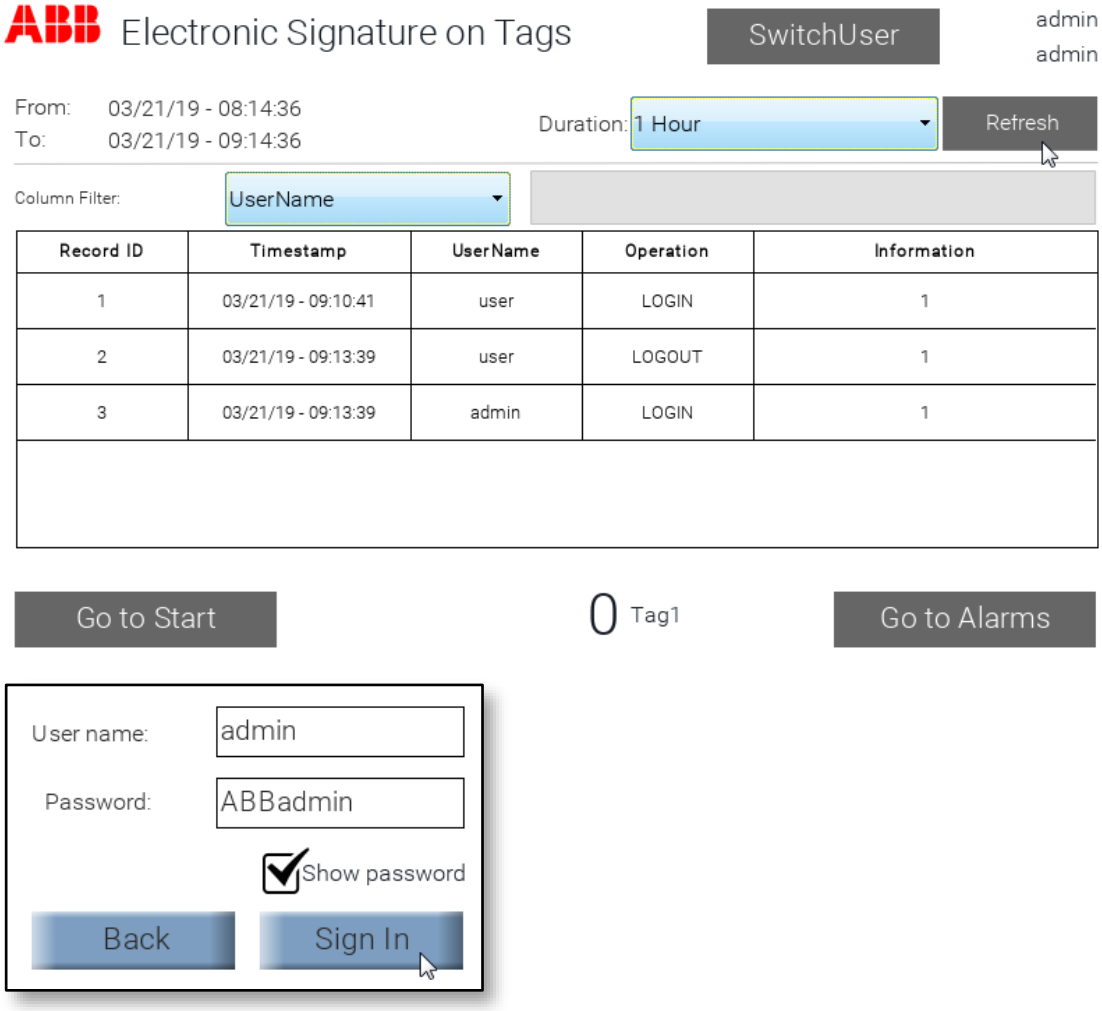
3.3 Refreshing Audit Trail Widget



After pressing “ok” Tag1 has the new value 123. After pressing “refresh” a new line in the audit trail table displays the operator´s setting (Tag1 changed from previous value 0 to new value

123) including his comment. The cell ‘Information’ includes tag name, previous value, new value, operator´s comment

