Branchenempfehlung Strommarkt Schweiz

Richtlinien für die Datensicherheit von intelligenten Messsystemen, Anhang 1

Zertifizierungsanforderungen an intelligente Messsysteme für die Datensicherheit

RL-DSP – CH, Anhang 1, Ausgabe 2018

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Telefon +41 62 825 25 25, Fax +41 62 825 25 26, info@strom.ch, www.strom.ch

Impressum und Kontakt

Herausgeber
Verband Schweizerischer Elektrizitätsunternehmen VSE
Hintere Bahnhofstrasse 10, Postfach
CH-5001 Aarau
Telefon +41 62 825 25 25
Fax +41 62 825 25 26
info@strom.ch
www.strom.ch

Autoren
Gemäss Hauptdokument

Druckschrift Nr. 1045 d, Ausgabe 2018

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Gültigkeitsbereich

(1) Im Dokument „Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz“, BFE 11/2014, [2], auch oft als „Mindestanforderungen“ bezeichnet, ist die Architektur eines intelligenten Messsystems definiert worden (Abbildung 1).

(2) Diese Definition ist in der Stromversorgungsverordnung (StromVV) Änderung vom 1. November 2017, [6], Artikel 8a, Absatz 1, formal ausformuliert:

> Für das Messwesen und die Informationsprozesse sind bei den Endverbrauchern und den Erzeugern intelligente Messsysteme einzusetzen. Diese bestehen aus folgenden Elementen:
>
> a. einem elektronischen Elektrizitätszähler beim Endverbraucher oder Erzeuger, der:
>
> 1. Wirkenergie und Blindenergie erfasst,
> 2. Lastgänge mit einer Periode von fünfzehn Minuten ermittelt und mindestens sechzig Tage speichert,
> 3. über Schnittstellen verfügt, wovon eine zur bidirektionalen Kommunikation mit einem Datenbearbeitungssystem reserviert ist und eine andere für den Endverbraucher oder den Erzeuger, die ihm mindestens ermöglicht, Messwerte im Moment ihrer Erfassung sowie die Lastgänge nach Ziffer 2 abzurufen, und
> 4. Unterbrüche der Stromversorgung erfasst und protokolliert;
>
> b. einem digitalen Kommunikationssystem, das die automatisierte Datenübermittlung zwischen dem Elektrizitätszähler und dem Datenbearbeitungssystem gewährleistet; und
>
> c. einem Datenbearbeitungssystem, mit dem die Daten abgerufen werden.

(3) Die Definitionen werden durch das intelligente Messgerät (Art. 8a, Absatz 1, Buchstabe a), ein Kommunikationssystem (Datenkonzentrator bzw. Gateway) (Art. 8a, Absatz 1, Buchstabe b) und ein Head End System (Art. 8a, Absatz 1, Buchstabe c) abgedeckt.

(4) Im Weiteren müssen für das Gesamtsystem unter Umständen Datensicherheitsrelevante Komponenten zusätzlich berücksichtigt werden:

- Visualisierung
  - lokal am iMG (Art. 8a, Absatz 1, Buchstabe a, 3.) als Schnittstelle
  - entfernt als Visualisierungsplattform
- Managementsystem für Kryptografische Schlüssel etc. als zentraler Sicherheitsanker eines iMS

(5) Entsprechend ergeben sich aus diesen Definitionen verschiedene Prüfgegenstände für eine Datensicherheitsprüfung gemäss Artikel 8b. Hier sind die Vorgaben für eine Datensicherheitsprüfung der im Rahmen eines iMS eingesetzten Elemente (in [2] sowie in diesem Dokument „Hauptkomponenten“ genannt) gefasst:

1 Es dürfen nur intelligente Messsysteme eingesetzt werden, deren Elemente erfolgreich auf die Gewährleistung der Datensicherheit hin geprüft wurden.

2 Die Netzbetreiber und die Hersteller erlassen für diese Prüfung auf der Basis einer Schutzbedarfsanalyse des BFE Richtlinien, die die zu prüfenden Elemente, die Anforderungen an diese und die Art und Weise der Prüfung festlegen.

3 Die Prüfung wird vom Eidgenössischen Institut für Metrologie durchgeführt. Es kann Dritte mit der Erfüllung dieser Aufgabe oder Teilen davon betrauen.

