Wir regeln das.

a-eberle

Security Documentation
Power Quality System

according to BDEW Whitepaper May 2018

This document describes all safety-relevant settings and parameters of the individual components as well as of the overall system according to the BDEW Whitepaper version May 2018. The safety-related notes and information contained in the operating instructions and product descriptions remain valid.

Document version 1.2 from 01.09.2021

A. Eberle GmbH & Co. KG
Frankenstraße 160
D-90461 Nürnberg
Phone: 0911 - 62 81 08 0
Telefax: 0911 - 62 81 08 99

E-Mail: info@a-eberle.de
Internet: www.a-eberle.de

The company A. Eberle GmbH & Co. KG assumes no liability for damages or losses of any kind resulting from printing errors or changes in this document.

The company A. Eberle GmbH & Co. KG assumes no liability for damages and losses of any kind resulting from faulty devices or from devices that have been modified by the user.

Contents

Overview of the security documentation

Components of the safety documentation

To meet the whitepaper's documentation requirements, the document is split into two parts. The first part A describes all basic safety-relevant settings and parameters of the individual components as well as the overall system. Part A also includes a description of the system architecture and security-specific implementation details. The second part B comprises the project-specific documentation and shall be added to this document at the latest for acceptance. Checking the entire documentation for completeness and correctness is part of the acceptance test. At the end of the document you will find the references as well as further, e.g. project-specific, appendices. At the beginning of each chapter, the corresponding sections of the BDEW White Paper are mentioned, i.e. which requirements are addressed.

Security documentation:

- **Administrator Documentation**: Security documentation of the entire system
- **Project Documentation**: Project specific documentation

The complete documentation consisting of installation, setup and further information which system users need for the start-up and operation of the system is described in the corresponding user manuals, see references V.1.

Manuals:

- **Hardware**: Operating instructions PQI-DA smart and PQI-DE
- **Software**: WinPQ operating manual and WinPQ commissioning manual

The release notes of the current software and firmware versions of the respective hardware and software components (see application area) contain all information on security-relevant changes, new functions and bug fixes in the version.

Release notes:

- **Hardware**: release notes PQI-DA smart and PQI-DE
- **Software**: release notes WinPQ and WinPQ lite

The latest versions of these documents as well as other data sheets etc. are available on the company website in the download center under the following link
https://www.a-eberle.de/en/downloads/power-quality

Field of application

This security documentation is exclusively intended for the system described in the following and its components from the company A. Eberle GmbH & Co. KG.

Hard- or software component	Firm- or software version
PQI-DA smart	2.0 or above
PQI-DE	2.0 or above
WinPQ lite	5.0 or above
WinPQ	5.0 or above

Information System IT security

A secure communication platform was set up on the company website to enable the secure exchange of information and data. The corresponding access is set up in the course of a maintenance contract. Further information for the setup and registration of an access will be provided at the beginning of the maintenance contract.

IT security requirements

The present documentation as well as the development and implementation of the requirements for the security of the system and the improvement and further development are based on the following documents:

- Whitepaper “Anforderungen an sichere Steuerungs- und Telekommunikationssysteme” Version 2.0 von Mai 2018
- Technische Richtlinien Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen Version 2018-01, Stand 22.01.2019
  - TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen - Teil 2 Version 2018-01
  - TR-02102-3 Kryptographische Verfahren: Empfehlungen und Schlüssellängen - Teil 3 Version 2018-01
  - TR-02102-4 Kryptographische Verfahren: Empfehlungen und Schlüssellängen - Teil 4 Version 2018-01
- ISO/IEC 27002:2013 / 27019:2017

General notes

According to §11 Abs. 1a EnWG the obligation to operate a safe energy supply network exists. The EEG 2014 also deals with safety:

"The design of the connection and the other facilities necessary for the security of the grid must comply with the technical requirements of the grid operator and § 49 of the Energy Industry Act, which are necessary in individual cases." Source §10 EEG 2014.

Furthermore, §36 - Remote Controllability of the EEG 2014 reads as follows: "[...] taking into account the relevant standards and recommendations of the Federal Office for Information Security, transmission technologies and transmission paths are permissible which correspond to the state of the art at the time of commissioning of the plant."

These statements give a certain amount of freedom in the design of the security levels. A good way of meeting the requirements is the white paper "Requirements for safe control and telecommunications systems" published by BDEW, which, when the user prepares the implementation instructions, individually defines the respective level of safety precautions of the plants, communication components and their infrastructure.

Depending on the importance of the plant for general supply security, different requirement profiles are defined in the BDEW white paper. The following aspects may become necessary:

- Use of security certificates
- Use of end-to-end encryption such as SSH
- Use of a user administration
- Use of secure protocols
- Use of firewalls

Section A

Administrator documentation

The following part is the security documentation for administrators and describes all security relevant information of the Power Quality (PQ) system. All relevant descriptions for safe operation with regard to the requirements of the BDEW whitepaper are described below.