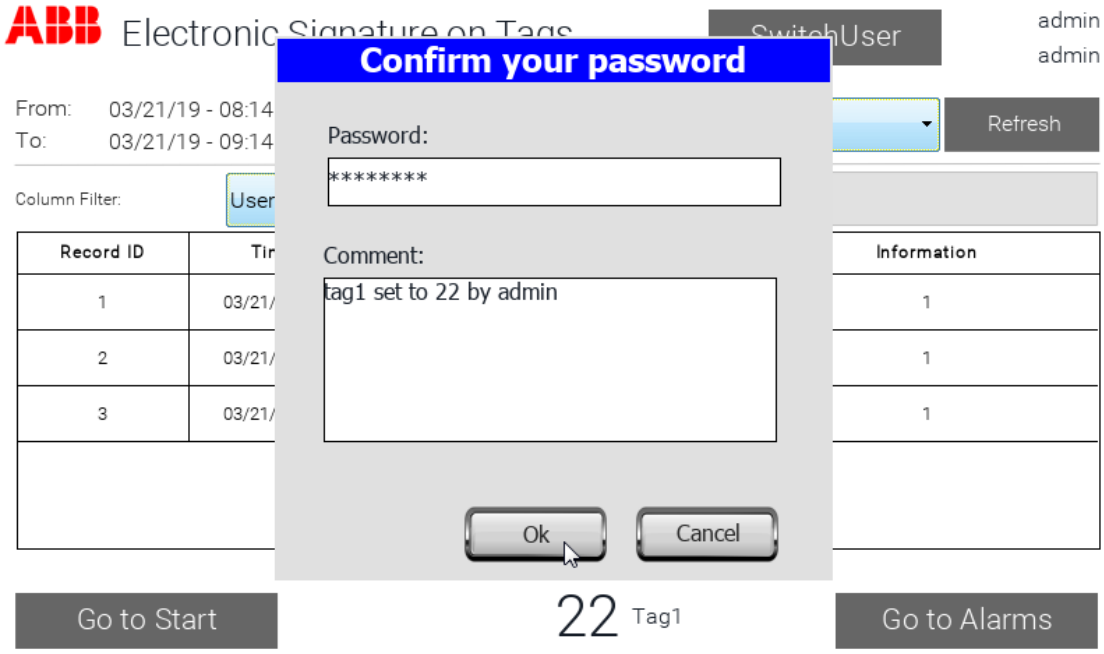
3.4 User Management: Switch User



In the upper right part of current page you can see current user “user” and his user group “guest”. By pressing the button “switch user” you can switch to a new operator, means, that the current one will automatically be logged out, as soon as the new operator has logged in with his name and password.

After having successfully logged in new Operator “admin” belonging to user group “admin” is displayed.

3.5 Set new Tag Value

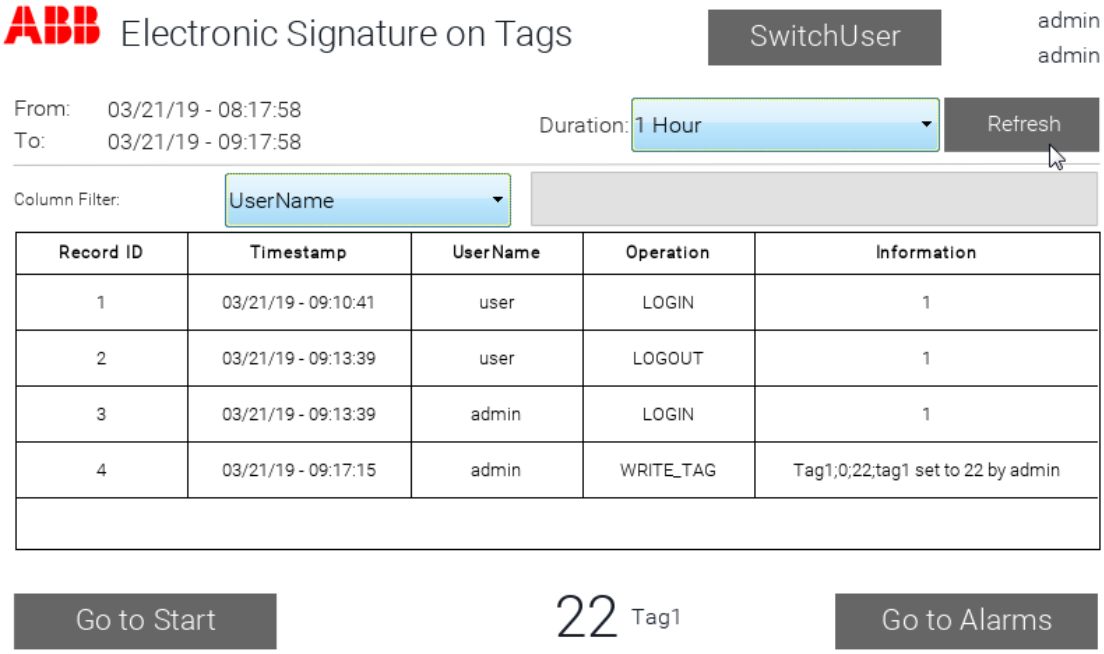


In the upper right part you see the logged user´s name ‘admin’ and his user group ‘admin’

Also the next setting of a new value for ‘Tag1’ has to be confirmed with the password of the user, who is currently logged in.