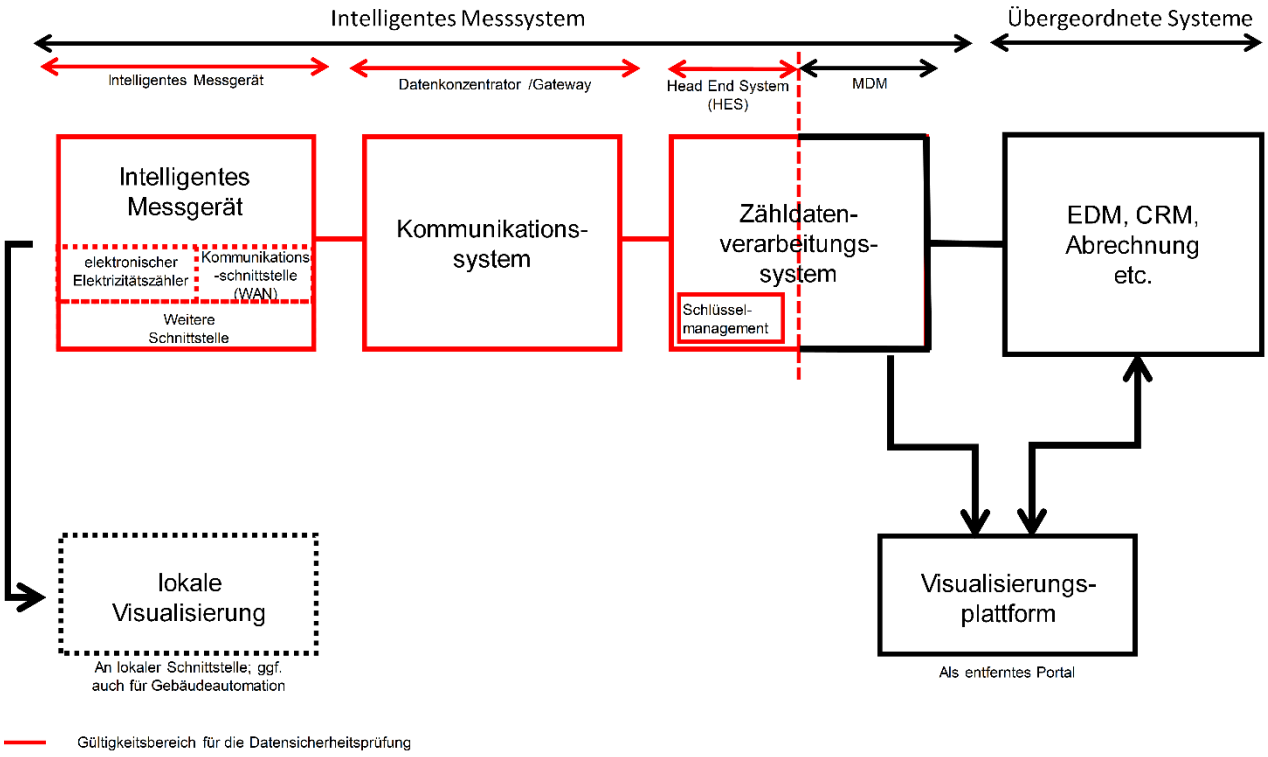

Abbildung 1: Relevante Systeme und Bereiche

(6) Prüfgegenstände der Datensicherheitsprüfung:
Hinsichtlich Architektur und Funktionalität generische Anforderungsprofile:

- Intelligentes Messgerät: iMG
- Kommunikationssystem: Datenkonzentrator oder Gateway
- Head End System

Aufgrund herstellerspezifischer Lösungen nicht generische Anforderungsprofile:

- Schlüsselmanagement
- Visualisierungsplattformen

(7) Für das in der Abbildung 1 dargestellte Gesamtsystem ist zu gewährleisten, dass die Betreiber der Smart Metering Systeme aus Sicht der Datensicherheit nicht nur auf vertrauenswürdige Komponenten zurückgreifen sondern gleichzeitig die Qualifikation besitzen, entsprechende Systeme in ihren IT-Landschaften auf vertrauenswürdige Weise zu betreiben. Dies geschieht üblicher Weise durch den Einsatz entsprechender Informationssicherheitsmanagementsysteme (ISMS) und wird in hohem

Masse durch den Einsatz IT-sicherheitsgeprüfter Systeme unterstützt. Dazu gehören unter anderem folgende Prozesse:

- Verantwortlichkeiten im Management sind definiert und werden gelebt.
- Sicherheitsrichtlinien (Security Policies) sind implementiert und werden gelebt.
- Informationssicherheit und Personalmanagement: Mutationen werden berücksichtigt.
- Wissen und Qualifikation sind auf hinreichendem Niveau und werden durch laufende Fortbildung aktualisiert.
- Hinreichendes Niveau der Datensicherheit ist definiert und implementiert und wird fortlaufend angepasst.
- Zugänge und Zugriffsrechte werden strukturiert und zeitnah verwaltet.