1 Description Power Quality System and Components

The components of the system are defined and fundamentally described below. The Power Quality System consists of the software and hardware components of the company A. Eberle GmbH & Co. KG and is briefly referred to as PQ-System. The task of such a PQ-System is, in addition to real-time monitoring of the energy system, to store the measurement data

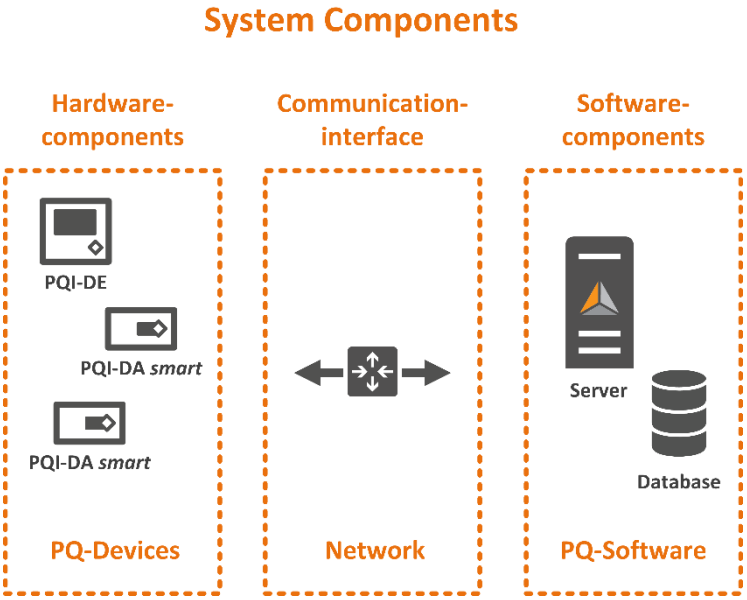


Figure 1: System components of the PQ-System

recorded by the measuring devices (generally described as hardware components) in a central database for further data processing tasks such as visualization, evaluation, report generation, etc.

1.1 Hardware components

A PQ system can consist of the device types PQI-DA smart and PQI-DE in basically any number. Detailed information about these device types, including the firmware running on the devices, is described in the corresponding operating manuals and data sheets. The PQ devices have the task of recording power quality data seamlessly at the installed measuring point and in some cases already process them. After the devices have been connected with the help of the PQ software, see section 1.2, and the recorded data can be processed further.

PQI-DA smart

The power quality measuring instrument PQI-DA smart has an Ethernet connection which is used for communication with the software components within the PQ system.

PQI-DE

The Power Quality measuring instrument PQI-DE is technically based on the PQI-DA smart PQ device. The communication with the software components is also carried out exclusively via the integrated Ethernet interface.

1.2 Software components

The programs WinPQ and WinPQ lite are used as user software. The two software packages are described in detail in the corresponding documents such as operating instructions, system requirements etc.

WinPQ

The software WinPQ for Windows operating systems has the task of storing the measurement data of the PQ devices PQI-DA smart and PQI-DE, which are connected via network, in a central database and thus making them available to the user for further tasks. In addition, the software has numerous other functions such as visualization and evaluation of measurement data as well as monitoring of the system and alerting in case of errors.

WinPQ lite

The software WinPQ lite is integrated in WinPQ, but is also available separately. With this software the user can carry out the setup and parameterization of the hardware components or PQ measuring instruments. In addition, a rudimentary evaluation of measurement data from connected PQ devices is also possible.

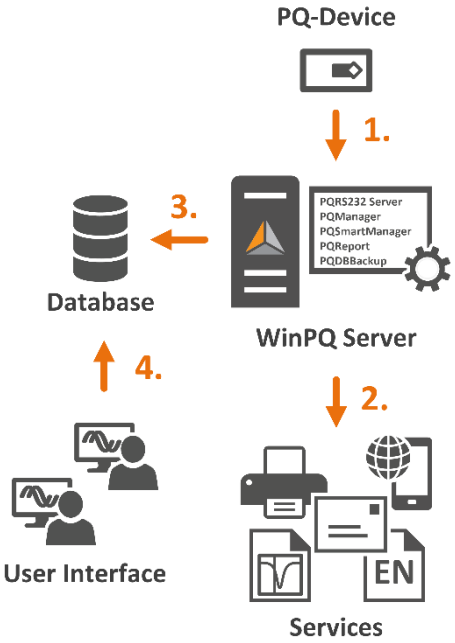
1.3 Communication interfaces

A communication link between these components is necessary for the data transfer from the PQ measuring instruments to the central database of the WinPQ software. The corresponding communication interface on the side of the measuring instruments is the Ethernet connection. On the WinPQ software side, the network interface of the computer on which the WinPQ software is installed. The network protocol used is TCP/IP. All system components must have appropriate IP settings etc. to be able to communicate with each other.

> **!** The following only describes the setup and operation of the PQ system in the safe (standard) configuration. In this configuration, the system is completely set up for safe operation. The setup or activation of additional interfaces is a deviation and is therefore not a safe configuration!

1.4 Functionality PQ-System

The functionality of the PQ system consisting of the components from the previous chapter is shown schematically in the following figure.



1. **Data transfer**
   WinPQ system processes transfer data from the configured measuring instruments to the WinPQ server
2. **Data- and alarm management**
   Processing and analysis of device data and possible triggering of (alarm) messages
3. **Database**
   Automatic storage of device data in the WinPQ database (locally or on remote database server)
4. **Data evaluation, analysis and visualization**
   by users via the user interface of the software

Figure 2: Functionality of the PQ-System

In the Power Quality System, the WinPQ software handles the entire data processing from the PQ measuring instrument to the storage of the measured data in the database. The software also offers several visualization components for operation and to enable access to the measurement data. The connection is established from the WinPQ server to the measuring instrument. The software realizes these tasks with several processes which are listed on the WinPQ server after the installation of the software. The processes for an operation with the above mentioned PQ devices and components are:

Process name	Application	Description
MySQL	mysql.exe	Instance of the database
PQSmartManager	PQSmartManager.exe	Data transmission and management of the PQ device types PQI-DA smart and PQI-DE
PQReport	PQReport.exe	System functions like maintenance (SQL checks, timeout monitoring, etc.) and administration tasks (messages between WinPQ programs) as well as calculation of statistics and reports

The processes are re-initialized every 24 hours in the task planning and are executed in the system account by default. The settings can be changed according to requirements and the corresponding adjustments are recorded in the project-specific part.

2 Security of the system components

This chapter describes the general features of safe system operation. In particular, the requirements of the BDEW White Paper Chapter 4.1 General requirements are dealt with.