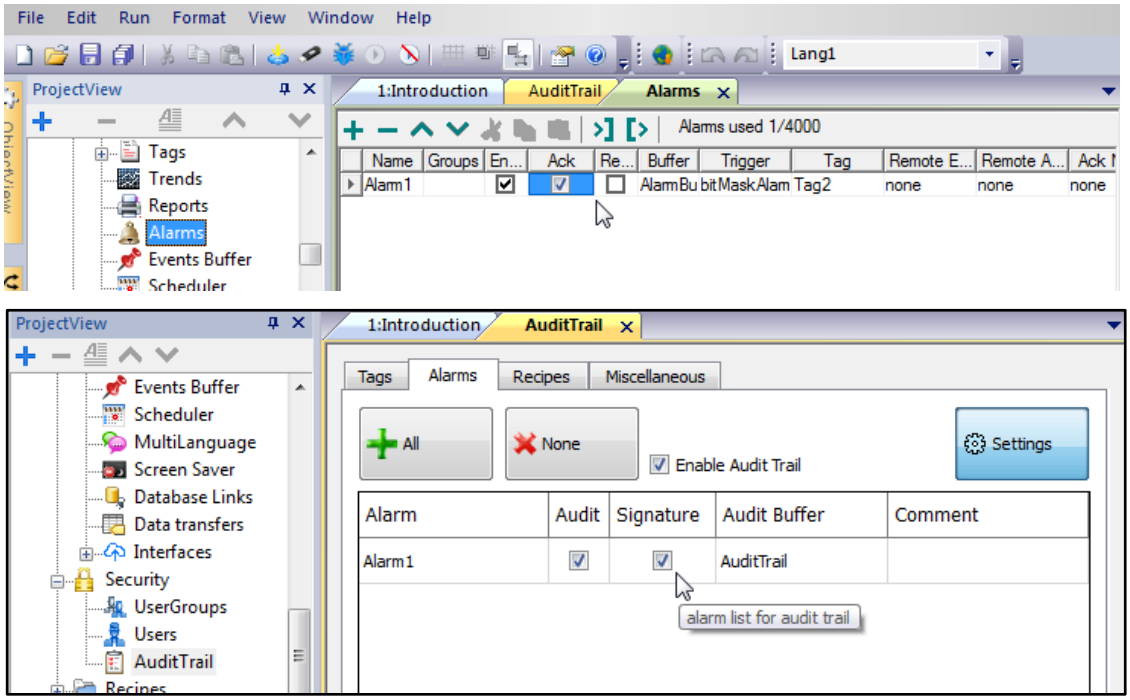
After entering the new value – in this example 22 – operator is asked for his password and can add a comment for his new setting.

3.6 Refreshing Audit Trail Widget



After pressing “ok” Tag1 has the new value 22. After pressing “refresh” a new line in the audit trail table displays the operator´s setting (Tag1 changed from previous value 0 to new value 22) including his comment.

3.7 Audit Trail of Alarms and Acknowledgement



In ‘Alarms’ each alarm can be checked for acknowledgement.

For recording the alarm and its acknowledgement in audit trail “audit” must be checked and for recording the user, who acknowledged, signature must be checked as well.

