Wir regeln das.

a-eberle

Sicherheitsdokumentation
Power Quality System

gemäß BDEW Whitepaper Mai 2018

Dieses Dokument beschreibt sämtliche sicherheitsrelevanten Einstellungen und Parameter der Einzelkomponenten sowie des Gesamtsystems gemäß BDEW Whitepaper der Version Mai 2018. Die sicherheitstechnischen Hinweise und Informationen in den Bedienungsanleitungen und Produktbeschreibungen behalten weiter ihre Gültigkeit.

Dokumentversion 1.2 vom 01.09.2021

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

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

Die Firma A. Eberle GmbH & Co. KG übernimmt keine Haftung für Schäden oder Verluste jeglicher Art, die aus Druckfehlern oder Änderungen in diesem Dokument entstehen.

Ebenso wird von der Firma A. Eberle GmbH & Co. KG keine Haftung für Schäden und Verluste jeglicher Art übernommen, die sich aus fehlerhaften Geräten oder durch Geräte, die vom Anwender geändert wurden, ergeben.

Copyright 2021 A. Eberle GmbH & Co. KG

Änderungen und Irrtümer vorbehalten.

Inhalt

Übersicht der Sicherheitsdokumentation 5
Bestandteile der Sicherheitsdokumentation 5
Anwendungsbereich 6
Informationssystem IT-Sicherheit 6
Anforderungen an die IT-Sicherheit 6
Allgemeine Hinweise 7
Teil A Administratordokumentation 8
1 Beschreibung Power Quality System und Komponenten 9
1.1 Hardwarekomponenten 9
1.2 Softwarekomponenten 10
1.3 Kommunikationsschnittstellen 10
1.4 Funktionsweise PQ-System 11
2 Sicherheit der Systemkomponenten 12
2.1 Sicherheitskonzept der Systemarchitektur 12
2.2 Aktualisierungen und Fehlerbehebungen der Systemkomponenten 12
2.3 Systemwartung und -pflege 13
2.4 Allgemeine Sicherheitsmechanismen 14
3 Einrichtung PQ-System und sicherer Systembetrieb 16
3.1 Anmerkungen zum PQ-System Einsatzbereich 16
3.2 Basissystem 16
3.3 Sicherheitsarchitektur PQ-System 18
3.4 Anwendungssicherheit der Systemkomponenten 19
3.5 Inbetriebnahme und sicherer Standard-Konfiguration 22
3.6 Sicherheit Netzwerk und Kommunikation 23
4 Entwicklung und Systemwartung 26
4.1 Entwicklung der Hard- und Software Komponenten des Systems 26
4.2 Systemwartung 27
4.3 Datensicherung und Notfallplanung 28

Teil B Projektspezifische Dokumentation 29
Projektbeschreibung 30
Systembeschreibung 30
Betriebskomponenten 30
Hardware 30
Software 30
Kommunikation 30
Vertrauliche Informationen 30
Anhang und Verweise 31
A.1 Rollen der RBAC Datenbank 31
A.2 Profile der RBAC Datenbank 31
A.3 Zuweisung der Rollen und Profile in der RBAC Datenbank 32
A.4 Einstellungen RADIUS 32
V.1 Bedienungsanleitungen, Handbücher und Veröffentlichungshinweise 33
V.2 Spezielle Einrichtung der Systemdatenbank 33

Übersicht der Sicherheitsdokumentation

Bestandteile der Sicherheitsdokumentation

Um die Anforderungen des Whitepapers an die Dokumentation zu erfüllen ist das Dokument zweigeteilt. Der erste Teil A beschreibt sämtliche grundlegenden sicherheitsrelevanten Einstellungen und Parameter der Einzelkomponenten sowie des Gesamtsystems. Bestandteil ist auch die Beschreibung der Systemarchitektur und sicherheitsspezifische Implementierungsdetails. Der zweite Teil B umfasst die projektspezifische Dokumentation und wird diesem Dokument spätestens zur Abnahme angefügt. Die Prüfung der gesamten Dokumentation auf Vollständigkeit und Richtigkeit ist Teil der Abnahmeprüfung. Am Ende des Dokuments sind die Verweise sowie weiterer, bspw. projektspezifischer, Anhang zu finden. Zu Beginn eines jeden Kapitels werden die korrespondierenden Abschnitte des BDEW Whitepaper genannt, also auf welche Anforderungen eingegangen wird.

Sicherheitsdokumentation:

- **Administratordokumentation**: Sicherheitsdokumentation des gesamten Systems
- **Projektdokumentation**: Projektspezifische Dokumentation

Die vollständige Dokumentation bestehend aus Installation, Einrichtung und weiterer Informationen welche System-Benutzer für die Inbetriebnahme und den Betrieb des Systems benötigen ist in den entsprechenden Bedienungsanleitungen beschrieben, siehe Verweise V.1.

Bedienungsanleitungen:

- **Hardware**: Bedienungsanleitung PQI-DA smart und PQI-DE
- **Software**: WinPQ Bedienungsanleitung und WinPQ Inbetriebnahmeanleitung

Die Versionshinweise (Release Notes) der aktuellen Soft- und Firmware Versionen der jeweiligen Hard- und Softwarekomponenten (siehe Anwendungsbereich) beinhalten sämtliche Informationen zu sicherheitsrelevanten Änderungen, neue, Funktionen sowie Fehlerbehebungen in der Version.

Versionshinweise:

- **Hardware**: Versionshinweise PQI-DA smart und PQI-DE
- **Software**: Versionshinweise WinPQ und WinPQ lite

Die aktuellsten Versionen dieser Dokumente sowie weitere Datenblätter etc. sind auf der Firmenwebsite im Download-Center unter folgendem Link verfügbar:
https://www.a-eberle.de/de/downloads/power-quality

Anwendungsbereich

Die vorliegende Sicherheitsdokumentation ist ausschließlich für das im Folgende beschriebene System sowie dessen Komponenten von der Firma A. Eberle GmbH & Co. KG gültig.

Hard- oder Software Komponente	Firm- oder Software Version
PQI-DA smart	2.0 oder höher
PQI-DE	2.0 oder höher
WinPQ lite	5.0 oder höher
WinPQ	5.0 oder höher

Informationssystem IT-Sicherheit

Auf der Firmenwebsite wurde für eine sichere Kommunikationsplattform eingerichtet um den sicheren Austausch von Informationen und Daten zu ermöglichen. Der entsprechende Zugang wird im Zuge eines Wartungsvertrages eingerichtet. Weitere Informationen für die Einrichtung und Anmeldung eines Zugangs werden bei Beginn des Wartungsvertrags zur Verfügung gestellt.

Anforderungen an die IT-Sicherheit

Die vorliegende Dokumentation sowie die Entwicklung und Umsetzung der Anforderungen an die Sicherheit des Systems sowie der Verbesserung und Weiterentwicklung basiert auf Grundlage folgender Dokumente:

- 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

Allgemeine Hinweise

Gemäß §11 Abs. 1a EnWG besteht die Pflicht zum Betrieb eines sicheren Energieversorgungsnetzes. Ebenso geht das EEG 2014 auf Sicherheit ein:

"Die Ausführung des Anschlusses und die übrigen für die Sicherheit des Netzes notwendigen Einrichtungen müssen den im Einzelfall notwendigen technischen Anforderungen des Netzbetreibers und § 49 des Energiewirtschaftsgesetzes entsprechen." Quelle §10 EEG 2014.

Des Weiteren heißt es im §36 - Fernsteuerbarkeit des EEG 2014 "[…] sind unter Berücksichtigung der einschlägigen Standards und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik Übertragungstechniken und Übertragungswege zulässig, die dem Stand der Technik bei Inbetriebnahme der Anlage entsprechen"

Diese Aussagen ergeben einen gewissen Freiraum bei der Ausgestaltung der Sicherheitsstufen. Eine gute Möglichkeit, den Anforderungen zu entsprechen, ist das vom BDEW veröffentlichte Whitepaper "Anforderungen an sichere Steuerungs- und Telekommunikationssysteme", dass mit der Ausarbeitung der Ausführungshinweise durch den Anwender den jeweiligen Grad der Sicherheitsvorkehrungen der Anlagen, Kommunikationskomponenten und deren Infrastruktur individuell festlegt.

Je nach Bedeutung der Anlage für die allgemeine Versorgungssicherheit sind im BDEW Whitepaper unterschiedliche Anforderungsprofile definiert. Folgende Aspekte können notwendig werden:

- Verwendung von Sicherheitszertifikaten
- Nutzung von einer Ende-zu-Ende Verschlüsselung wie SSH
- Verwendung einer Benutzerverwaltung
- Nutzung gesicherter Protokolle
- Verwendung von Firewalls

Teil A

Administratordokumentation

Der folgende Teil ist die Sicherheitsdokumentation für Administratoren und beschreibt sämtliche sicherheitsrelevanten Information des Power Quality (PQ) Systems. Sämtliche relevanten Beschreibungen für einen sicheren Betrieb hinsichtlich der Anforderungen des BDEW Whitepapers sind im Folgenden ausgeführt.