2.1 Security concept of the system architecture

The security concept of the PQ system was developed and implemented holistically for all system components and their interaction with each other and with the users. From the initial commissioning and normal operation to the maintenance and care of the system, all individual components and the overall system were designed for safe operation. This system design is based on the principles of Security-By-Design, Minimal-Need-To-Know principle, Defence-In-Depth principle and the redundancy principle.

The implementation is described and explained in detail below. The security architecture, commissioning and safe operation of the system are described in Chapter 3.

2.2 Updates and bug fixes of system components

Updates or patchability of system components

All components of the PQ system are patchable, i.e. they can be updated with safety-relevant and functional updates using new software or firmware versions. The respective procedure is described in the corresponding manuals of the software and hardware components. For security reasons, a downgrade of the software and firmware version, i.e. a downgrade is not possible.

Patch-Management and -security

The user can independently update all components of the system. If desired, the update can also be carried out by the manufacturer or a service provider. The process is not performed automatically and can only be performed by users with the appropriate administrative role. The authorization for performing updates is carried out on the components as follows:

Component	Authorization Update	Protection mechanism
Software WinPQ and WinPQ lite	Software Update: Verification of digital signature by software and fingerprint by user	Login to the operating system through Windows authentication
Hardware PQI-DA smart and PQI-DE	Firmware Update: Checking the check sum (hash value)	User login on the device via local or remote (RADIUS) RBAC

The integrity of the updates is secured as follows and an update may be denied.

Component	Integrity check Update	Cryptographic mechanism
Software WinPQ and WinPQ lite	Software Update: Verification of the digital signature by operating system (Code Signing Certificate)	Public key: RSA 2048 Bit signature hash algorithm: SHA-256
Hardware PQI-DA smart and PQI-DE	Firmware Update: Checking the check sum (hash value)	Hash algorithm: SHA-256

All processes are recorded or logged by the components. The corresponding log files are protected against unauthorized access and manipulation. A readout is only possible for users with appropriate rights. The exact description of how to read out log files can be found in the respective operating instructions.

2.3 System maintenance and service

Provision of security patches for all system components

Updates or patches of the system components are provided via the company website. In the publicly accessible area only the latest software and firmware versions are made available for download. In the closed area, which is available to every registered user with a maintenance contract by appropriate login, also individual versions and possibly further data for this user. This closed login area is described in section "Information System IT Security" at the beginning of this document. An overview of the update periods and deployment sources of the system components can be found in the following table.

Component	Update period	Provision of update files
WinPQ	2 years from date of purchase then fee required extension	https://www.a-eberle.de/de/download-center-categories/für-festinstallierte-geräte
WinPQ lite	Total product life time	https://www.a-eberle.de/de/download-center-categories/für-festinstallierte-geräte
PQI-DA smart und PQI-DE	Total product life time	https://www.a-eberle.de/de/download-center-categories/für-festinstallierte-geräte-0

The updates will only be published after successfully passing the corresponding release tests, for details see chapter 4. The most important implementations or changes of the software and firmware updates like new functions, bug fixes etc. are listed in the release notes, which are also available on the company website.

Support for used system components

The components of the system are intensively tested in the course of the operation and runtime tests with regard to compatibility with various externally developed components. Especially the software components WinPQ and WinPQ lite are tested for error-free operation with new versions of operating and database systems. The list of the supported operating and database systems as well as the system requirements and demands of the software components can be found in the WinPQ Commissioning Manual V.1. This manual is continuously updated for each new software version. The software components can be purchased with different database systems and versions.

Maintenance contracts

The provision of continuous support for the system or the import of e.g. updates of the database system is realized via maintenance contracts. The scope and duration of these are agreed individually with the contractor. With these contracts it can be ensured that the used system is always up to date. The exact agreements with contact persons, discontinuation procedures and all relevant minimum terms, such as load-customer shipping and end-of-support, are bindingly defined in the project-specific part of this document. Further details are described in chapter 4.2 System Maintenance.

2.4 General security mechanisms

Encryption of confidential data and cryptographic processes

The system transmits and secures confidential data always encrypted using current encryption standards recommended by the BSI. In chapter 3 the used protocols and cryptographic procedures are described in detail.

Secure standard configuration

All components of the system are delivered in a defined basic configuration. In the course of commissioning the system components, the remaining security settings, e.g. the setup of user accounts and passwords and the coupling of the measuring devices to the software components, are carried out. After this initial installation or (re)commissioning, the individual components are set up for safe operation in accordance with the requirements of the BDEW white paper. After completion of this setup, the components are in safe operating condition. The basic configuration as well as commissioning or completion of the setup for safe system operation are described in detail in chapter 3.

Integrity check

The system files, applications, configuration files and application parameters can be checked for integrity as follows.

	Software WinPQ and WinPQ lite	**Hardware** PQI-DA smart and PQI-DE
Operating System	Microsoft Windows (use of different server and client versions)	Sciopta (special embedded real-time operating system)
System data	Installation files full version and update file: Verification of the digital signature by operating system (code signing certificate) and user	Installation file is firmware file Checking the test value (hash value) of type SHA-256
Application data	PQAdmin.exe PQClient.exe PQDBBackup.exe PQLVRSys.exe PQManager.exe PQOSMServer.exe PQPara.exe PQReport.exe PQRS232Server.exe PQSmartManager.exe PQStart.exe PQVisu.exe WinPQlite.exe Verification of the digital signature (Code Signing Certificate) analogous to the installation files	Not applicable, since application files are not accessible on the measuring instrument, access only possible via the user interface of the software (access see Chapter 3)
Configuration and parameter-files	Part of the SQLite system database with AES-256 encryption	Part of the firmware file, see line System

Use of cloud services

The system components do not support cloud services.