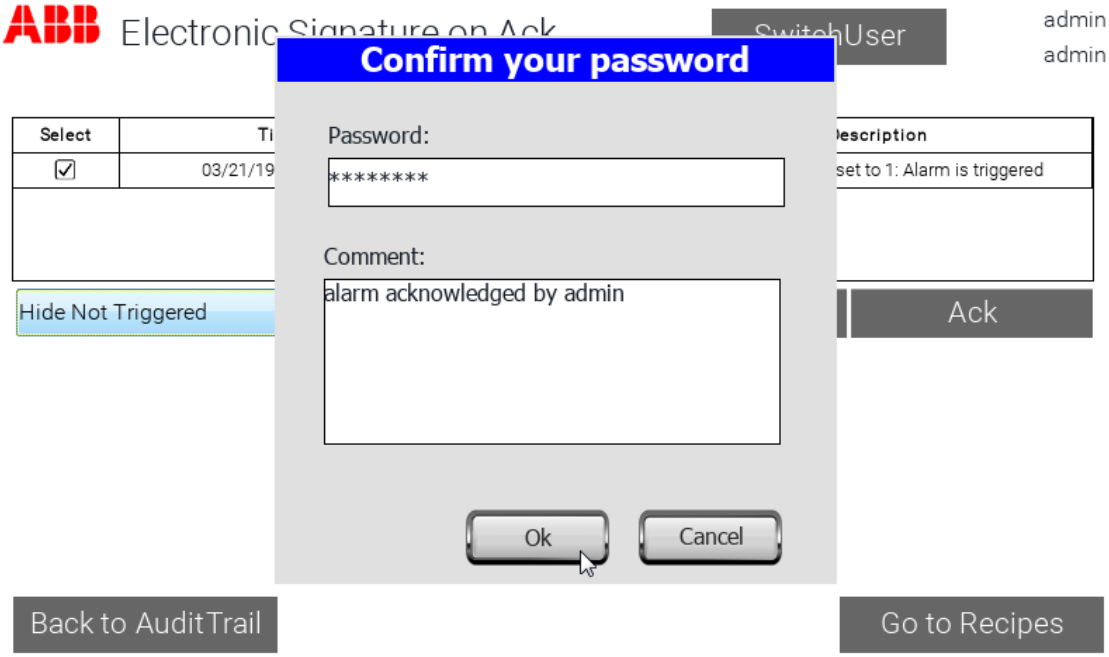
3.8 Alarm widget

Demonstration: After having pressed ‘Go to Alarms’ next page with alarm widget is displayed.

By means of ‘set alarm’ – moving the slider from ‘false’ to ‘true’ – an alarm can be simulated.

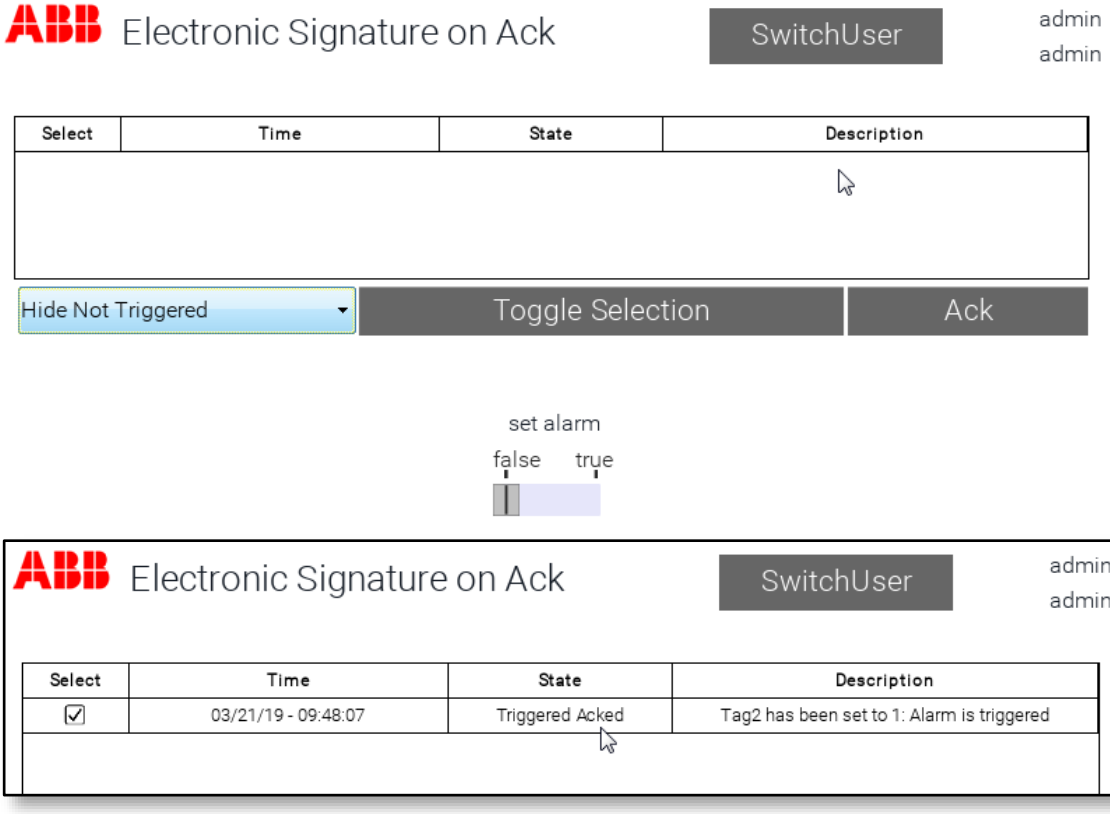
The alarm is visible as one line in the alarm widget and can be selected by the operater for acknowledgement.