1 Beschreibung Power Quality System und Komponenten

Die Komponenten des Systems werden im Folgenden definiert und grundlegend beschrieben. Das Power Quality System besteht aus den im Folgenden definierten Software- und Hardware-Komponenten der Firma A. Eberle GmbH & Co. KG und wird kurz mit PQ-System bezeichnet. Aufgabe eines solchen PQ-Systems ist neben einem Echtzeit-Monitoring des Energiesystems

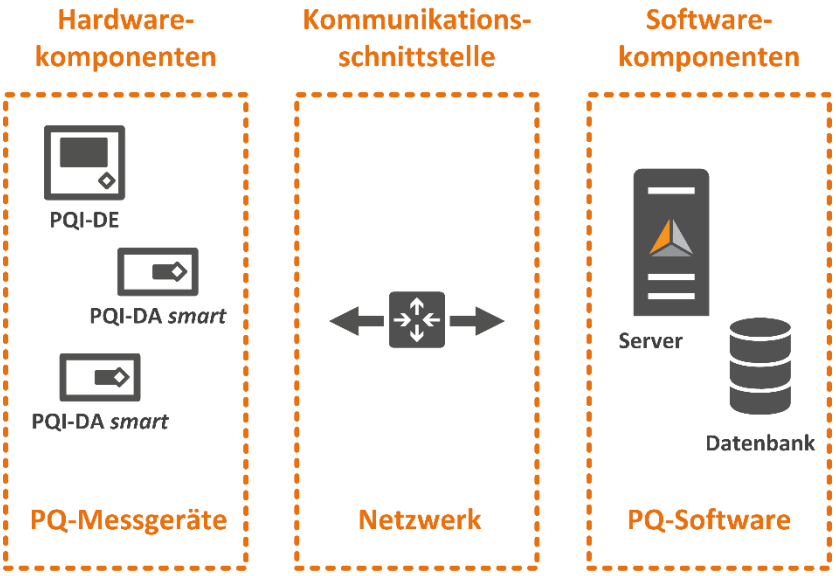


Abbildung 1: Systemkomponenten des PQ-System

die Messdaten, welche von den Messgeräten (allgemein als Hardwarekomponenten beschrieben) aufgezeichnet werden, in einer zentralen Datenbank für weitere Aufgaben der Datenverarbeitung wie Visualisierung Auswertung, Erstellung von Berichten etc. abzulegen.

1.1 Hardwarekomponenten

Ein PQ-System kann aus der Gerätetypen PQI-DA smart und PQI-DE in prinzipiell beliebiger Anzahl bestehen. Diese Detaillierte Informationen zu diesen Gerätetypen, einschließlich der Firmware welche auf den Geräten ausgeführt wird, sind in den entsprechenden Bedienungsanleitungen und Datenblättern beschrieben. Die PQ-Geräte haben die Aufgabe Power Quality Daten lückenlos an der installierten Messstelle aufzuzeichnen und teils bereits weiterzuverarbeiten. Nachdem die Geräte mit Hilfe der PQ-Software angebunden wurden, siehe Abschnitt 1.2, können die aufgezeichneten Daten dann weiterverarbeitet werden.

PQI-DA smart

Das Power Quality Messgerät PQI-DA smart verfügt über einen Ethernet Anschluss welcher für die Kommunikation mit den Softwarekomponenten innerhalb des PQ-Systems genutzt wird.

PQI-DE

Das Power Quality Messgerät PQI-DE basiert technisch auf dem PQI-DA smart PQ-Gerät. Die Kommunikation mit den Softwarekomponenten findet ebenfalls ausschließlich über die integrierte Ethernet-Schnittstelle statt.

1.2 Softwarekomponenten

Die Programme WinPQ und WinPQ lite kommen als Anwendersoftware zum Einsatz. Die beiden Softwarepakete sind in den entsprechenden Dokumenten wie Bedienungsanleitungen, Systemvoraussetzungen etc. detailliert beschrieben.

WinPQ

Die Software WinPQ für Windows Betriebssysteme hat zur Aufgabe die Messdaten der via Netzwerk angebundenen PQ-Geräte PQI-DA smart und PQI-DE in eine zentrale Datenbank abzulegen und so dem Anwender für weitere Aufgaben zur Verfügung zu stellen. Daneben verfügt die Software über zahlreiche weitere Funktionen wie beispielsweise Visualisierung und Auswertung von Messdaten sowie die Überwachung des Systems und Alarmierung im Fehlerfall.

WinPQ lite

Die Software WinPQ lite ist in der WinPQ integriert, aber auch einzeln verfügbar. Mit dieser kann der Nutzer die Einrichtung und Parametrierung der Hardwarekomponenten bzw. PQ-Messgeräte durchführen. Daneben ist auch eine rudimentäre Auswertung von Messdaten von angebundenen PQ-Geräten möglich.

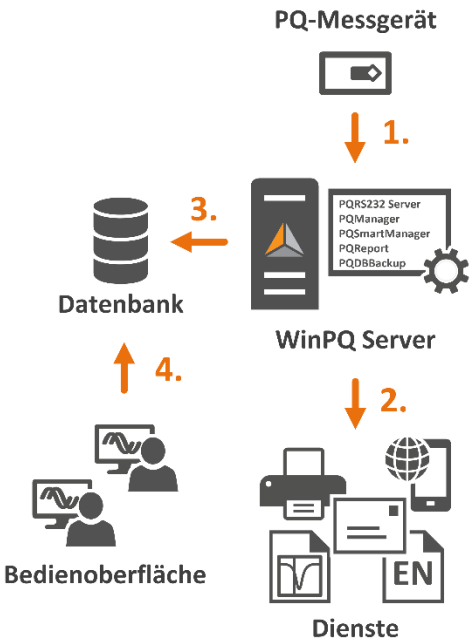
1.3 Kommunikationsschnittstellen

Für die Datenübertragung von den PQ-Messgeräten in die zentrale Datenbank der WinPQ Software ist eine Kommunikationsstrecke zwischen diesen Komponenten notwendig. Die entsprechende Kommunikationsschnittstelle auf Seiten der Messgeräte ist der Ethernet-Anschluss. Auf Seiten der WinPQ Software die Netzwerkschnittstelle des Computers auf welchem die WinPQ Software installiert ist. Als Netzwerkprotokoll kommt TCP/IP zum Einsatz. Sämtliche Systemkomponenten müssen über entsprechende IP-Einstellungen etc. verfügen um miteinander kommunizieren zu können.

! Im Weiteren wird ausschließlich die Einrichtung sowie der Betrieb des PQ-Systems in der sicheren (Standard-) Konfiguration beschrieben. In dieser Konfiguration wurde das System für den sicheren Betrieb vollständig eingerichtet. Die Einrichtung bzw. das Aktivieren von weiteren Schnittstellen ist eine Abweichung und ist somit keine sichere Konfiguration!

1.4 Funktionsweise PQ-System

Die Funktionsweise des PQ-Systems bestehend aus den Komponenten aus dem vorherigen Kapitel ist schematisch in folgender Abbildung dargestellt.



1. **Datentransfer**
   WinPQ System Prozesse transferieren Daten von den eingerichteten Messgeräten auf den WinPQ Server
2. **Daten- und Alarmmanagement**
   Verarbeitung und Analyse der Gerätedaten sowie evtl. Auslösung von (Alarm-) Meldungen
3. **Datenbank**
   Automatische Ablage der Gerätedaten in der WinPQ Datenbank (lokal oder auf entferntem Datenbankserver)
4. **Datenauswertung, Analyse und Visualisierung** durch Anwender über die Bedienoberfläche der Software

Abbildung 2: Funktionsweise PQ-System

Die WinPQ Software übernimmt im Power Quality System die gesamte Datenverarbeitung vom PQ-Messgerät bis hin zur Ablage der Messdaten in der Datenbank. Auch bietet die Software mehrere Visualisierungskomponenten für die Bedienung und um den Zugriff auf die Messdaten zu ermöglichen. Der Verbindungsaufbau erfolgt vom WinPQ Server zum Messgerät. Die Software realisiert diese Aufgaben mit mehreren Prozessen welche auf dem WinPQ Server nach der Installation der Software aufgeführt werden. Die Prozesse für einen Betrieb mit den zuvor genannten PQ-Geräten und Komponenten sind:

Prozessname	Anwendung	Beschreibung
MySQL	mysql.exe	Instanz der Datenbank
PQSmartManager	PQSmartManager.exe	Datenübertragung und -management der PQ-Gerätetypen PQI-DA smart und PQI-DE
PQReport	PQReport.exe	Systemfunktionen wie Pflege- (SQL-Checks, Timeout Überwachung, etc.) und Verwaltungsaufgaben (Nachrichten zwischen WinPQ Programmen) sowie Berechnung von Statistiken und Berichten

Die Prozesse werden in der Aufgabenplanung alle 24 Stunden neu initialisiert und werden im per Standard im Systemkonto ausgeführt. Die Einstellungen können je nach Anforderung geändert werden und die entsprechenden Anpassungen werden im projektspezifischen Teil festgehalten.