3 PQ system setup and secure system operation

In this chapter, the safety requirements of the BDEW white paper on the basic system (chapter 4.3) in which the PQ system is integrated are explained at the beginning. This is followed by the implementation of the requirements of the BDEW Whitepaper regarding the safety of the entire system consisting of the hardware and software components as well as its interfaces (chapters 4.4. and 4.5).

3.1 Notes on the PQ system field of application

The PQ system is always part of an already existing system, so it is always integrated into already existing infrastructures or environments. The software components and programs WinPQ and WinPQ lite are usually installed and set up on server systems which also provide other tasks and services. The hardware components are usually integrated into the existing network infrastructure and are usually not the only participants in these networks. Consequently, the systems are very different and due to this diversity and the fact that the PQ system has no influence on the security properties of the system into which it is integrated, only general security requirements and system requirements are formulated in the following which must be fulfilled for secure system operation. The security features of the PQ system are described and explained in detail starting in section 3.3.

3.2 Basic system

The basic prerequisites and/or requirements of the BDEW White Paper Chapter 4.3 for safe system operation of the basic system of components, i.e. the operating system in the case of software components and the firmware in the case of hardware components, are described below.

System requirements

The system requirements depend on the current version of the system components and are therefore stored in a separate document. The necessary network ports described there can be changed if necessary. These modifications, also e.g. the selection of the IP addresses of the components as well as other specific settings, must be recorded in the project-specific part of this document. The following requirements of the BDEW whitepaper regarding the security of the basic system are, as it were, prerequisites for the PQ system.

Basic protection and system hardening

All components of the basic system must be permanently hardened according to recognized best practice guides and be provided with current service packs and security patches. Unnecessary users, default users, programs, network protocols, services and services must be uninstalled or - if uninstallation is not possible - permanently deactivated and protected against accidental reactivation. The secure basic configuration of the entire system must be checked and documented. A detailed description of the measures to be taken is described in the BDEW white paper in Section 4.3.1. Setting up the PQ system itself for safe system operation is described below from Section 3.4 onwards.

Malware protection

The user of the PQ system is responsible for protecting the system on which the system components are operated. The basic system must meet the safety requirements of the BDEW white paper according to section 4.3.2.

Autonomous user authentication

Autonomous user authentication is described in detail in chapter 3.4.

Virtualization Technologies

The software components can also be set up on virtualized systems (note the system requirements of the WinPQ software). When using virtualization technologies on the part of the operator, e.g. setting up and operating the WinPQ software on a virtual server system, the requirements of the BDEW White Paper Section 4.3.4 must be met.

3.3 Security Architecture PQ-System

In the following section, the exact implementation of the requirements of the BDEW Whitepaper regarding the security of system components (BDEW Whitepaper chapter 4.5) as well as in chapter 3.6 of the interfaces, i.e. the network and communication (BDEW Whitepaper chapter 4.4) between the system components, is explained. The safety architecture of the entire system consisting of the numbered system components and the communication interfaces between these is schematically represented in the following fig. 3.

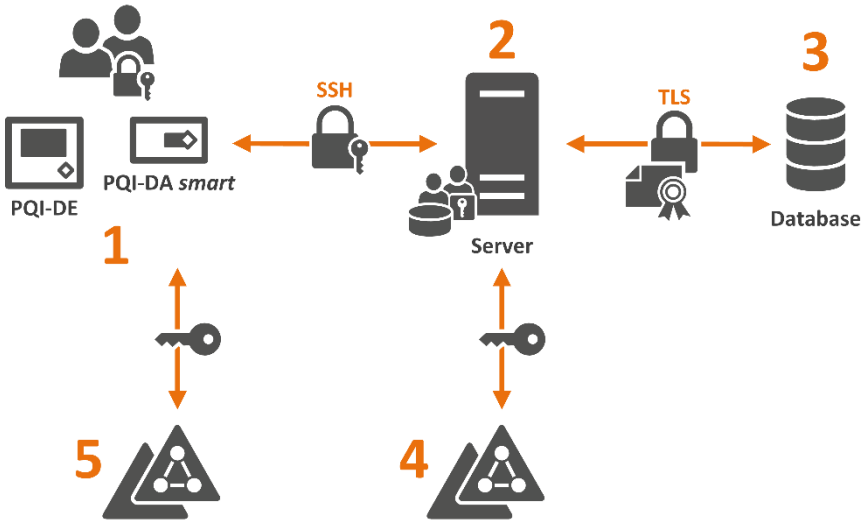


Figure 3: Schematic Overview Security Architecture Power Quality System

1 **Devices**
PQ-measuring devices (at mostly different installation locations or measuring points) which are connected to the WinPQ software to store the measured data in the system database (3) for further processing
Security: Users authenticate themselves with username and password when logging in to the device

2 **Server**
(Virtual) server on which the WinPQ software was installed and the corresponding processes are executed
Security: Users authenticate themselves on the WinPQ server by means of Windows user administration (Windows Authentication), e.g. at the domain controller (setup and administration by the responsible IT department, not part of the system description because it is individual, described in the project-specific part)

3 **Database**
System database of the WinPQ software
Security: Database access with username and password (setup during software installation, advanced database setup), database connection TLS encrypted

4 **Access service**
Administration and control of user access to the WinPQ server
Security: Windows logon service (operating system component)

5 **RADIUS authentication service (optional)**
Support of the Remote Authentication Dial-In User Service (RADIUS) service of the PQI-DA smart and PQI-DE devices (RADIUS server required)

The PQ devices (number 1 in Fig. 3) PQI-DA smart and PQI-DE (at mostly locally different installation locations or measuring points) record the measured data and WinPQ software (2) retrieves them for storage in the database (3). Access to the operating system of the (virtual) server system on which the software components WinPQ and WinPQ lite are installed is protected by the corresponding logon (4), e.g. Windows Authentication. The devices PQI-DA smart and PQI-DE from firmware version 2.2.8 also support the Remote Authentication Dial-In User Service (RADIUS) protocol as clients for authentication on a corresponding server (5). Setting up and maintaining the operating system as well as its administration and access protection is the task of the administrator who manages the system. The requirements of the BDEW whitepaper must be observed!