(8) Dies umfasst insbesondere diejenigen Systeme, welche nicht einer speziellen Datensicherheitsprüfung unterworfen sind, sowie die spezifikationskonforme Verwendung geprüfter Komponenten:

- Übergeordnete Systeme des Energiedatenmanagements
- das gesamte Zähldatenverarbeitungssystem (ZDVS), von dem die Prüfgegenstände nur ein Teil ausmachen
- entfernte, z.B. Web-basierte, Visualisierungskomponenten
- Endverbrauchern zur lokalen Anwendung überlassene Visualisierungskomponenten
- Betrieb von iMS

(9) Dazu ist von den entsprechenden Betreibern ein Managementsystem zu implementieren mit:

- Nachweis des sicheren Betriebs der geprüften Hauptkomponenten (iMS)
- Nachweis des sicheren Betriebs des Schlüsselmanagement-Systems
- Nachweis des sicheren Betriebs des ZDVS
- Nachweis sicherer Visualisierung
  - entfernt
  - lokal, NUR FALLS der Betreiber ein Visualisierungsgerät den Endkunden zur Verfügung stellt
- Nachweis des sicheren Betriebs der übergeordneten Systeme

(10) Der Hersteller des ZDVS ist verpflichtet, die Abgrenzung der Prüfgegenstände „Head End System“ sowie „Schlüsselmanagement“ hinreichend zu dokumentieren.

1.1 Prämissen

a) Verwendung der Anhänge des Dokuments «Richtlinien für die Datensicherheit von iMS»

(1) Anhang 1: «Zertifizierungsanforderungen an intelligente Messsysteme für die Datensicherheit» enthält grundsätzlich Anforderungen an die Hauptkomponenten eines iMS und damit mittelbar an die Hersteller derselben. Die Anforderungen werden in Architektur und Funktionalität der Hauptkomponenten umgesetzt, und Korrektheit und Wirksamkeit werden durch eine Datensicherheitsprüfung nachgewiesen.

(2) Anhang 2: «Betriebliche Anforderungen an intelligente Messsysteme für die Datensicherheit» enthält grundsätzlich Anforderungen an die Betreiber der iMS.

b) Hauptkomponenten

(1) Die Funktionalitäten der Hauptkomponenten wirken gegen die Bedrohungen der schutzbedürftigen Objekte aus der Schutzbedarfsanalyse.

(2) Die Hauptkomponenten erfüllen die prozeduralen Anforderungen der Betreiber im Betreiberdokument.

c) Zusätzliche Aspekte

(1) Das Schlüsselmanagement als Subsystem des ZDVS wird ebenfalls auf die Erfüllung der im Herstellerdokument formulierten Anforderungen geprüft.

(2) Der Hersteller eines ZDVS ermöglicht die verschlüsselte Übertragung ohne Rück-Kanal von Kundendaten an eine entfernte Visualisierungsplattform, falls sein Produkt diese Funktion unterstützt.

(3) Die Erfüllung der Anforderungen an Datensicherheit und Datenschutz muss vom Betreiber der entfernten Visualisierungsplattform gewährleistet werden. Falls die entfernte Visualisierungsplattform bidirektionalen Datenverkehr mit einem der „übergeordneten Systeme“ aufweist, muss die Erfüllung der Anforderungen an Datensicherheit und Datenschutz von den Betreibern beider Systeme gewährleistet werden.

(4) Die Erfüllung der Anforderungen an Datensicherheit und Datenschutz muss vom Herausgeber eines Geräts zur lokalen Visualisierung an seine Endkunden gewährleistet werden.

2. Generische Beschreibung der Hauptkomponenten des intelligenten Messsystems

(1) Die folgenden Darstellungen verwenden generische, logische Module, welche zur Lokalisierung der Sicherheitseigenschaften dienen und geben keinerlei konstruktive Vorgaben an die Hersteller.

(2) Enthält eine Hauptkomponente (HK) schutzbedürftige Objekte, sind diese entsprechend abzusichern. Enthält eine HK bestimmte schutzbedürftige Objekte nicht, so kann das entsprechende Modul entfallen.

2.1 Das intelligente Messgerät (iMG)

2.1.1 Das iMG in der Grundkonfiguration als Einzelsystem

(1) Das iMG umfasst mehrere funktional abgrenzbare Teile, die aus Hardware und Software bestehen (Abbildung 2). Aus Sicht der Datensicherheit kann deren Zusammenwirken durch eine modulare Beschreibung bestimmter Funktionen, Kommunikationsbeziehungen, Schnittstellen, Subjekte, Objekte und Rollen abgebildet werden. Daher wird im Folgenden zunächst die Hauptkomponente intelligentes Messgerät näher betrachtet.

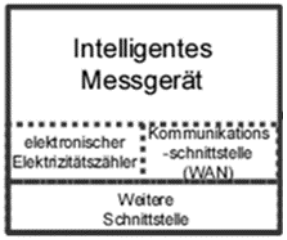

Abbildung 2 Das iMG als Hauptkomponente des iMS

(2) Das iMG ist grundsätzlich aus elektromechanischen und elektronischen Baugruppen zusammengesetzt (Abbildung 3).Es kann eine Breaker-Schaltung enthalten, die den Stromfluss zwischen Stromnetz und Prosumer durch von einem entfernten System aus gesendete Steuerbefehle unterbricht. Ebenso können Relais, die eine dem Rundsteuerempfänger vergleichbare Funktion ausführen, verbaut sein. Offensichtlich enthält das iMG auf jeden Fall einen geeichten Strom- bzw. Energiezähler. Es ergeben sich diesbezüglich externe Schnittstellen (KS0 bis KS3) zur Kommunikation mit Subjekten ausserhalb des iMG sowie interne Schnittstellen zur Kommunikation zwischen den Teilkomponenten. Falls ein Kommunikationsmodul steckbar ist, gelten dieselben Anforderungen an diesen Steckplatz sinngemäss.