2 Sicherheit der Systemkomponenten

Im diesem Kapitel werden die allgemeinen Merkmale des sicheren Systembetriebs beschrieben. Speziell wird auf die Anforderungen des BDEW Whitepaper Kapitel 4.1 Allgemeine Anforderungen eingegangen.

2.1 Sicherheitskonzept der Systemarchitektur

Das Sicherheitskonzept des PQ-Systems wurde ganzheitlich für alle Systemkomponenten und deren Interaktion untereinander sowie mit den Benutzern entwickelt und umgesetzt. Von der initialen Inbetriebnahme über den Normalbetrieb bis hin zur Wartung und Pflege des Systems wurden alle Einzelkomponenten und das Gesamtsystem auf einen sicheren Betrieb hin entworfen. Grundlage für dieses Systemdesign bilden die Prinzipien Security-By-Design, Minimal-Need-To-Know-Prinzip, Defence-In-Depth Prinzip und das Redundanz-Prinzip. Die Umsetzung wird im Folgenden näher beschrieben und erläutert. Die Sicherheitsarchitektur, die Inbetriebnahme sowie der sichere Betrieb des Systems werden in Kapitel 3 ausgeführt.

2.2 Aktualisierungen und Fehlerbehebungen der Systemkomponenten

Aktualisierungen bzw. Patchfähigkeit der Systemkomponenten

Alle Komponenten des PQ-Systems sind patchfähig, können also mittels neuer Soft- oder Firmware Versionen um sicherheitsrelevante und funktionale Updates aktualisiert werden. Die jeweilige Vorgehensweise ist in den entsprechenden Handbüchern der Soft- und Hardware Komponenten beschrieben. Aus Sicherheitsgründen ist eine Herabstufung der Soft- und Firmware Version, also ein Downgrade nicht möglich.

Patch-Management und -Sicherheit

Der Anwender kann sämtliche Komponenten des Systems eigenständig aktualisieren. Die Aktualisierung kann auf Wunsch auch durch den Hersteller oder einen Dienstleister durchgeführt werden. Der Vorgang wird nicht automatisch durchgeführt und kann nur durch Benutzer mit entsprechender administrativen Rolle durchgeführt werden. Die Autorisierung für die Durchführung von Updates erfolgt an den Komponenten wie folgt:

Komponente	**Autorisierung Update**	**Schutzmechanismus**
Software WinPQ und WinPQ lite	Software Update: Überprüfung der digitalen Signatur durch Software und Fingerabdruck durch Nutzer	Anmeldung am Betriebssystem durch Windows Authentifizierung
Hardware PQI-DA smart und PQI-DE	Firmware Update: Überprüfung des Prüfwerts (Hashwert)	Benutzeranmeldung auf dem Gerät mittels lokaler oder entferner (RADIUS) RBAC

Die Integrität der Aktualisierungen ist wie folgt gesichert und ein Update wird gegebenenfalls verweigert.

Komponente	Integritätsprüfung Update	Kryptograf. Mechanismus
Software WinPQ und WinPQ lite	Software Update: Überprüfung der digitalen Signatur durch Betriebssystem (Code Signing Zertifikat)	Öffentlicher Schlüssel: RSA 2048 Bit Signaturhashalgorithmus: SHA-256
Hardware PQI-DA smart und PQI-DE	Firmware Update: Überprüfung des Prüfwerts (Hashwert)	Hashalgorithmus: SHA-256

Sämtliche Vorgänge werden von den Komponenten aufgezeichnet bzw. geloggt. Die entsprechenden Log-Dateien sind vor nicht autorisiertem Zugriff und Manipulation geschützt. Ein Auslesen ist nur Benutzern mit entsprechenden Rechten möglich. Die genaue Beschreibung des Auslesens von Log-Dateien ist den jeweiligen Bedienungsanleitungen zu entnehmen.

2.3 Systemwartung und -pflege

Bereitstellung von Sicherheits-Patches für alle Systemkomponenten

Die Bereitstellung der Aktualisierungen bzw. Patches der Systemkomponenten erfolgt über die Firmenwebsite. Im öffentlich zugänglichen Bereich werden immer ausschließlich die aktuellsten Software- und Firmware-Version zum Download bereitgestellt. Im geschlossenen Bereich, welcher jedem registriertem Nutzer mit Wartungsvertrag durch entsprechende Anmeldung zur Verfügung steht, auch individuelle Versionen sowie u.U. weitere Daten für diesen. Dieser geschlossene Login-Bereich ist in Abschnitt „Informationssystem IT-Sicherheit“ am Beginn dieses Dokuments beschrieben. Eine Übersicht der Updatezeiträume und Bereitstellungsquellen der Systemkomponenten können folgender Tabelle entnommen werden.

Komponente	Updatezeitraum	Bereitstellung Updatedateien
WinPQ	2 Jahre ab Kaufdatum dann kostenpflichtige Verlängerung	https://www.a-eberle.de/de/download-center-categories/für-festinstallierte-geräte
WinPQ lite	Gesamte Produktlebenszeit	https://www.a-eberle.de/de/download-center-categories/für-festinstallierte-geräte
PQI-DA smart und PQI-DE	Gesamte Produktlebenszeit	https://www.a-eberle.de/de/download-center-categories/für-festinstallierte-geräte-0

Die Aktualisierungen werden erst nach erfolgreichem Bestehen der entsprechenden Freigabetests veröffentlicht, Details siehe Kapitel 4. Die wichtigsten Implementierungen bzw. Änderungen der Soft- und Firmware-Updates wie neue Funktionen, Fehlerbehebungen etc. sind in den Änderungslisten (Release Notes) aufgeführt, welche ebenfalls auf der Firmenwebsite zur Verfügung gestellt werden.

Unterstützung für eingesetzte Systemkomponenten

Die Komponenten des Systems werden im Zuge der Betriebs- und Laufzeittests hinsichtlich der Kompatibilität mit verschiedenen fremdentwickelten Komponenten intensiv geprüft. Insbesondere die Softwarekomponenten WinPQ und WinPQ lite werden auf einen fehlerfreien Betrieb mit neuen Versionen von Betriebs- und Datenbanksystemen getestet. Die Liste der unterstützten Betriebs- und Datenbanksysteme sowie die Systemvoraussetzungen bzw. -anforderungen der Softwarekomponenten sind der WinPQ Inbetriebnahmeanleitung V.1 zu entnehmen. Diese wird für jede neue Softwareversion fortlaufend aktualisiert. Die Softwarekomponenten können mit unterschiedlichen Datenbanksystemen und -versionen erworben werden.

Wartungsverträge

Die Bereitstellung eines kontinuierlichen Supports für das System bzw. das Einspielen von bspw. Aktualisierungen des Datenbanksystems wird über Wartungsverträge realisiert. Diese werden in Umfang und Laufzeit individuell mit dem Auftragnehmer vereinbart. Mit diesen kann sichergestellt werden, dass das eingesetzte System zu jeder Zeit auf dem aktuellsten Stand ist. Die genauen Vereinbarungen mit Ansprechpartnern, Abkündigungsverfahren und alle relevanten Mindestlaufzeiten wie z.B. Last-Customer-Shipping und End-Of-Support werden im projektspezifischen Teil dieses Dokuments verbindlich festgelegt. Weitere Details sind im Kapitel 4.2 Systemwartung beschrieben.

2.4 Allgemeine Sicherheitsmechanismen

Verschlüsselung vertraulicher Daten und kryptografische Verfahren

Das System überträgt und sichert vertrauliche Daten stets verschlüsselt unter Verwendung aktueller Verschlüsselungsstandards welche durch das BSI entsprechend empfohlen werden. Im Kapitel 3 werden die eingesetzten Protokolle und kryptografischen Verfahren detailliert beschrieben.

Sichere Standard-Konfiguration

Alle Komponenten des Systems werden in einer definierten Grundkonfiguration ausgeliefert. Im Zuge der Inbetriebnahme der Systemkomponenten wird die verbleibenden Sicherheitseinstellungen, bspw. die Einrichtung von Benutzerkonten und Passwörtern sowie die Kopplung der Messgeräte an die Softwarekomponenten, durchgeführt. Nach dieser Erstinstallation bzw. (Wieder-) Inbetriebnahme werden die einzelnen Komponenten für einen sicheren Betrieb bezüglich der Anforderungen des BDEW Whitepapers eingerichtet. Nach Abschluss dieser Einrichtung befinden sich die Komponenten in sicheren Betriebszustand. Die Grundkonfiguration sowie die Inbetriebnahme bzw. der Abschluss der Einrichtung für einen sicheren Systembetrieb werden im Detail in Kapitel 3 beschrieben.

Integritätsprüfung

Die Systemdateien, Anwendungen, Konfigurationsdateien und Anwendungsparameter sind wie folgt auf Integrität prüfbar.