3.4 Application security of the system components

The safety of using the system components (cf. BDEW white papers, chapter 4.5) is described below. Users are authenticated directly at the devices or by means of the RADIUS authentication service (for further details and setup, refer to the manual of the devices). The necessary settings on the part of the RADIUS server are listed in Appendix A.4. The authentication of the users at the software is the corresponding login at the Windows operating system (Windows Authentication).

Access control with role concept

Access to the devices requires a login with user name and password. The granular access control to the different device functions, such as reading out measurement data or performing a firmware update, is realized by means of a role-based access control (RBAC). During the initial setup of the measuring instruments the following user accounts must be created with the help of the WinPQ lite software (for details on the implementation see the manual of the measuring instruments):

User	Rolle	Description
Name of the Administrator	Administrator	User who installs, maintains and supports the system. Among other things, the administrator has the right to change the security and system configuration: • Add, delete and lock users • Reset failed login attempts • Change role assignment of users • Change passwords of users • Create key for the WinPQ user (see below)
Name of the Operator	Operator	User who operates the system within the scope of its intended use. This also includes the right to change operationally relevant settings
Name of the user	User (read-only)	User who is allowed to retrieve the status of the system and read defined operating data, but is not authorized to make changes

WinPQ	winpq-m2m	For the autonomous (without direct login of a user) communication between the software WinPQ and the devices, e.g. the continuous reading of measurement data, a so-called machine-to-machine (M2M) user must be created

For normal system use, users with the roles operator and operator are sufficient. In the user administration of the devices it is also possible to set up additional user accounts with individual role assignment (for details see the manual of the devices). The user then logs on to the device in the software with the corresponding user name. A granular access control is realized via a RBAC database on the devices which contains all login data after the described setup. In this database the different device functions are also mapped to the corresponding execution rights. The assignment of execution and access rights of the roles are internally assigned to different profiles. These assignments are stored in Appendix A.1. An adaptation or extension of the roles is possible on request. Due to the high complexity and error-proneness such adaptations can only be made by the manufacturer. Any adjustments made must be documented in the project-specific part.

User Authentication and Login

Logging on to the device is done with user name and password, thus enabling personalized identification and authentication. An exception is the WinPQ M2M user, because he has to be able to log on to the device autonomously to perform continuous data transmission. When this M2M user is created, a key pair is generated, consisting of public and private key, with which the software can log on to the device. The key pairs are created in the installation directory \\\WinPQ\Ini\Keys named after IP address and port. The private key is encrypted using the Windows Data Protection API. This ensures that only users who have access to the Windows system on which WinPQ was installed can use the keys. Further details are described in Section 3.5.

Failed login attempts will be logged by the device and after several times (adjustable, see following table) wrong input of a password the corresponding user will be locked for a certain time (adjustable, see following table). The choice of the password must comply with the defined password policy. The settings must be configured individually for each device. These settings can be individually adjusted by users who belong to the Administrator role using the software in the user administration of the device:

Parameter	Default	Description
Min. password length	10	Minimum password length
Min. capital letters	1	Minimum number of capital letters in password
Min. small letters	1	Minimum number of lower case letters in password
Min. numbers	1	Minimum number of numbers in password
Min. other characters	1	Minimum number of other characters (special characters) in password
Login attempts	5	Minimum number of failed login attempts
Blocking time	1 sec	Time that must pass between two login attempts before you can login again
Unlock time	24 h	Time for which the user is blocked after the number of logon attempts has been reached

Authorization of actions on user and system level

The authorization of actions (with the described login) currently takes place locally on the devices. A connection to authentication services is in preparation to establish a non-local authorization authority. The PQ devices are pure measurement systems and therefore cannot execute any security relevant/critical actions.

Web applications and web services

No web applications or web services are used in the system.

Integrity check

The data integrity is checked on the side of the software components as well as the measuring devices themselves with regard to validity, syntax and value range. All security-relevant parameters and settings, e.g. changing passwords, can only be performed by users with the appropriate role assignment and are also checked accordingly by software and hardware before acceptance. Invalid data and actions are rejected and denied. As already mentioned, the PQ devices are pure measuring systems and therefore cannot perform any security relevant/critical actions.

Logging

All components of the system can be set to a uniform system time and this system time can be synchronized to external time sources with different possibilities. The devices support the following time sources or protocols, further details for setup are described in the manuals of the devices and the software:

- Synchronization with the local time of the computer connected to the device
- Synchronization with a DCF77 radio clock
- Time synchronization according to IEEE1344 or IRIGB formats 0 to 3 or 4 to 7
- Time synchronization by GPS clock with NMEA protocol

- Time synchronization via Network Time Protocol (NTP)
- Synchronization with a DCF77 radio clock
- Time synchronization according to IEEE1344 or IRIGB formats 0 to 3 or 4 to 7
- Time synchronization by GPS clock with NMEA protocol
- Time synchronization via Network Time Protocol (NTP)

The time synchronization of an entire system is very easy to achieve using NTP, for example, with an external GPS clock as a time source. The desired quality of the time source should be guaranteed in any case!

The measuring devices as well as the software components record precisely all actions, occurrences, possible errors etc. during runtime. In the WinPQ software this information is collected, processed and displayed in a message book and a system status. The log files are backed up at an adjustable central location. The transmission of log messages via syslog is possible and there are also different possibilities of alerting in the software. Further information regarding the different logging and alarm management options and settings are described in the manuals.