(3) Die Firmware des iMG beinhaltet bestimmte logische Module, denen aus Sicht der Datensicherheit bestimmte Funktionalitäten zugeordnet sind:

- externe Schnittstelle: logischer, IT-basierter Zugang zur Firmware von ausserhalb des iMG
  - **KS3**: WAN-Schnittstelle zum Kommunikationsmodul im Head-End oder in einem Datenkonzentrator bzw. Gateway; je nach Gerät Ethernet, PLC, Datenfunk oder Glasfaser etc.
  - **KS0**: Lokale Schnittstelle zur Systemkonfiguration sowie Zählerablesung
  - **KS2**: Schnittstelle, über die ein Prosumer Visualisierungsdaten abrufen kann
- interne Schnittstelle: Verbindung zu im iMG verbauten sonstigen Systemen (dem Zähler sowie ggf. einem Unterbrecher-Relais oder einem Breaker o.ä.)
  - **Zähler:** elektronischer Strom- oder Energiezähler; metrologischer Teil des iMG
  - **Breaker:** Unterbrecher-Relais, das von einem entfernten Operator via iMG ausgelöst wird
  - **Relais** (im Sinne einer Rundsteuerung)

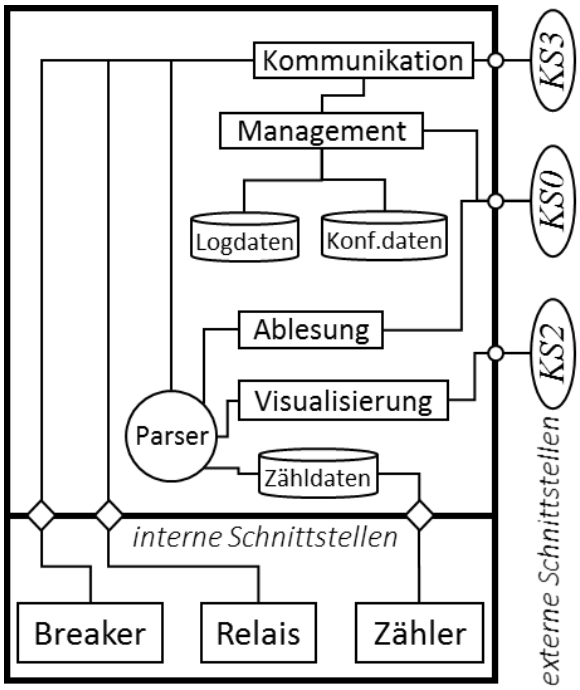

Abbildung 3 Funktionale Basis-Architektur des iMG

- Kommunikation: Modul der Firmware, das die Daten-Verbindung über die WAN-Schnittstelle (KS3) mit dem Head End System steuert.
- Management: Modul der Firmware, das das Gerätemanagement des iMG durch lokalen (via Schnittstelle KS0) oder entfernten Administrator (via Schnittstelle KS3) steuert
  - Konf.daten: elektronischer Speicherort der Konfigurationsdaten
  - Logdaten: elektronischer Speicherort der Logdaten
- Ablesung: Modul der Firmware, das die lokale Zählerablesung vor Ort (via Schnittstelle KS0) steuert
- Visualisierung: Modul der Firmware, das lokal Visualisierungsdaten für den Prosumer (Endkunde ohne oder mit eigener Stromerzeugung) via Schnittstelle KS2 ausgibt (nur lesbar)
- Parser: Modul der Firmware, das die Zähldaten für die Bereitstellung an den entsprechenden Schnittstellen für die jeweiligen Benutzerrollen geeignet aufbereitet
- Zähldaten: elektronischer Speicherort der Zähldaten

2.1.2 Das iMG als Gateway mit LMN

(1) Falls an das iMG weitere Zähler angeschlossen werden sollen und es deren Zähldaten über seine WAN-Schnittstelle KS3 an ein Head End System übertragen soll, muss es eine weitere externe Schnittstelle KS1 zum LMN (Local Metrological Network) erhalten (Abbildung 4).

(2) Es behält grundsätzlich seine Funktionen als intelligentes Messgerät, die sich jedoch auf die Zähldaten des in ihm verbauten Zählers beschränken. Zähldaten anderer, über KS1 angeschlossener Zähler und deren Konfigurationsdaten werden nur an diese weitergeleitet bzw. über die KS3-Schnittstelle an ein Head End übertragen.