	Software WinPQ und WinPQ lite	**Hardware** PQI-DA smart und PQI-DE
Betriebssystem-plattform	Microsoft Windows (Einsatz von verschiedenen Server- und Client-Versionen)	Sciopta (spezielles eingebettetes Echtzeit-Betriebssystem)
System-dateien	Installationsdateien Vollversion- und Update-Datei: Überprüfung der digitalen Signatur durch Betriebssystem (Code Signing Zertifikat) und Anwender	Installationsdatei ist Firmware-Datei Überprüfung des Prüfwerts (Hashwert) vom Typ SHA-256
Anwendungs-dateien	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 Überprüfung der digitalen Signatur (Code Signing Zertifikat) analog der Installationsdateien	Nicht anwendbar, da Anwendungsdateien auf Messgerät nicht zugänglich, Zugriff nur über Anwenderschnittstelle der Software möglich (Zugang siehe Kapitel 3)
Konfiguration- und Parameter-dateien	Bestandteil der SQLite Systemdatenbank mit AES-256 Verschlüsselung	Bestandteil der Firmware-Datei, siehe Zeile System

Nutzung von Cloud-Diensten

Die Systemkomponenten unterstützen keine Cloud-Dienste.

3 Einrichtung PQ-System und sicherer Systembetrieb

In diesem Kapitel werden eingangs die Sicherheitsanforderungen des BDEW Whitepapers an das Basissystem (Kapitel 4.3) in welches das PQ-System integriert wird ausgeführt. Anschließend die Umsetzung der Anforderungen des BDEW Whitepapers an die Sicherheit des gesamten Systems bestehend aus den Hard- und Software Komponenten sowie dessen Schnittstellen (Kapitel 4.4. und 4.5).

3.1 Anmerkungen zum PQ-System Einsatzbereich

Das PQ-System ist immer Teil eines bereits vorhandenen Systems, wird also immer in bereits bestehende Infrastrukturen bzw. Umgebungen integriert. Die Softwarekomponenten bzw. Programme WinPQ und WinPQ lite werden meist auf Serversystemen installiert und eingerichtet welche teils auch andere Aufgaben und Dienste bereitstellen. Die Hardwarekomponenten werden meist in die bestehende Netzwerkinfrastruktur eingebunden und sind meist nicht die einzigen Teilnehmer in diesen Netzen. Folglich sind die Systeme sehr unterschiedlich und aufgrund dieser Vielfältigkeit sowie dem Umstand, dass das PQ-System keinen Einfluss auf die Sicherheitseigenschaften des Systems in welches es integriert wird hat, werden im Folgenden nur allgemeine Sicherheitsanforderungen sowie Systemvoraussetzungen formuliert welche für einen sicheren Systembetrieb erfüllt werden müssen. Die Sicherheitseigenschaften des PQ-Systems werden ab Abschnitt 3.3 genau beschrieben und erläutert.

3.2 Basissystem

Die grundlegenden Voraussetzungen bzw. Anforderungen des BDEW Whitepaper Kapitels 4.3 für einen sicheren Systembetrieb des Basissystems der Komponenten, also das Betriebssystem bei den Softwarekomponenten sowie die Firmware bei den Hardwarekomponenten, sind im Folgenden beschrieben.

Systemvoraussetzungen

Die Systemvoraussetzungen sind abhängig von der aktuellen Version der Systemkomponenten und deswegen in einem separaten Dokument hinterlegt. Die dort beschriebenen notwendigen Netzwerkports können falls notwendig geändert werden. Diese Anpassungen, auch bspw. die Wahl der IP-Adressen der Komponenten sowie weitere spezifische Einstellungen müssen im projektspezifischen Teil dieses Dokuments festgehalten werden. Die folgenden Anforderungen des BDEW Whitepapers an die Sicherheit des Basissystems sind gleichsam Voraussetzungen für das PQ-System.

Grundsicherung und Systemhärtung

Alle Komponenten des Basissystems müssen anhand anerkannter Best-Practice-Guides dauerhaft gehärtet und mit aktuellen Service-Packs und Sicherheits-Patches versehen sein. Unnötige Benutzer, Default User, Programme, Netzwerkprotokolle, Dienste und Services müssen deinstalliert, oder – falls eine Deinstallation nicht möglich ist – dauerhaft deaktiviert und gegen versehentliches Reaktivieren geschützt werden. Die sichere Grundkonfiguration des Gesamtsystems muss überprüft und dokumentiert sein. Eine detaillierte Ausführung der

Maßnahmen ist im BDEW Whitepaper im Abschnitt 4.3.1 beschrieben. Die Einrichtung des PQ-Systems selbst für einen sicheren Systembetrieb ist ab Abschnitt 3.4 im Folgenden ausgeführt.

Schadsoftware-Schutz

Der Nutzer des PQ-Systems ist für den Schutz des Systems auf welchem die Systemkomponenten betrieben werden verantwortlich. Das Basissystem muss den Sicherheitsanforderungen des BDEW Whitepapers nach Abschnitt 4.3.2 genügen.

Autonome Benutzerauthentifizierung

Die autonome Benutzerauthentifizierung wird in Kapitel 3.4 detailliert beschrieben.

Virtualisierungstechnologien

Die Softwarekomponenten können auch auf virtualisierten Systemen (Systemanforderungen der WinPQ Software beachten) eingerichtet werden. Beim Einsatz von Virtualisierungstechnologien seitens des Betreibers, bspw. die Einrichtung und Betrieb der WinPQ Software auf einem virtuellen Serversystem, müssen die Anforderungen des BDEW Whitepaper Abschnitt 4.3.4 erfüllt werden.

3.3 Sicherheitsarchitektur PQ-System

Im folgenden Abschnitt wird die exakte Umsetzung der Anforderungen des BDEW Whitepapers an die Sicherheit der Systemkomponenten (BDEW Whitepaper Kap. 4.5) sowie in Kapitel 3.6 der Schnittstellen, also des Netzwerks und der Kommunikation (BDEW Whitepaper Kap. 4.4) zwischen den Systemkomponenten, erläutert. Die Sicherheitsarchitektur des gesamten Systems bestehend aus den nummerierten Systemkomponenten und den Kommunikationsschnittstellen zwischen diesen ist schematisch in folgender Abb. 3 dargestellt.

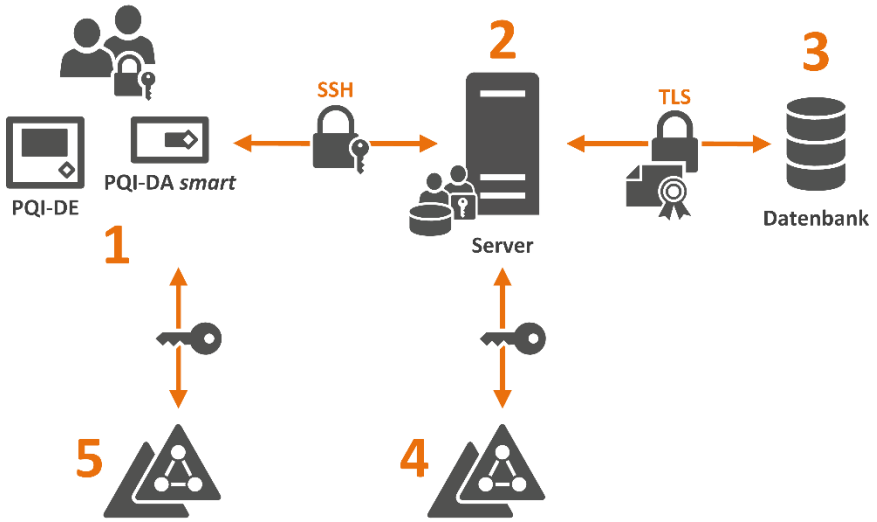


Abbildung 3: Schematische Übersicht Sicherheitsarchitektur Power Quality System

1 **Messgeräte**
PQ-Messgeräte (an meist unterschiedlichen Einbauorten bzw. Messstellen) welche an die WinPQ Software angebunden sind um die Messdaten in der Systemdatenbank (3) für die weitere Verarbeitung abzulegen
Sicherheit: Benutzer authentifizieren sich bei einer Anmeldung auf dem Gerät mittels Benutzername und Passwort

2 **Server**
(Virtueller) Server auf dem die WinPQ Software installiert wurde und die entsprechenden Prozesse ausgeführt werden
Sicherheit: Benutzer authentifizieren sich auf dem WinPQ Server mittels eingerichteter Windows Benutzerverwaltung (Windows Authentication) bspw. am Domänencontroller (Einrichtung und Administration durch zuständige IT, nicht Teil der Systembeschreibung da individuell, wird im projektspezifischen Teil beschrieben)

3 **Datenbank**
Systemdatenbank der WinPQ Software
Sicherheit: Datenbankzugang mit Benutzername und Passwort (Einrichtung bei der Softwareinstallation, Erweiterte Datenbankeinrichtung), Datenbankverbindung TLS verschlüsselt