3.5 Commissioning and safe standard configuration

All components of the system are prepared at the factory for a safe standard configuration. After installation and connection of the measuring lines, the measuring devices must be put into operation directly at the device by means of a start-up assistant (short IBN-Wizard). In order to ensure a safe standard configuration, this IBN-Wizard must be completely executed before using the devices. As long as this procedure was not completed, the devices do not record any data and cannot be connected to the network or system. The practical execution of the IBN-Wizard is described in the manual of the devices. The integration of the devices into the software WinPQ, i.e. into the PQ system, requires a completion on the software side. As already described the initial user accounts are created. The initial operation of the measuring instrument is only completed when the user accounts listed in section 3.4 have been created. This ensures that the minimum requirements of the BDEW white paper regarding the role concepts are always met and that the standard access rights always correspond to the secure standard configuration. Only users who are assigned to the administrator role can create, lock and delete, read and edit security-relevant system settings and configuration values, e.g. users. All operations are logged in the device logs to track changes, see Section 3.4 Logging.

After completion of the IBN-Wizard on the measuring instruments the connection to the PQ-system is done in the software with another assistant. Afterwards the commissioning of the device in the safe standard configuration is completely finished. This coupling of the devices is necessary so that the software can read out the measurement data from the devices autonomously, i.e. without active user intervention. For this purpose, the WinPQ user (so-called machine-to-machine or M2M user) is set up when the user accounts are set up, which still has to be coupled with the software. The exact procedure is described in detail in the manual of the WinPQ software and the measuring instruments. The cryptographic mechanisms and protocols used are listed in Section 3.6 Network and Communication. The devices are only

configured in the safe operating state after the described setup and connection to the software.

The connection data of the connected measuring devices (IP address, port and hash of the public key for identification) are stored in the following folders

- *WinPQlite: \\Users\<USER>\AppData\Roaming\WinPQlite\Ini\Hash*
- *WinPQ: \\WinPQ\INI\Hash*

It is possible to reset configured measuring instruments, e.g. in case of an error due to a device defect. This process resets the devices completely to the factory settings, i.e. all data and settings are deleted. The measuring device must then be completely set up again (including the creation of user accounts etc.). The procedure is described in detail in the manual of the devices. In this way a clear separation of the safe and unsafe operating state is given.

3.6 Network and Communication Security

This chapter describes the implementation of the security requirements for the communication and network architecture of the system according to BDEW Whitepaper chapter 4.4 Network and Communication. The communication interfaces between the system components according to Fig. 3 are as follows:

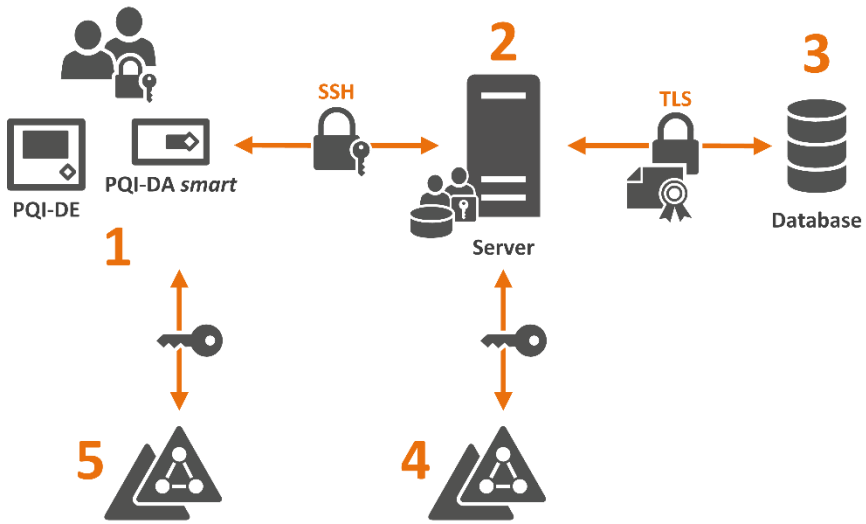


Figure 3: Schematic Overview Security Architecture Power Quality System

Used protocols and technologies

The security of the system with regard to the requirements of the BDEW white paper is guaranteed by the following cryptographic mechanisms, protocols and technologies. For a better overview, these are divided into the three interfaces or communication paths shown in Fig. 3.

1-2 Communication between devices and WinPQ server:
Secure setup or commissioning of the system components as well as secure communication during system operation between the hardware and software components or PQ measuring instruments and the WinPQ server

Section	**Communication between measuring devices and server (1-2)**
Technology standard	Secure Shell (SSH) Version 2
Encryption	Advanced Encryption Standard with 256 Bit (AES-256) key length
Key exchange	Elliptic Curve Diffie-Hellman (ECDH) porcedure
Key geneeration	Elliptic Curve Digital Signature Algorithm (ECDSA) with 512 Bit key length
Crypt. hashfunction	SHA2-512-HMAC (Verification of authenticity and integrity)

The second communication link is the database connection between the system with the software component WinPQ and the system database. In the standard installation (see commissioning instructions of the WinPQ software) the database is installed on the same system as the WinPQ software. However, it can also be installed at any other location within the system network as long as the system requirements are met (see System requirements of the WinPQ software).