(3) Je nach der im LMN verwendeten Übertragungstechnik kann die LMN-Schnittstelle KS1 andere Kommunikationsprotokolle als die WAN-Schnittstelle KS3 unterstützen.
Es ergeben sich folgende zusätzliche Randbedingungen für ein iMG als Gateway:

- Zusätzliche Schnittstelle **KS1** zum LMN
- Zähldaten der Geräte an der **KS1**-Schnittstelle werden durch das Modul Kommunikation nur via **KS3** ohne Daten-Bearbeitung im iMG, jedoch ggf. mit Protokoll-Umwandlung und Umschlüsselung, übertragen.
  - Falls Zähldaten anderer Zähler im iMG für andere Zwecke zwischengespeichert werden, erfolgt eine Speicherplatzverwaltung und -wiederaufbereitung
  - Falls Zähldaten unterschiedlicher Kunden zwischengespeichert werden, erfolgt die Speicherung mandantentauglich (Definition sh. Anhang)
- Die Schnittstelle **KS1** unterstützt Netzwerk-Protokolle geringer Reichweite.
- Falls andere Hauptkomponenten im LMN diese Schnittstelle nutzen, erfolgt die Kommunikation verschlüsselt.

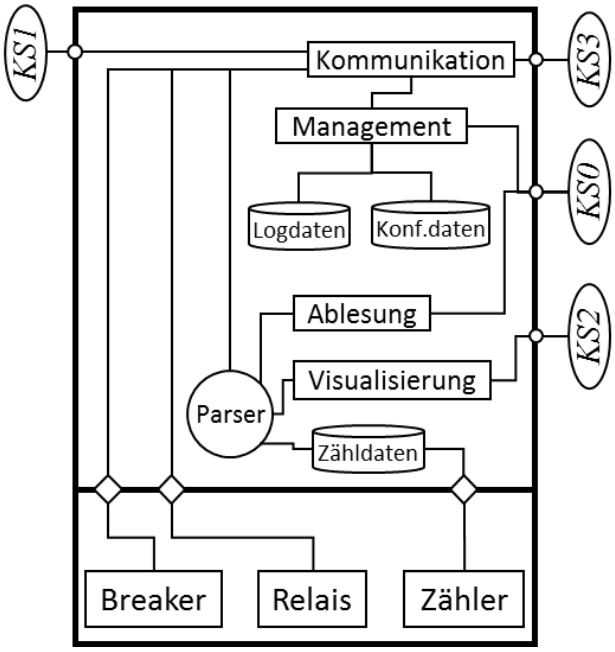

Abbildung 4 Das iMG als Gateway mit eigenem Zähler

- Das Modul Kommunikation separiert den Datenverkehr von und zu den LMN-Zählern von demjenigen bezogen auf seine eigenen Zähldaten, Konfigurationsdaten und Benutzer im iMG.
- Ablesung und Visualisierung ist nur für lokal integrierten Zähler möglich.
  Falls das iMG keinen eigenen Zähler hat, ist eine Reihe interner Module überflüssig, so dass eine vereinfachte Architektur entsteht. Die Anforderungen aus Sicht der Datensicherheit an die verbleibenden Module bleiben bestehen.
  Dem entsprechend kann ein Anforderungsprofil für einen auf dieser Architektur basierenden Datenkonzentrator (DC) bzw. für ein Gateway ohne Zähler abgeleitet werden.

(4) **Anmerkung:**
Für dedizierte Lastschaltgeräte gelten die Anforderungen aus diesem Abschnitt an die Komponenten-Architektur, die implementierten internen Funktionalitäten und die externen Schnittstellen entsprechend.

2.2 Das Kommunikationssystem

(1) Hierzu zählen die Hauptkomponenten Gateway bzw. Datenkonzentrator. Je nach Ausprägung übertragen diese Komponenten entweder lediglich die Zähldaten der angeschlossenen iMG an das HES oder erlauben zusätzlich eine lokale Speicherung zur Weiterbearbeitung. Die Anforderungen in diesem Abschnitt gelten daher nur für die jeweils implementierten Funktionen und entfallen entsprechend für alle nicht implementierten Funktionen.

2.2.1 Das Gateway basierend auf einem iMG ohne eigenen Zähler

(1) Falls ein Gateway (Abbildung 5) ausschliesslich Zähldaten von LMN-Geräten verarbeitet, anzeigt und überträgt, entspricht dessen logische Architektur grundsätzlich derjenigen eines iMG. Jedoch müssen die entsprechenden logischen Module teilweise erweiterte Funktionalitäten aufweisen. Die Module müssen für den Fall, dass Zähldaten verschiedener Kunden in demselben Gateway bearbeitet werden mandantentauglich sein. In der Abbildung ist eine solche Komponente beispielhaft dargestellt. Es ergeben sich folgende zusätzliche Randbedingungen:

- Die Mandantentauglichkeit im Mehrparteienbetrieb ist sichergestellt.
- Das Modul Kommunikation separiert den Datenverkehr von und zu den LMN-Zählern von demjenigen via KS3 gemäss den jeweiligen Verwendungszwecken (z.B. Konfigurationsdaten und Benutzerzugriff).
- Zähldaten werden mandantentauglich (sh. Abschnitt „Abkürzungen und Definitionen“ im Anhang) gespeichert.
- Wenn implementiert, müssen Visualisierung und Ablesung mandantentauglich sein.
- Die Übertragung der Zähldaten ans HES muss mandantentauglich erfolgen.
- Die Funktion des Parsers muss um eine mandantentaugliche Filterfunktionalität erweitert werden.