4 **Zugangsdienst**
Verwaltung und Steuerung des Benutzerzugangs auf den WinPQ Server
Sicherheit: Windows Anmeldedienst (Betriebssystemkomponente)

5 **RADIUS Authentifizierungsdienst (Optional)**
Unterstützung des Remote Authentication Dial-In User Service (RADIUS) Dienstes der PQI-DA smart und PQI-DE Geräte (RADIUS Server notwendig)

Die PQ-Geräte (Nummer 1 in Abb. 3) PQI-DA smart und PQI-DE (an meist örtlich unterschiedlichen Einbauorten bzw. Messstellen) zeichnen die Messdaten auf und WinPQ Software (2) holt diese für die Ablage in der Datenbank (3) ab. Der Zugang auf das Betriebssystem des (virtuellen) Serversystems auf welchem die Softwarekomponenten WinPQ und WinPQ lite installiert sind wird über die entsprechende Anmeldung (4), bspw. Windows Authentication, geschützt. Die Geräte PQI-DA *smart* und PQI-DE unterstützen ab Firmware Version 2.2.8 auch das Remote Authentication Dial-In User Service (RADIUS) Protokoll als Clients für die Authentifizierung an einem entsprechenden Server (5). Die Einrichtung und Wartung des Betriebssystems sowie dessen Verwaltung und Zugangssicherung ist Aufgabe des Administrators welcher das System verwaltet. Die Anforderungen des BDEW Whitepapers sind hierbei zu beachten!

3.4 Anwendungssicherheit der Systemkomponenten

Die Sicherheit der Anwendung der Systemkomponenten (vgl. BDEW Whitepapers Kap. 4.5) ist im Folgenden beschrieben. Die Authentifizierung der Nutzer erfolgt direkt an den Geräten oder mittels des Authentifizierungsdienstes RADIUS (weitere Details und Einrichtung im Handbuch der Geräte). Die notwendigen Einstellungen seitens des RADIUS Servers sind in Anhang A.4 gelistet. Die Authentifizierung der Nutzer an der Software ist die entsprechende Anmeldung an dem Windows Betriebssystem (Windows Authentication).

Zugriffskontrolle mit Rollenkonzept

Der Zugriff auf die Geräte erfordert eine Anmeldung mit Benutzername und Passwort. Die granulare Zugriffskontrolle auf die unterschiedlichen Gerätefunktionen wie bspw. das Auslesen von Messdaten oder die Durchführung eines Firmware-Updates ist mittels einer rollenbasierten Zugangskontrolle (role-based-access-control, kurz RBAC) realisiert. Bei der initialen Einrichtung der Messgeräte müssen mit Hilfe der Software WinPQ lite folgende Benutzerkonten angelegt werden (Details zur Durchführung siehe Handbuch der Messgeräte):

Benutzername	Rolle	Beschreibung
Name des Administrators	Administrator	Benutzer, der das System installiert, wartet und betreut. Der Administrator hat u. a. die Berechtigung zur Änderung der Sicherheits- und Systemkonfiguration: • Hinzufügen, löschen und sperren von Benutzern • Fehlgeschlagenen Anmeldeversuche zurücksetzen • Rollenzugehörigkeit von Benutzern ändern • Passwörter von Benutzern ändern • Schlüssel für den WinPQ Benutzer (siehe weiter unten) erzeugen
Name des Operators	Operator	Benutzer, der das System im Rahmen der vorgesehenen Nutzung bedient. Dies beinhaltet auch das Recht zur Änderung von betriebsrelevanten Einstellungen

Name des Benutzers	Bediener (read-only)	Benutzer, der den Status des Systems abrufen und definierte Betriebsdaten lesen darf, aber nicht berechtigt ist Änderungen durchzuführen
WinPQ	winpq-m2m	Für die autonome (ohne direkte Anmeldung eines Benutzers) Kommunikation zwischen der Software WinPQ und den Geräten, bspw. das kontinuierliche Auslesen von Messdaten, muss ein sogenannter Machine-to-Machine (M2M) Nutzer angelegt werden

Zur normalen Systemnutzung sind Nutzer mit der Rollenzugehörigkeit Operator und Bediener ausreichend. In der Benutzerverwaltung der Geräte ist es auch möglich weitere Benutzerkonten mit individueller Rollenzugehörigkeit einzurichten (Details siehe Handbuch der Geräte). Der Nutzer meldet sich am Gerät dann in der Software mit dem entsprechend vergebenen Nutzernamen an. Eine granulare Zugriffskontrolle wird über eine RBAC Datenbank auf den Geräten realisiert welche nach der beschriebenen Einrichtung sämtlich Anmeldedaten enthält. In dieser sind auch die unterschiedlichen Gerätefunktionen auf entsprechende Ausführungsrechte abgebildet. Die Zuweisungen der Ausführungs- und Zugriffsrechte der Rollen sind intern weiter unterschiedlichen Profilen zugewiesen. Diese Zuweisungen sind im Anhang A.1 hinterlegt. Eine Anpassung oder Erweiterung der Rollen ist auf Anfrage möglich. Aufgrund der hohen Komplexität und Fehleranfälligkeit sind solche Anpassungen nur durch den Hersteller möglich. Vorgenommene Anpassungen sind im projektspezifischen Teil zu dokumentieren.

Benutzer-Authentifizierung und Anmeldung

Die Anmeldung am Gerät erfolgt mit Benutzername und Passwort und ermöglicht so eine personenspezifische Identifizierung und Authentifizierung. Eine Ausnahme stellt der WinPQ M2M Benutzer dar, da dieser sich auch autonom am Gerät anmelden können muss um die kontinuierliche Datenübertragung durchführen zu können. Beim Anlegen dieses M2M Benutzers wird ein Schlüsselpaar erzeugt, bestehend aus öffentlichem und privaten Schlüssel, mit welchem sich die Software am Gerät anmelden kann. Die Schlüsselpaare werden im Installationsverzeichnis *\\WinPQ\Ini\Keys* nach IP-Adresse und Port genannt angelegt wobei der private Schlüssel mittels der Windows Data Protection API verschlüsselt wird. Hiermit ist sichergestellt, dass nur Benutzer welche Zugriff auf das Windows System haben, auf welchem die WinPQ installiert wurde, die Schlüssel nutzen können. Weitere Details sind im Abschnitt 3.5 beschrieben.

Fehlgeschlagene Anmeldeversuche werden von dem Gerät protokolliert bzw. geloggt und nach mehrmaliger (einstellbar, siehe folgende Tabelle) Falscheingabe eines Passworts der entsprechende Nutzer für eine bestimmte Zeit (einstellbar, siehe folgende Tabelle) gesperrt. Die Wahl des Passworts muss den festgelegten Passwort Richtlinien (Passwort-Policy) entsprechen. Die Einstellungen müssen für jedes Gerät individuell konfiguriert werden. Diese

Einstellungen können durch Nutzer welche der Rolle Administrator angehören individuell mit Hilfe der Software in der Benutzerverwaltung des Geräts angepasst werden:

Parameter	Default	Beschreibung
Min. Passwortlänge	10	Minimale Länge des Passworts
Min. große Buchstaben	1	Minimale Anzahl an Großbuchstaben im Passwort
Min. kleine Buchstaben	1	Minimale Anzahl an Kleinbuchstaben im Passwort
Min. Zahlen	1	Minimale Anzahl an Zahlen im Passwort
Min. sonstige Zeichen	1	Minimale Anzahl sonstiger Zeichen (Sonderzeichen) im Passwort
Anmeldeversuche	5	Minimale Anzahl an fehlgeschlagenen Anmeldeversuchen
Sperrzeit	1 sec.	Zeit welche zwischen zwei Anmeldeversuchen verstreichen muss bevor sich wieder angemeldet werden kann
Entsperrzeit	24 h	Zeit für welche der Benutzer nachdem die Anzahl an Anmeldeversuchen erreicht wurde gesperrt wird

Autorisierung von Aktionen auf Benutzer- und Systemebene

Die Autorisierung von Aktionen (mit der beschriebenen Anmeldung) findet aktuell lokal auf den Geräten statt. Eine Anbindung an Authentifizierungsdienste ist in Vorbereitung um eine nicht-lokale Autorisierungsstelle zu etablieren. Die PQ-Geräte sind reine Messsysteme und können folglich keine sicherheitsrelevanten/-kritischen Aktionen ausführen.

Web-Applikationen und Web-Services

In dem System kommen keinerlei Web-Applikationen oder Web-Services zum Einsatz.

Integritätsprüfung

Die Datenintegrität wird auf Seiten der Softwarekomponenten sowie den Messgeräten selbst hinsichtlich Gültigkeit, Syntax und Wertebereich geprüft. Sämtliche sicherheitsrelevanten Parameter und Einstellungen, bspw. Ändern von Passwörtern, können nur durch Nutzer mit der entsprechenden Rollenzugehörigkeit durchgeführt werden und wird ebenfalls entsprechend von Software und Hardware vor Übernahme geprüft. Ungültige Daten und Aktionen werden verworfen und verweigert. Wie bereits erwähnt sind die PQ-Geräte reine Messsysteme und können folglich keine sicherheitsrelevanten/-kritischen Aktionen ausführen.