2-3 Communication between server and database
Secure communication between the WinPQ software components and the system database

Section	**Communication between server and database (2-3)**
Technology standard	Transport Layer Security (TLS) for MySQL database use (requires MySQL Version 5.7.18 or above) Active Directory via Windows Authentication when using Microsoft SQL databases
Cipher-Suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
Certificate	SSL certificate (standard self-signed, use of other certificates possible, see references V.3)

2-4 Access Service Server

Integration of the server into a domain or similar with corresponding access control to the WinPQ server system (setup and administration by responsible IT, not part of the system description as individual, details are to be described in the project-specific part)

Section	Authentication and system login (2-3)
Technology standard	Windows authentication on the system (setup and administration by the system administrator) also for remote connections

1-5 Authentication service RADIUS

Devices PQI-DA smart and PQI-DE can optionally use the RADIUS protocol as client for authentication (for details see Appendix A.4) this requires at least one appropriately configured RADIUS server and corresponding configuration of the devices (for details see operating manuals of the devices)

Section	Authentication Service (1-5)
Technology standard	See appendix A.4

All system components use the above-mentioned security mechanisms with standard technologies for communication and application and can thus be easily integrated into the corporate network. The other network components, e.g. routers or switches, must meet the requirements of the BDEW white paper. These network components are not supplied by A. Eberle GmbH & Co. KG.

Secure network structure

The network structure and its segmentation must meet the requirements of the BDEW white paper. The PQ system is only to be integrated into already existing structures as described.

Secure remote access

The setup and operation of remote accesses (remote connections, etc.) is carried out by the operator of the network or infrastructure in which the PQ system is integrated. These must meet the requirements of the BDEW white paper.

Radio technologies

The system components do not have any radio technologies. If wireless technologies are used for the network infrastructure (e.g. UMTS modem), the requirements of the BDEW white paper must be met.

4 Development and system maintenance

This chapter deals in detail with the requirements of sections 4.6, 4.7 and 4.8 of the BDEW Whitepaper.

4.1 Development of the hardware and software components of the system

Secure development standards, quality management and release processes

The devices are developed by reliable and trained employees. Parts of the development have been outsourced to subcontractors who are subject to the same safety requirements. This is checked by regular audits. The A. Eberle GmbH & Co. KG develops devices according to recognized development standards and quality management/assurance processes. Within the development process, the following safety-relevant development steps are particularly taken into account:

- Definition of security requirements
- Threat modeling and risk analysis
- Derivation of requirements for system design and implementation
- Secure programming
- Request tests
- Safety tests before commissioning

Testing is based on the 4-eyes principle: development and tests are performed by different people. Test plans and procedures as well as expected and actual test results are documented and traceable. They can be viewed if required.

The A. Eberle GmbH & Co. KG has a documented development security process that covers physical, organizational and personal security and protects the integrity and confidentiality of the system. The effectiveness of the above mentioned process can be verified by an external audit. The A. Eberle GmbH & Co. KG has a programming guideline in which security-relevant requirements are explicitly addressed. With this guideline, for example, unsafe programming techniques and functions are avoided. Input data is verified, e.g. to prevent buffer overflow errors. Wherever possible, security-enhancing compiler options and libraries were used.

Secure development and test systems, integrity checks

The development is done on secure systems, the development environment, source code and binary files are protected against unauthorized access. All development systems are hardened according to recognized best-practice guidelines and the current state of the art and have up-to-date malware protection and all current security patches. Development and testing of the system as well as updates, extensions and security patches are carried out in a test environment separate from the production system.

No source code is stored on production systems with the exception of interpreted script languages. It is possible to check the integrity of source code and binary files for unauthorized changes by using secured checksums (SHA-2).

A version history is kept for all software in use, which makes it possible to trace the software changes made.

4.2 System maintenance

The requirements of the BDEW white paper regarding system maintenance (Chapter 4.7) will be dealt with in the following. All processes ensuring safe system management as well as maintenance processes must be recorded in the project-specific part.

Requirements for the maintenance processes

Remote and on-site access can only be carried out by a defined and trained group of people and only from secure systems. The access systems and IT infrastructures used for remote and on-site access are hardened in accordance with recognized best practice and the current state of the art and have up-to-date malware protection and all current security patches.

The defined maintenance process ensures that maintenance personnel only have access to the required systems, services and data and access to the corresponding premises within the scope of their activities.

The interactive remote access is carried out via personalized accounts and using 1-factor authentication. Remote access can only be granted if it is approved by the responsible operator for the respective person(s). In the case of external service providers, the release and disconnection must be done individually for each remote access session. A session shall be disconnected automatically after a reasonable period of time. In particular, the access systems used for remote access must be logically or physically decoupled from other networks during remote access. Physical decoupling is preferable to logical decoupling.

Secure update processes

The deployment and installation of updates, extensions and patches as well as the corresponding processes are described in detail in chapter 2. In addition, an information system and contact persons provide the corresponding information and data. Further individual processes are recorded in the project-specific part.

Configuration and change management, rollback options

The system components are operated with configuration and change management. The parameter and configuration files of the devices are to be saved, for example, if an error occurs. A rollback to a defined number of configuration states is supported. The corresponding execution instructions are described in the operating manuals of the measuring devices as well as in the software commissioning instructions. When the system is commissioned, appropriate measures and processes are defined together with the system operator and recorded in the project-specific part.

Handling of security vulnerabilities

The A. Eberle GmbH & Co. KG has a documented process for dealing with security vulnerabilities. Within this process it is possible for all parties involved, but also outsiders, to report actual or potential security gaps. A. Eberle GmbH & Co. KG is also informed promptly

about current security problems that could affect the system or subcomponents. The process defines how and in what time frame a known vulnerability is checked, classified, fixed and reported to all affected customers with appropriate recommendations for action. If the A. Eberle GmbH & Co. KG becomes aware of a security gap, it informs the customer under the condition of confidentiality and in a timely manner, even if no patch is yet available to fix the problem.

4.3 Data backup and emergency planning

The requirements of the BDEW white paper with regard to data backups and emergency planning (Chapter 4.8) are dealt with in the following. All processes ensuring safe system management and to be executed in case of emergency (deviation from normal operation) must be recorded in the project-specific part.