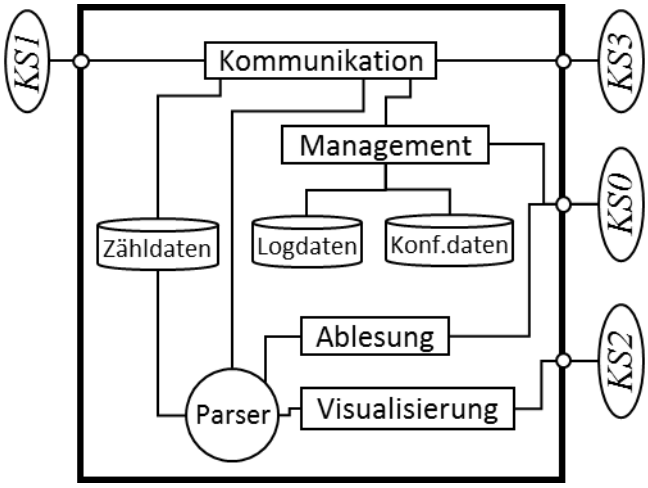

Abbildung 5 Gateway ohne eigenen Zähler

2.2.2 Das Gateway ohne Zähldatenspeicherung

(1) Falls ein Gateway über keine lokale Zähldatenspeicherung verfügt, entfallen die damit verbundenen Module (Abbildung 6). Es kann zu übertragende Zähldaten temporär zwischenspeichern (Temp.daten).

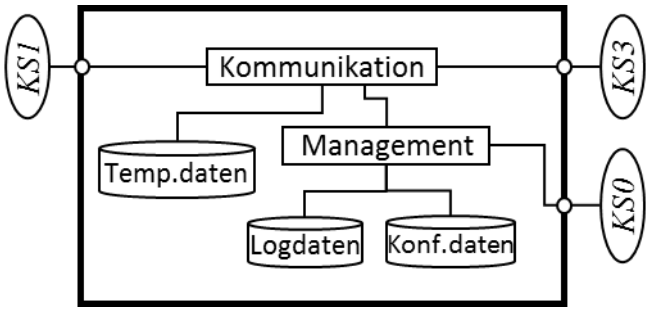

Abbildung 6 Gateway ohne Zähldatenspeicherung

2.2.3 Der Datenkonzentrator (DC)

(1) Der Datenkonzentrator ist als Kommunikationssystem eine Hauptkomponente des iMS (Abbildung 7). Er verbindet iMG und andere Geräte mit dem HES des Datenmanagers. Er muss nicht zwingend baugleich mit oder technisch abgeleitet aus einem iMG sein, jedoch gelten dieselben Anforderungen sinngemäss für die spezifizierten logischen Module.

- Schnittstellen **KS0**, **KS1**, **KS3$_{HK}$** und **KS3$_{HES}$**
- Zähldaten der Geräte an **KS1**-Schnittstelle werden durch das Modul Kommunikation nur via **KS3$_{HES}$** ohne Daten-Bearbeitung im DC, jedoch ggf. mit Protokoll-Umwandlung und Umschlüsselung, ans HES übertragen.
- Die Schnittstelle **KS1** unterstützt Netzwerk-Protokolle geringer Reichweite.
- Die Schnittstelle **KS3$_{HK}$** unterstützt Netzwerk-Protokolle grösserer Reichweite und ist in der Regel mit mehreren iMG (HK=Hauptkomponente) verbunden.
- Zähldaten der iMG an **KS3$_{HK}$**-Schnittstelle werden durch das Modul Kommunikation nur via **KS3$_{HES}$** ohne Daten-Bearbeitung im DC, jedoch ggf. mit Umschlüsselung, übertragen.