Protokollierung (Logging)

Alle Komponenten des Systems können auf eine einheitliche Systemzeit gestellt werden und diese Systemzeit mit unterschiedlichen Möglichkeiten auf externe Zeitquellen synchronisiert werden. Die Geräte unterstützen folgende Zeitquellen bzw. Protokolle, weitere Details zur Einrichtung sind in den Handbüchern der Geräte und der Software beschrieben:

- Synchronisation mit der Lokalzeit des Computers welche mit dem Gerät verbunden ist

- Synchronisation mit einer DCF77 Funkuhr
- Zeitsynchronisation nach IEEE1344 oder IRIGB Formate 0 bis 3 oder 4 bis 7
- Zeitsynchronisation mittels GPS-Uhr mit NMEA Protokoll
- Zeitsynchronisation via Network Time Protokoll (NTP)

Die Zeitsynchronisation eines gesamten Systems ist mittels NTP bspw. mit einer externen GPS-Uhr als Zeitquelle sehr einfach möglich. Die gewünschte Qualität der Zeitquelle sollte in jedem Fall sichergestellt sein!
Die Messgeräte wie auch die Softwarekomponenten protokollieren präzise alle Aktionen, Vorkommnisse, evtl. Fehler usw. während der Laufzeit. In der WinPQ Software werden diese Informationen gesammelt, aufbereitet und in einem Meldebuch sowie einem Systemstatus angezeigt. Die Logdateien werden an einem einstellbaren zentralen Ort gesichert. Die Übermittlung der Log Meldungen via *syslog* ist möglich und es sind auch unterschiedliche Möglichkeiten der Alarmierung in der Software einstellbar. Weitere Informationen hinsichtlich der verschiedenen Protokollierungs- und des Alarm-Management Optionen und Einstellungen sind in den Handbüchern beschrieben.

3.5 Inbetriebnahme und sicherer Standard-Konfiguration

Alle Komponenten des Systems werden werksseitig für eine sichere Standard-Konfiguration vorbereitet. Die Messgeräte müssen nach Einbau und Anschluss der Messleitungen mittels eines Inbetriebnahme Assistenten (kurz IBN-Wizard) direkt am Gerät in Betrieb genommen werden. Um eine sichere Standard-Konfiguration zu gewährleisten, muss vor Verwendung der Geräte dieser IBN-Wizard vollständig durchgeführt werden. Solange dieser Vorgang nicht abgeschlossen wurde zeichnen die Geräte keinerlei Daten auf und können auch nicht in das Netzwerk bzw. System angebunden werden. Die praktische Durchführung des IBN-Wizards ist im Handbuch der Geräte beschrieben. Die Einbindung der Geräte an die Software WinPQ also in das PQ-System erfordert einen Abschluss auf Seiten der Software. Wie bereits beschrieben werden die initialen Benutzerkonten angelegt. Die Inbetriebnahme des Messgeräts ist erst abgeschlossen, wenn die Einrichtung der in Abschnitt 3.4 gelisteten Benutzerkonten erfolgt ist. Auf diese Weise ist sichergestellt, dass die Minimalanforderungen des BDEW Whitepapers hinsichtlich der Rollenkonzepte immer erfüllt werden und das die Standard-Zugriffsrechte so immer der sicheren Standard Konfiguration entsprechen. Nur Benutzer welche der Rolle Administrator zugehörig sind können sicherheitsrelevante Systemeinstellungen und Konfigurationswerte, bspw. Nutzer anlegen, sperren und löschen, lesen und editieren. Die Alle Vorgänge werden in den Logs der Geräte protokolliert um Änderungen nachverfolgen zu können, siehe in Abschnitt 3.4 Protokollierung.

Nach Abschluss des IBN-Wizards an den Messgeräten wird die Anbindung an das PQ-System in der Software mit einem weiteren Assistenten durchgeführt. Anschließend ist die Inbetriebnahme des Geräts in der sicheren Standard-Konfiguration vollständig abgeschlossen. Diese Kopplung der Geräte ist notwendig, damit die Software autonom, also ohne aktives Zutun eines Benutzers, die Messdaten von den Geräten auslesen kann. Für diesen Zweck wird bei der Einrichtung der Benutzerkonten der WinPQ Nutzer (sogenannter Machine-to-Machine

kurz M2M Nutzer) eingerichtet, welcher noch mit der Software gekoppelt werden muss. Der exakte Vorgang ist im Handbuch der Software WinPQ sowie der Messgeräte detailliert beschrieben. Die eingesetzten kryptografischen Mechanismen und Protokolle werden im Abschnitt 3.6 Netzwerk und Kommunikation gelistet. Die Geräte sind erst nach der beschriebenen Einrichtung und Anbindung an die Software im sicheren Betriebszustand konfiguriert.

Die Verbindungsdaten der angebundenen Messgeräte (IP-Adresse, Port und Hash des öffentlichen Schlüssels für die Identifizierung) werden in den folgenden Ordnern abgelegt:

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

Ein Zurücksetzen von eingerichteten Messgeräten, bspw. im Fehlerfall bei einem Gerätedefekt ist möglich. Dieser Vorgang setzt die Geräte vollständig auf die Werkseinstellungen zurück, löscht also sämtliche Daten und Einstellungen. Das Messgerät muss anschließend wieder vollständig neu eingerichtet werden (inkl. Anlegen der Benutzerkonten etc.). Das Vorgehen ist in Handbuch der Geräte detailliert beschrieben. Auf diese Weise ist eine eindeutige Trennung von dem sicheren und unsicheren Betriebszustand gegeben.

3.6 Sicherheit Netzwerk und Kommunikation

Dieses Kapitel beschreibt die Umsetzung der Sicherheitsanforderungen an die Kommunikations- und Netzwerkarchitektur des Systems nach BDEW Whitepaper Kapitel 4.4 Netzwerk und Kommunikation. Die Kommunikationsschnittstellen zwischen den Systemkomponenten nach Abb. 3 sind wie folgt:

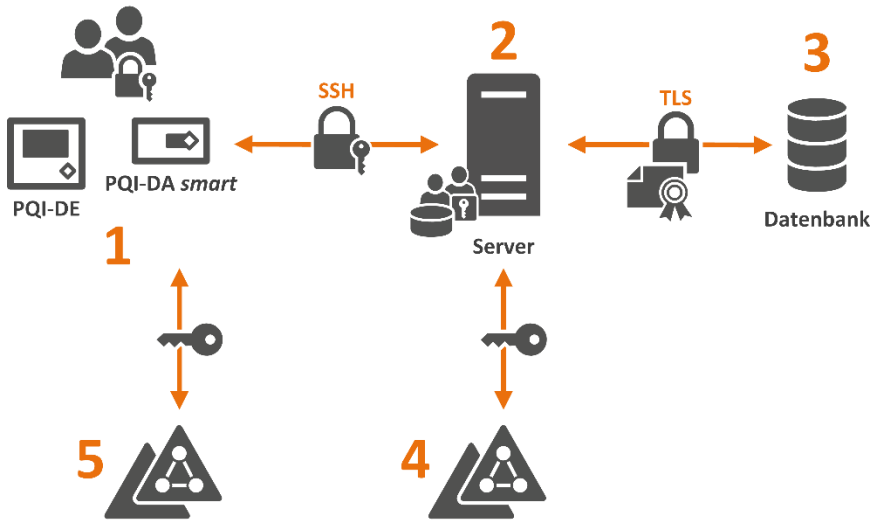


Abbildung 3: Schematische Übersicht Sicherheitsarchitektur Power Quality System

Eingesetzte Protokolle und Technologien

Die Sicherheit des Systems hinsichtlich der Anforderungen des BDEW Whitepaper wird mit folgenden kryptografischen Mechanismen, Protokollen und Technologien gewährleistet. Zur besseren Übersicht sind diese in die drei Schnittstellen bzw. Kommunikationsstrecken nach Abb. 3 aufgeteilt.

1-2 Kommunikation zwischen Geräten und WinPQ Server:
Sichere Einrichtung bzw. Inbetriebnahme der Systemkomponenten sowie eine sichere Kommunikation während des Systembetriebs zwischen den Hardware- und Softwarekomponenten bzw. PQ-Messgeräten und dem WinPQ Server

Bereich	**Kommunikation zwischen Messgeräten und Server (1-2)**
Technologiestandard	Secure Shell (SSH) Version 2
Verschlüsselung	Advanced Encryption Standard mit einer Schlüssellänge von 256 Bit (AES-256)
Schlüsselaustausch	Elliptic Curve Diffie-Hellman (ECDH) Verfahren
Schlüsselerzeugung	Elliptic Curve Digital Signature Algorithm (ECDSA) mit 512 Bit Schlüssellänge
Krypt. Hashfunktion	SHA2-512-HMAC (Prüfung Authentizität und Integrität)

Die zweite Kommunikationsstrecke ist die Datenbankverbindung zwischen dem System mit der Softwarekomponenten WinPQ und der Systemdatenbank. In der Standardinstallation (vgl. Inbetriebnahmeanleitung der WinPQ Software) wird die Datenbank auf demselben System installiert wie auch die Software WinPQ. Diese kann aber auch an beliebiger anderer Stelle innerhalb des Systemnetzwerks eingerichtet werden solange die Systemvoraussetzungen erfüllt werden (siehe Systemvoraussetzungen der WinPQ Software).