Backup: concept, procedures, documentation, tests

The software components have extensive options for planning and creating backups and restores. The corresponding concepts, procedures and tests are configured and carried out when the system is put into operation and their function is checked with tests. The work carried out is recorded in the project-specific part. Backups, e.g. of the entire operating system including the database, are also to be documented there, if set up. The configuration parameters of decentralized components can be saved centrally (on the software system). The documentation and procedures are adapted and retested if necessary in case of relevant system updates.

Emergency concept and restart planning

For relevant emergency and crisis scenarios, documented and tested procedures and recovery plans are provided, including information on recovery times. The documentation and procedures are adapted in case of relevant system updates and tested again within the acceptance procedure for release upgrades. The corresponding documentation is to be created in the project-specific part.

Section B

Project specific documentation

The following part of the security documentation represents the project-specific description. All project- or customer-specific extensions, adaptations and engineering services as well as all project-specific parameterizations, changes and adjustments are fully documented in the following. The following structure is exemplary and can be adapted according to requirements.

Project description

Short overview of the project as well as the responsible persons and their contact etc. as well as a description of the project including duration and other agreements etc.

System description

Detailed description of the commissioned system and its components.

Operating components

Detailed description of the system components.

Hardware

Detailed description of the hardware to be used, e.g. PQ devices including setup details etc.

Software

Detailed description of the software used, e.g. PQ software, antivirus programs, backup solutions including setup details etc.

Communication and network

Detailed description of the components used for system communication, e.g. network components including setup details etc.

Confidential information

Documentation of potentially confidential information, e.g. access data such as passwords or port clearances, should be submitted separately and securely.

Appendix and references

A.1 Roles of the RBAC database

No	Role	Description
1	administrator	A user, who installs, maintains and administrates the system. Has privileges to change the system and security configuration and settings.
2	operator	User who performs regular system operations. This might include the privilege to change operational system settings.
3	user	User, who is allowed to view the status of the system but is not allowed to make any changes to the system.
4	winpq-m2m	Role that is solely for WinPQ machine to machine communication.

A.2 Profiles of the RBAC database

No	Profile name	Description
1	WinPQ Connect	Connect WinPQ software to device.
2	Read Device Configuration	List and read all system settings.
3	Write Device Configuration	List and modify all system settings.
4	Stream Online Data	Open and close streams.
5	Trigger Record	Manually trigger a record via software
6	Remote Display Control	Read display screenshots and send keypress commands.
7	Read Log Files	Flush and read log data.
8	Read Device Status	Read the devices online status information.
9	Network Packet Capture	Start/stop network packet capturing.
10	Firmware Update	Perform firmware updates.
11	Read Measured Data	List and read (event) recordings.
12	Delete Measured Data	Delete (event) recordings.
13	CCCI Lua Cmnd Execution	Generally allow LUA command execution via CCCI.
14	User Account Management	Add, delete, read and modify user accounts.
15	Read PQ Statistics	Read the Power Quality statistic counter.
16	Set Device Time	Manually manipulate the devices data and time settings.

A.3 Assignment of roles and profiles in the RBAC database

		Profiles															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Roles	1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	2	X	X	X	X	X		X	X			X	X			X	
	3	X			X							X				X	
	4	X			X							X		X		X	

A.4 Settings RADIUS

	Description	**Note**
Devices	PQI-DA smart and PQI-DE	Supported devices
Firmware	Version 2.2.8 or above	Supported Firmware-Versions
Software	WinPQ 6.0 or above	Supported Software-Versions
Supported RFC	2865 2866	https://tools.ietf.org/html/rfc2865 https://tools.ietf.org/html/rfc2866
Modi	RADIUS inactive RADIUS exclusively RADIUS with fallback level RADIUS and Standard	local registration (reg.) only only reg. via RADIUS reg. via RADIUS and emergency users local and RADIUS registration possible
Vendor ID	59339	Vendor ID of A. Eberle GmbH & Co. KG
RADIUS Server	1-4	Support of max. 4 RADIUS servers
Port	1812	Used port can be changed
Server Secret	1-63 characters	Secret des RADIUS Servers
Timeout	3-10 seconds	Standard 3 seconds
Connection	1-5	Number of connection attempts per server
Role definitions	Administrator with role_id = 1 ControlOperator with role_id = 2 Oberserver with role_id = 3	Roles which must be set up with the corresponding ID on the RADIUS server!

V.1 Operating instructions, manuals and release notes

PQ-Devices

PQI-DA smart	Instruction manual https://www.a-eberle.de/sites/default/files/media/BA_PQI-DA%20smart_de_201910.pdf Release notes https://www.a-eberle.de/wp-content/uploads/2021/04/ReleaseNotes_WinPQlite_EN.pdf
PQI-DE	Instruction manual https://www.a-eberle.de/wp-content/uploads/2021/02/BA_PQI-DA-smart_EN.pdf Release notes see PQI-DA smart (identical)

PQ-Software

WinPQ	Instruction manual https://www.a-eberle.de/wp-content/uploads/2021/06/BA_WinPQ-Manual_EN_v5.1.pdf Commissioning manual https://www.a-eberle.de/wp-content/uploads/2021/06/BA_WinPQ-Commissioning_EN.pdf Release notes https://www.a-eberle.de/wp-content/uploads/2021/04/ReleaseNotes_WinPQ_EN.pdf
WinPQ lite	Operating manual (integrated in operating manual PQI-DA smart) https://www.a-eberle.de/sites/default/files/media/BA_PQI-DA%20smart_de_201910.pdf Release notes https://www.a-eberle.de/wp-content/uploads/2021/04/ReleaseNotes_WinPQlite_EN.pdf

V.2 Special setup of the system database

https://dev.mysql.com/doc/refman/5.7/en/using-encrypted-connections.html