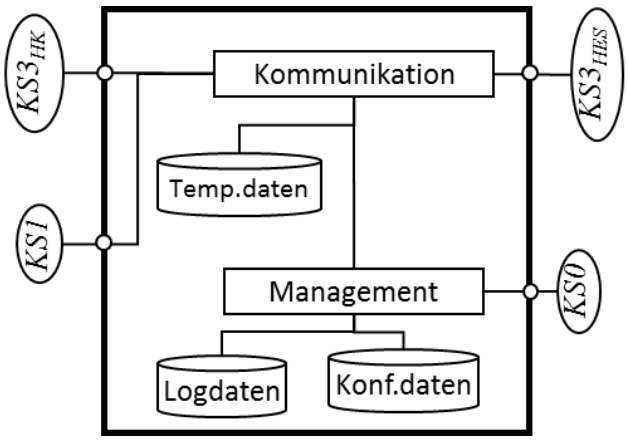

Abbildung 7 Der Datenkonzentrator

- Der DC kann zu übertragende Zähldaten temporär zwischenspeichern (Temp.daten)
- Das Modul Kommunikation separiert den Datenverkehr von und zu den LMN-Zählern bzw. den an **KS3$_{HK}$** angeschlossenen Hauptkomponenten demjenigen via KS3$_{HES}$ gemäss den jeweiligen Verwendungszwecken (z.B. Konfigurationsdaten und Benutzerzugriff).
- Der DC hat keine lokalen Schnittstellen für Ablesung oder Visualisierung, jedoch für lokale Administration (**KS0**).

2.3 Das Head End System (HES)

(1) Diese Komponente ist Teil der Hauptkomponente Zähldatenverarbeitungssystem (Abbildung 8). Sie übermittelt Zähldaten an den Datenmanager und erlaubt Systemadministratoren den Zugriff auf entfernte Hauptkomponenten des iMS. Dafür verfügt das Head End über eine WAN-Schnittstelle sowie über den Rollen seiner Benutzer entsprechende lokale Schnittstellen. Unabhängig von der Ausprägung dieser Schnittstellen (API, I&A-Maske, Webserver o.ä.) erfüllen diese die Sicherheitsanforderungen in geeigneter Weise und integrieren sich in die Prozesse des Informationssicherheitsmanagements des Datenmanagers. Vergleichbar mit der logischen Architektur der Hauptkomponenten umfasst das Head End ebenfalls logisch abgrenzbare Module, die spezifische Funktionen erbringen.

- **WAN**: Schnittstelle zu einem iMG bzw. zu einem DC bzw. Gateway; je nach Gerät Ethernet, PLC, Datenfunk oder Glasfaser
- **Kommunikation**: Modul des HES, das die Datenübertragung von und zu einem iMG bzw. einem DC steuert
- **Management**: Modul des HES, das das Gerätemanagement eines iMG, DC oder Gateway durch einen entfernten Administrator steuert
- **Zähldaten**: Modul des HES, das die vom iMG erhaltenen Messdaten an den Datenmanager weitergibt
- **Sonstiges**: Modul des Head End, das herstellerspezifische Funktionen unterstützt, wie z.B. einen Support-Techniker einer Hauptkomponente, der beim Datenmanager Zugriff auf Hauptkomponenten des iMS hat
- **Lokale Schnittstellen**: funktionsspezifische Schnittstellen des Head End Systems, welche von verschiedenen Rollen oder Systemen beim Datenmanager genutzt werden (Benutzerzugriff, Datentransfer, API etc.)

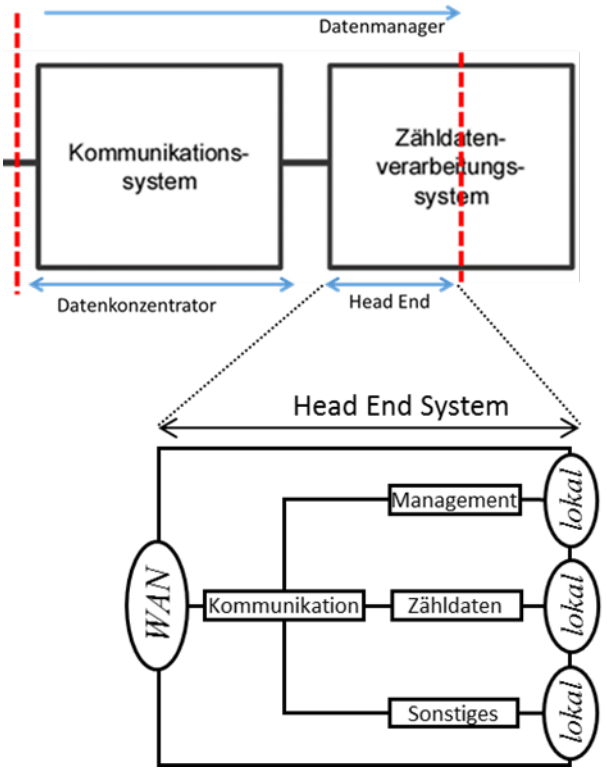

Abbildung 8 Das Head End System in der Domäne des Datenmanagers

2.4 Die Visualisierungsplattform

(1) Diese Hauptkomponente dient der Bereitstellung von Daten über den tatsächlichen Energieverbrauch, die tatsächliche Energieproduktion sowie von Informationen zu Tarifen für Endkunden.