2-3 Kommunikation zwischen Server und Datenbank
Sichere Kommunikation zwischen den Softwarekomponenten WinPQ und der Systemdatenbank

Bereich	**Kommunikation zwischen Server und Datenbank (2-3)**
Technologiestandard	Transport Layer Security (TLS) bei Einsatz von MySQL Datenbanken (Voraussetzung MySQL Version 5.7.18 oder höher) Active Directory via Windows Authentication bei Einsatz von Microsoft SQL Datenbanken
Cipher-Suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
Zertifikat	SSL-Zertifikat (Standard selbstsigniert, Verwendung anderer Zertifikate möglich, siehe Verweise V.3)

2-4 Zugangsdienst Server

Integration des Servers in eine Domäne o.ä. mit entsprechendem Zugangssteuerung auf das WinPQ Serversystem (Einrichtung und Administration durch zuständige IT, nicht Teil der Systembeschreibung da individuell, Details sind im projektspezifischen Teil zu beschreiben)

Bereich	**Authentifikation und Anmeldung am System (2-3)**
Technologiestandard	Windows Authentication auf dem System (Einrichtung und Verwaltung durch den Systemadministrator) auch für Remote-Verbindungen

1-5 Authentifizierungsdienst RADIUS

Geräte PQI-DA smart und PQI-DE können für die Authentifizierung optional das RADIUS Protokoll als Client nutzen (Details siehe Anhang A.4) dies erfordert mindestens einen entsprechend eingerichteten RADIUS Server sowie entsprechende Konfiguration der Geräte (Details siehe Bedienungsanleitungen der Geräte)

Bereich	**Authentifizierungsdienst (1-5)**
Technologiestandard	Siehe Anhang A.4

Alle Systemkomponenten nutzen für die Kommunikation und Anwendung die genannten Sicherheitsmechanismen mit Standardtechnologien und können so auf einfache Art und Weise in das Unternehmensnetzwerk eingebunden werden. Die weiteren Komponenten des Netzwerks, bspw. Router oder Switches müssen die Anforderungen des BDEW Whitepapers erfüllen. Diese Netzwerkkomponenten werden nicht von der Firma A. Eberle GmbH & Co. KG zur Verfügung gestellt.

Sichere Netzwerkstruktur

Die Netzwerkstruktur sowie deren Segmentierung müssen die Anforderungen des BDEW Whitepapers erfüllen. Das PQ-System ist ausschließlich in bereits vorhandene Strukturen, wie beschrieben, zu integrieren.

Sichere Fernzugänge

Die Einrichtung und der Betrieb von Fernzugängen (Remote-Verbindungen etc.) ist durch den Betreiber des Netzwerks bzw. der Infrastruktur in welche das PQ-System integriert wird ausgeführt. Diese müssen die Anforderungen des BDEW Whitepapers genügen.

Funktechnologien

Die Systemkomponenten verfügen über keinerlei Funktechnologien. Wenn für die Netzwerkinfrastruktur Funktechnologien zum Einsatz kommen sollten (z.B. UMTS-Modem) müssen die Anforderungen des BDEW Whitepapers erfüllt werden.

4 Entwicklung und Systemwartung

In diesem Kapitel wird ausführlich auf die Anforderungen der Abschnitte 4.6, 4.7 und 4.8 des BDEW Whitepapers eingegangen.

4.1 Entwicklung der Hard- und Software Komponenten des Systems

Sichere Entwicklungsstandards, Qualitätsmanagement und Freigabeprozesse

Die Geräte werden von zuverlässigen und geschulten Mitarbeitern entwickelt. Teile der Entwicklung wurden an Subunternehmer ausgelagert, an die die gleichen Sicherheitsanforderungen gestellt werden. Dies wird durch regelmäßige Audits geprüft. Die A. Eberle GmbH & Co. KG entwickelt Geräte nach anerkannten Entwicklungsstandards und Qualitätsmanagement/-sicherungs-Prozessen. Im Rahmen des Entwicklungsprozesses werden insbesondere die folgenden sicherheitsrelevanten Entwicklungsschritte berücksichtigt:

- Definition der Sicherheitsanforderungen
- Bedrohungsmodellierung und Risikoanalyse
- Ableitung von Anforderungen an Systemdesign und Implementierung
- Sichere Programmierung
- Anforderungstests
- Sicherheitsprüfungen vor der Inbetriebnahme

Das Testen erfolgt nach dem 4-Augen-Prinzip: Entwicklung und Tests werden von verschiedenen Personen durchgeführt. Die Testpläne und -prozeduren sowie erwartete und tatsächliche Test-ergebnisse sind dokumentiert und nachvollziehbar. Sie können bei Bedarf eingesehen werden.
Die A. Eberle GmbH & Co. KG verfügt über einen dokumentierten Entwicklungs-Sicherheitsprozess, der die physische, organisatorische und personelle Sicherheit abdeckt und die Integrität und Vertraulichkeit des Systems schützt. Die Effektivität des o.g. Prozesses kann durch eine externe Auditierung überprüft werden. Die A. Eberle GmbH & Co. KG verfügt über eine Programmierrichtlinie, in der auf sicherheitsrelevante Anforderungen explizit eingegangen wird. Mit dieser werden bspw. unsichere Programmiertechniken und Funktionen vermieden. Eingabedaten werden verifiziert, um z.B. Pufferüberlauf-Fehler zu verhindern. Wo möglich, wurden sicherheitserhöhende Compileroptionen und Bibliotheken benutzt.

Sichere Entwicklungs- und Test-Systeme, Integritäts-Prüfung

Die Entwicklung erfolgt auf sicheren Systemen, die Entwicklungs-umgebung, Quellcode und Binärdateien sind gegen fremde Zugriffe gesichert. Alle Entwicklungssysteme sind anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik gehärtet und verfügen über einen aktuellen Schadsoftwareschutz sowie sind mit allen aktuellen Sicherheits-Patches versehen. Entwicklung und Test des Systems sowie von Updates, Erweiterungen und Sicherheits-Patches erfolgen in einer vom Produktivsystem getrennten Test-Umgebung erfolgen.
Auf Produktiv-Systemen werden mit Ausnahme von interpretierten Skriptsprachen kein Quellcode gespeichert. Es ist möglich, die Integrität von Quellcode und Binärdateien durch

gesicherte Prüfsummen (SHA-2) auf unerlaubte Veränderungen hin zu überprüfen. Es wird eine Versionshistorie für alle eingesetzte Software geführt, die es ermöglicht, die durchgeführten Softwareänderungen nachzuvollziehen.

4.2 Systemwartung

Auf die Anforderungen des BDEW Whitepapers hinsichtlich der Wartung des Systems (Kapitel 4.7) wird im Folgenden eingegangen. Sämtliche Prozesse welche die sichere Systemführung gewährleisten wie auch Wartungsprozesse müssen im projektspezifischen teil festgehalten werden.

Anforderung an die Wartungsprozesse

Der Fern- und Vor-Ort-Zugriff kann nur durch einen definierten und geschulten Personenkreis und nur von abgesicherten Systemen aus erfolgen. Die für den Fern- und Vor-Ort-Zugriff genutzten Zugangs-Systeme und IT-Infrastrukturen sind anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik gehärtet und verfügen über einen aktuellen Schadsoftwareschutz sowie sind mit allen aktuellen Sicherheits-Patches versehen. Durch den definierten Wartungsprozess ist sichergestellt, dass das Wartungspersonal im Rahmen seiner Tätigkeiten nur Zugriff auf die benötigten Systeme, Dienste und Daten und Zutritt zu den entsprechenden Räumlichkeiten erhält.
Der interaktive Fern-Zugang erfolgt über personalisierte Accounts und unter Nutzung von 1-Faktor-Authentifizierung. Ein Fern-Zugriff kann nur erfolgen kann, wenn dieser vom verantwortlichen Betreiber für die entsprechende Person(en) freigegeben wird. Bei externen Dienstleistern müssen die Freigabe und die Trennung für jede Fernzugriffssitzung einzeln erfolgen. Eine Sitzung ist nach Ablauf einer angemessenen Zeit automatisch zu trennen. Insbesondere sind die für den Fernzugriff genutzten Zugangs-Systeme während des Fern-Zugriffs von anderen Netzen logisch oder physisch zu entkoppeln. Eine physische Entkopplung ist der logischen vorzuziehen.