3.9 Alarm Acknowledgement



Demonstration: After having selected an alarm for acknowledgement and having pressed the ‘Ack’ button the ‘Confirm your password’ dialog pops up. Beside entering the correct password (user who is currently logged in) operator also can add a comment, but not mandatory.

After acknowledgement alarm ‚State' is displayed as ‚Triggered Acked'. Disappearing of the alarm – ‚set alarm' moved to ‚false': Alarm disappeared

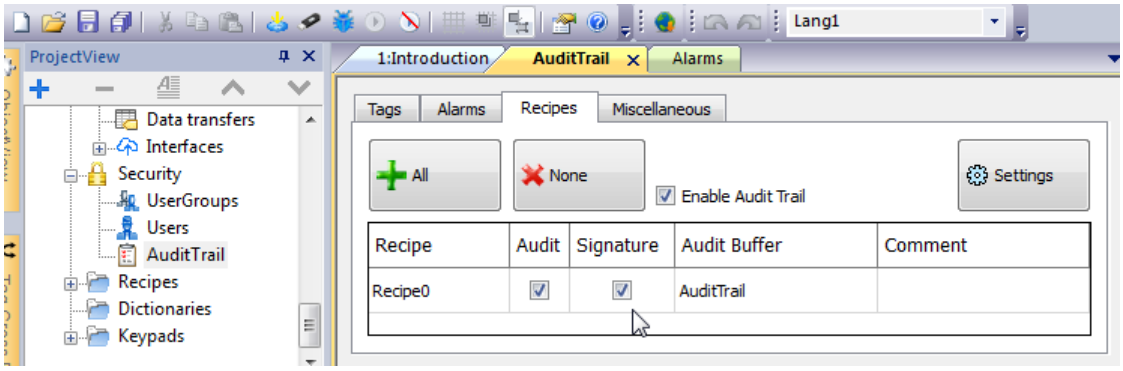


After acknowledgement alarm ‚State' is displayed as ‚Triggered Acked'.

Disappearing of the alarm – slider ‚set alarm' is moved to ‚false': Alarm is no longer visible in the alarm widget.

3.10 Audit Trail of Recipes

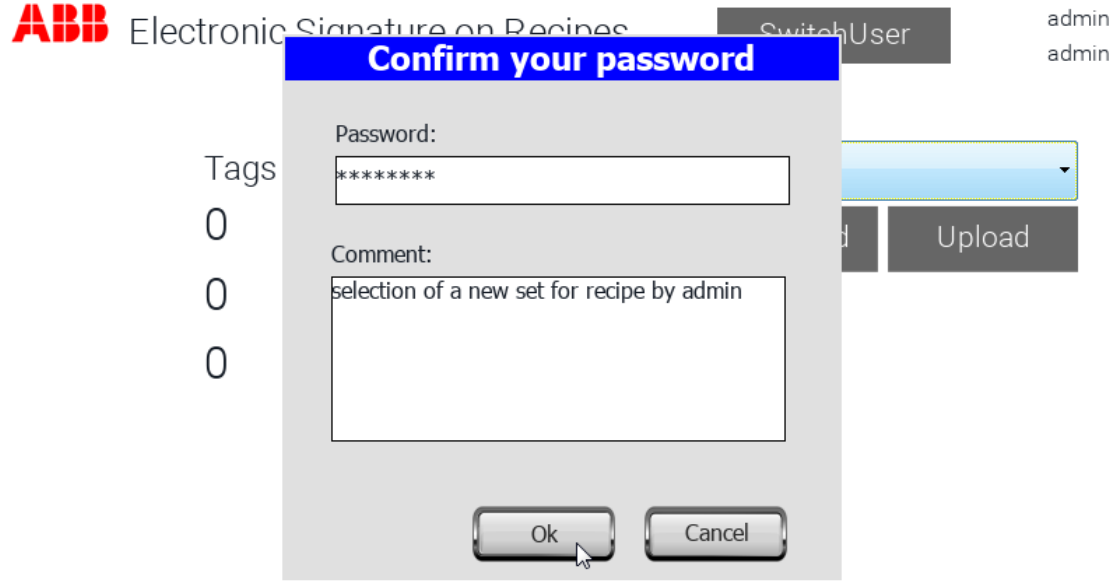
Audit trail of recipes is realized in the same way as for alarms.



3.11 Confirmation of Recipes Modification

The operator can select a new set of tag values for the recipe:
As soon as the operator presses the download button he must confirm his password and can enter a comment, since “signature” was checked for this recipe:

As soon as the operator presses the download button he must confirm his password and can enter a comment as well.



After password confirmation the new values of set 1 are visible in the demonstration project.
The same procedure is vald for uploads.

3.12 Certification Schema - Workflow

Workflow (see PB610 V2.8 manual / chapter 22 ‚21 CFR part 11 Compliance' / headline ‚x.509 Certificate')

1. Each HMI device contains two keys:

- Key1 is the secret key, that is used to sign the reports generated by the HMI device. This key is securely

stored inside the HMI device.

Key2 is the public key that anyone can use to verify the authenticity of the reports signed by the HMI device.

2. The macro SaveEventArchive can be used to generate signed reports (see "SaveEventArchive" on page 168 for

additional details)

3. Users can use the public key and the signed file to verify a report is authentic and has not been modified after it has

been generated.

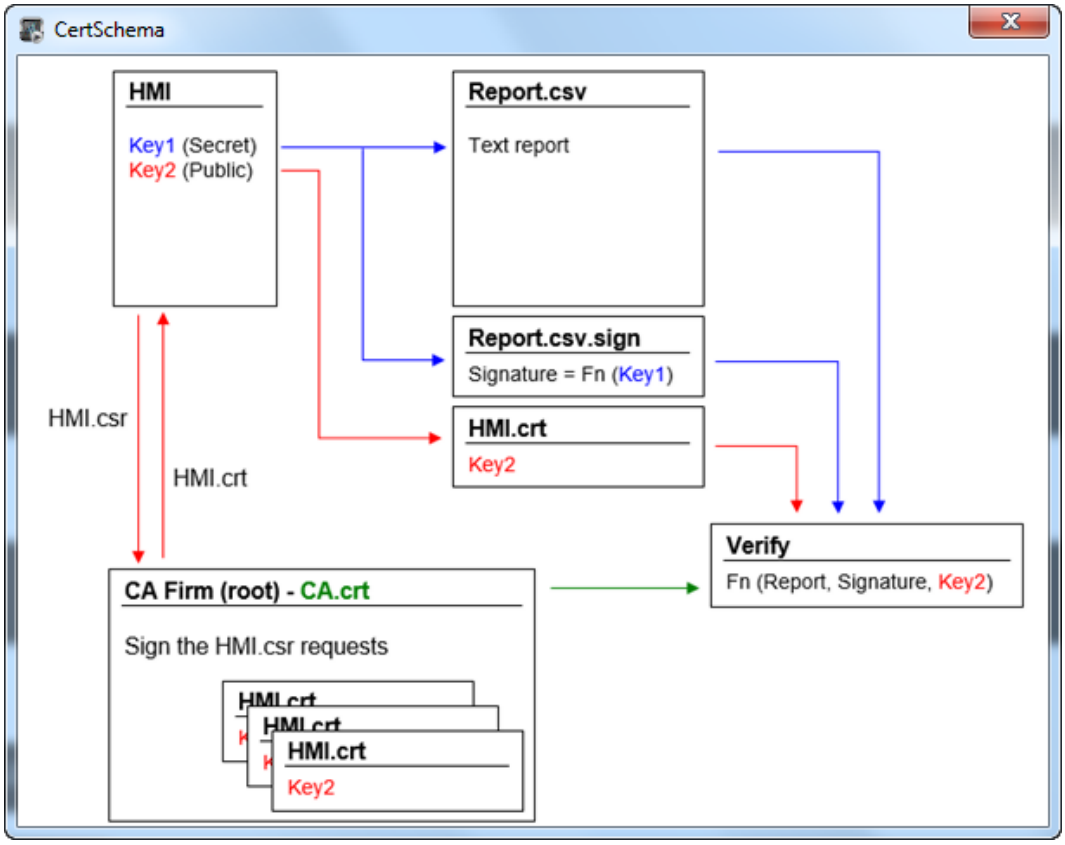
Authenticity of the public key

Before verifying a report (Report.csv) with its signed file (Report.csv.sign), users must be sure of the authenticity of the

public key (HMI.crt).