Sichere Updateprozesse

Die Bereitstellung und Installation von Updates, Erweiterungen und Patches sowie die entsprechenden Prozesse werden detailliert in Kapitel 2 beschrieben. Darüber hinaus werden über ein Informationssystem und Ansprechpartner entsprechende Informationen und Daten zu Verfügung gestellt. Weitere individuelle Prozesse werden im projektspezifischen Teil festgehalten.

Konfigurations- und Change-Management, Rollbackmöglichkeiten

Die Systemkomponenten werden mit einem Konfigurations- und Change-Management betrieben. Die Parameter- und Konfigurationsdateien der Geräte sollen bspw. gesichert werden, falls ein Fehlerfall eintritt. Ein Rollback auf eine festgelegte Anzahl an Konfigurationszuständen wird unterstützt. Die entsprechenden Ausführungshinweise sind in den Bedienungsanleitungen der Messgeräte sowie der Inbetriebnahme-Anleitung der Software beschrieben. Bei der Inbetriebnahme des Systems werden entsprechende Maßnahmen und Prozesse gemeinsam mit dem Systembetreiber definiert und im projektspezifischen Teil festgehalten.

Behandlung von Sicherheitslücken

Die A. Eberle GmbH & Co. KG verfügt über einen dokumentierten Prozess, um Sicherheitslücken zu behandeln. Innerhalb dieses Prozesses ist es allen Beteiligten, aber auch Außenstehenden möglich, tatsächliche oder potentielle Sicherheitslücken zu melden. Auch informiert sich die A. Eberle GmbH & Co. KG zeitnah über aktuelle Sicherheitsprobleme, die das System oder Teilkomponenten betreffen könnten. Der Prozess definiert, wie und in welchem Zeitrahmen eine bekanntgewordene Lücke überprüft, klassifiziert, behoben und an alle betroffenen Kunden mit entsprechenden Maßnahmenempfehlungen weitergemeldet wird. Wenn der A. Eberle GmbH & Co. KG eine Sicherheitslücke bekannt wird, informiert sie den Auftraggeber unter der Maßgabe der Vertraulichkeit und zeitnah, auch wenn noch kein Patch zur Behebung des Problems zur Verfügung steht.

4.3 Datensicherung und Notfallplanung

Auf die Anforderungen des BDEW Whitepapers hinsichtlich von Datensicherungen und Notfallplanung (Kapitel 4.8) wird im Folgenden eingegangen. Sämtliche Prozesse welche die sichere Systemführung gewährleisten und im Notfall (Abweichung vom Normalbetrieb) ausgeführt werden müssen im projektspezifischen Teil festgehalten werden.

Backup: Konzept, Verfahren, Dokumentation, Tests

Die Softwarekomponenten verfügen über umfangreiche Möglichkeiten für die Planung und Erstellung von Datensicherungen (Backups) und Wiederherstellungen. Die entsprechenden Konzepte, Verfahren und Tests werden bei der Inbetriebnahme des Systems konfiguriert und durchgeführt sowie deren Funktion mit Tests geprüft. Die vorgenommenen Arbeiten werden im projektspezifischen Teil festgehalten. Auch Sicherungen bspw. des gesamten Betriebssystems inklusive Datenbank sind dort, falls eingerichtet, zu dokumentieren. Die Konfigurationsparameter von dezentralen Komponenten können zentral (auf dem Softwaresystem) gesichert werden. Die Dokumentation und die Verfahren werden bei relevanten System Updates falls notwendig angepasst und erneut getestet.

Notfallkonzeption und Wiederanlaufplanung

Für relevante Notfall- und Krisenszenarien werden dokumentierte und getestete Vorgehensweisen und Wiederanlaufpläne inklusive Angabe der Wiederherstellungszeiten zur Verfügung gestellt. Die Dokumentation und Verfahren werden bei relevanten System-Updates angepasst und im Rahmen des Abnahmeverfahrens für Release-Wechsel erneut getestet. Die entsprechende Dokumentation ist im projektspezifischen Teil anzulegen.

Teil B

Projektspezifische Dokumentation

Der folgende Teil der Sicherheitsdokumentation stellt die projektspezifische Beschreibung dar. Alle projekt- bzw. kundenspezifischen Erweiterungen, Anpassungen und Engineering-Dienstleistungen sowie alle projektspezifischen Parametrierungen, Änderungen und Anpassungen werden im Folgenden vollständig dokumentiert. Die folgende Gliederung ist beispielhaft und kann je nach Anforderung angepasst werden.

Projektbeschreibung

Kurze Übersicht des Projekts sowie der verantwortlichen Personen und deren Kontakt etc. sowie eine Beschreibung des Projekts inkl. Laufzeit und sonstiger Vereinbarungen etc.

Systembeschreibung

Detaillierte Beschreibung des in Betrieb genommenen Systems und dessen Komponenten.

Betriebskomponenten

Detaillierte Beschreibung der Systemkomponenten.

Hardware

Detaillierte Beschreibung der zum Einsatz kommenden Hardware, bspw. PQ-Geräte inkl. Einrichtungsdetails etc.

Software

Detaillierte Beschreibung der zum Einsatz kommenden Software, bspw. PQ-Software, Antivirenprogramme, Backuplösungen inkl. Einrichtungsdetails etc.

Kommunikation

Detaillierte Beschreibung der zum Einsatz kommenden Komponenten für die Systemkommunikation bspw. Netzwerkkomponenten inkl. Einrichtungsdetails etc.

Vertrauliche Informationen

Dokumentation von potentiell vertraulichen Informationen, z.B. Zugangsdaten wie Passwörter oder Portfreigaben sollte separat auf sicherem Wege übergeben werden.

Anhang und Verweise

A.1 Rollen der RBAC Datenbank

Nr.	Rolle	Beschreibung
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 Profile der RBAC Datenbank

Nr.	Profilname	Beschreibung
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 Zuweisung der Rollen und Profile in der RBAC Datenbank

		Profile															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Rollen	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 Einstellungen RADIUS

	Beschreibung	**Anmerkung**
Geräte	PQI-DA smart und PQI-DE	Unterstützte Geräte
Firmware	Version 2.4.2 oder höher	Unterstützte Firmware-Versionen
Software	WinPQ 6.0 oder höher	Unterstützte Software-Versionen
Unterstützte RFC	2865 2866	https://tools.ietf.org/html/rfc2865 https://tools.ietf.org/html/rfc2866
Modi	RADIUS inaktiv RADIUS ausschließlich RADIUS mit Rückfallebene RADIUS und Standard	nur lokale Anmeldung nur Anmeldung via RADIUS Anmeldung via RADIUS und Notfallnutzer lokale und RADIUS Anmeldung möglich
Vendor ID	59339	Vendor ID von A. Eberle GmbH & Co. KG
RADIUS Server	1-4	Unterstützung von max. 4 RADIUS Servern
Port	1812	Verwendeter Port kann geändert werden
Server Secret	1-63 Zeichen	Secret des RADIUS Servers
Timeout	3-10 Sekunden	Standard 3 Sekunden
Verbindung	1-5	Anzahl der Verbindungsversuche je Server
Rollendefinitionen	Administrator mit role_id = 1 ControlOperator mit role_id = 2 Oberserver mit role_id = 3	Rollen welche mit der entsprechenden ID auf dem RADIUS Server eingerichtet sein müssen!

V.1 Bedienungsanleitungen, Handbücher und Veröffentlichungshinweise

PQ-Messgeräte

PQI-DA smart	Bedienungsanleitung https://www.a-eberle.de/wp-content/uploads/2021/02/BA_PQI-DA-smart_DE.pdf Veröffentlichungshinweise https://www.a-eberle.de/wp-content/uploads/2021/04/ReleaseNotes_WinPQlite_DE.pdf
PQI-DE	Bedienungsanleitung https://www.a-eberle.de/wp-content/uploads/2021/02/BA_PQI-DE-144_DE.pdf Veröffentlichungshinweise siehe PQI-DA smart (identisch)

PQ-Software

WinPQ	Bedienungsanleitung https://www.a-eberle.de/wp-content/uploads/2021/06/BA_WinPQ-Manual_DE_v5.1.pdf Inbetriebnahmeanleitung https://www.a-eberle.de/wp-content/uploads/2021/06/BA_WinPQ-Commissioning_DE.pdf Veröffentlichungshinweise https://www.a-eberle.de/wp-content/uploads/2021/04/ReleaseNotes_WinPQ_DE.pdf
WinPQ lite	Bedienungsanleitung (in Bedienungsanleitung PQI-DA smart integriert) https://www.a-eberle.de/wp-content/uploads/2021/02/BA_PQI-DA-smart_DE.pdf Veröffentlichungshinweise https://www.a-eberle.de/wp-content/uploads/2021/04/ReleaseNotes_WinPQlite_DE.pdf

V.2 Spezielle Einrichtung der Systemdatenbank

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