The public key can be signed by a Certificate Authority (CA) that guarantees its authenticity. As an alternative, the public

key can be taken directly from the HMI device.



3.13 SaveEventArchive

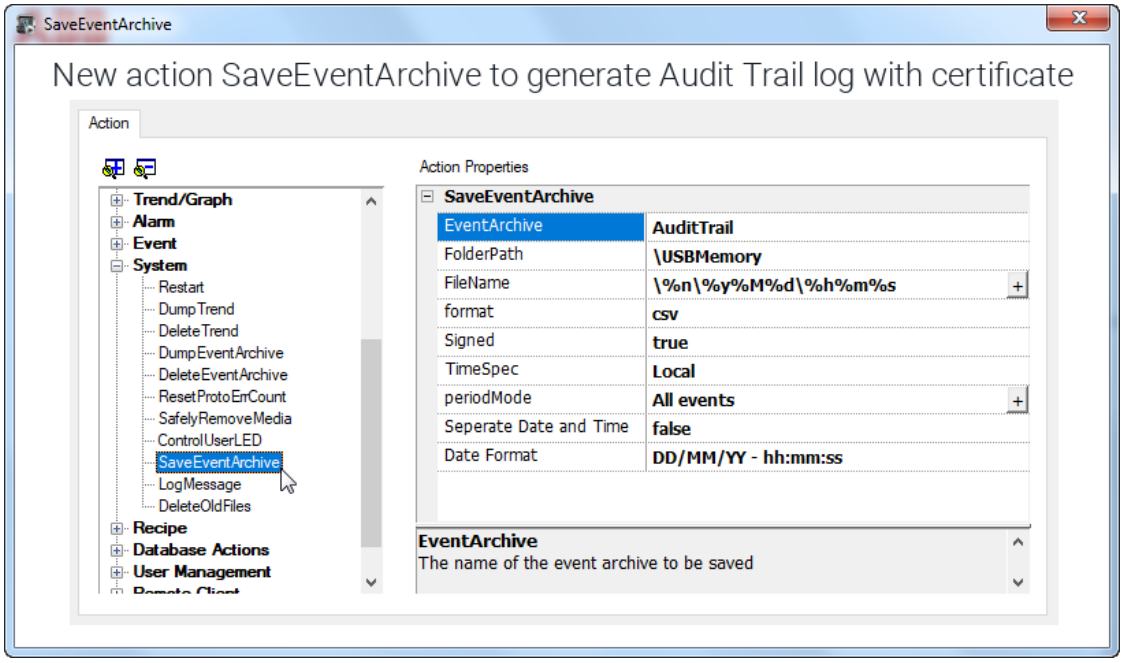
The HMI can use a self signed certificate that can be exported from its system settings. The certificate also can be imported from a certification authority (CA Firm (root) – CA.crt). This file from the certification authority can be imported into the HMI. Electronic signature then can be performed by means of this imported signature.

How to export this report including electronic signatures and relevant certificate for verifying the authenticity of the report: To verify, that the report has not be manually modified there is a new action in PB610 that is called ‘SaveEventArchive’.

There are several parameters to define/select. Most import regarding electronic signature is to set “signed” to true.

Following files will be created:

- Report.csv — report file containing all the audit trail information
- Report.csv.sign — file with the electronic signatures
- HMI.crt — electronic certificate of the HMI that has been used to sign the report



3.14 Batch files to manage certificate files using public OpenSSL-Win32 tool

Here are example of how certificate files can be managed using a public OpenSSL-Win32 library:

Reference.: https://www.openssl.org/

ABB Automation Products GmbH
Eppelheimer Straße 82
69123 Heidelberg, Germany
Phone: +49 62 21 701 1444
Fax: +49 62 21 701 1382
E-Mail: plc.support@de.abb.com
www.abb.com/plc