(2) Diese Informationen stehen jedoch nicht zwingend jederzeit an allen Schnittstellen des iMS den berechtigten Prosumern gesamthaft zur Verfügung.

(3) Dem entsprechend muss für diese Hauptkomponente dahin gehend differenziert betrachtet werden, wo sie zum Einsatz kommt und welche Daten sie jeweils dort dem Prosumer und Eigentümer der Daten zugänglich macht.

(4) Die Unterschiedlichkeit in den Datenquellen besteht mindestens in der möglichen zeitlichen Granularität der zur Verfügung stehenden Daten. Am iMG kann der Prosumer theoretisch auf seine momentanen Energiedaten zugreifen, bevor das iMG diese über 15 Minuten aggregiert abspeichert bzw. überträgt. Dies wäre dann aber wiederum die feinste zeitliche Auflösung die die entfernte Visualisierungsplattform anbieten könnte. Ebenso ist es z.B. unrealistisch, dass ein Prosumer an der lokalen Schnittstelle des iMG aktiv mit Tarifinformationen (z.B. HT oder NT (Hoch- bzw. Niedertarif)) arbeiten wird, welche über den jeweils aktuell im iMG angewendeten Tarif hinausgehen.

2.4.1 Visualisierung an lokaler Schnittstelle

(1) Die Zähldaten des iMG werden vom Parser-Modul entsprechend den vorgesehenen Formaten und Filtern aufbereitet und vom Visualisierungs-Modul über die Schnittstelle **KS2** an den Prosumer oder ein anderes berechtigtes Subjekt exportiert. Entscheidend ist die Eigenschaft, dass die Daten nur von berechtigten Subjekten ausgelesen werden können und dass über diese Schnittstelle keine Beeinflussung des iMG erfolgen kann. Weitere technische Eigenschaften liegen im Ermessen des Herstellers.

2.4.2 Visualisierung an entfernter Schnittstelle

(1) An der entfernten Schnittstelle können Verbrauchsdaten und auch deren Visualisierung sowie Tarifinformationen abgerufen werden. Diese Daten stammen aus dem Kundendatenmanagement des Datenmanagers und können von diesem direkt oder über einen weiteren Energiedatendienstleister zur Verfügung gestellt werden. Entscheidend sind hier die Eigenschaften, dass die Daten vertraulich zum authentifizierten Prosumer oder einem anderen berechtigten Subjekt übertragen werden. Unberechtigte Zugriffe über diese Schnittstelle auf das Kundendatenmanagement werden durch das Informationssicherheitsmanagement des Datenmanagers verhindert. Weitere technische Eigenschaften liegen im Ermessen des Datenmanagers.

2.5 Architekturen

2.5.1 Parallel angebundene intelligente Messgeräte

(1) Jedes iMG hat eine WAN-Verbindung zum HES oder zum DC und verwendet **KS3**. Das ist die typische Architektur bei Schmalband PLC Lösungen. Hier kommt der Schutzbedarf der **KS3**, also immer verschlüsselt, zum Tragen.

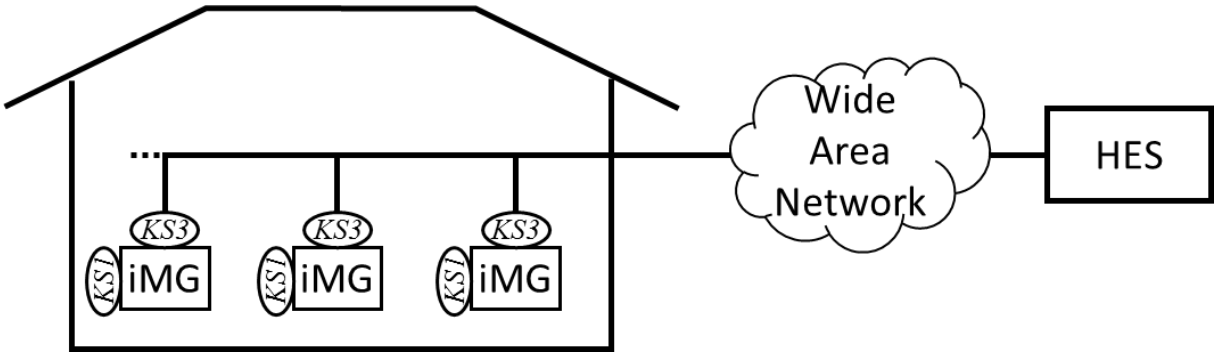

Abbildung 9 Parallel angebundene intelligente Messgeräte

2.5.2 Intelligentes Messgerät mit LMN

(1) Ein iMG funktioniert zusätzlich als Gateway. Es hat eine WAN-Verbindung zum HES oder zum DC und verwendet **KS3**. Weitere iMG sind parallel in seinem LMN über ihre **KS3** an das **KS1** des mit dem WAN verbundenen iMG angebunden. Hier kommt der Schutzbedarf der **KS3**, also immer verschlüsselt, zum Tragen.

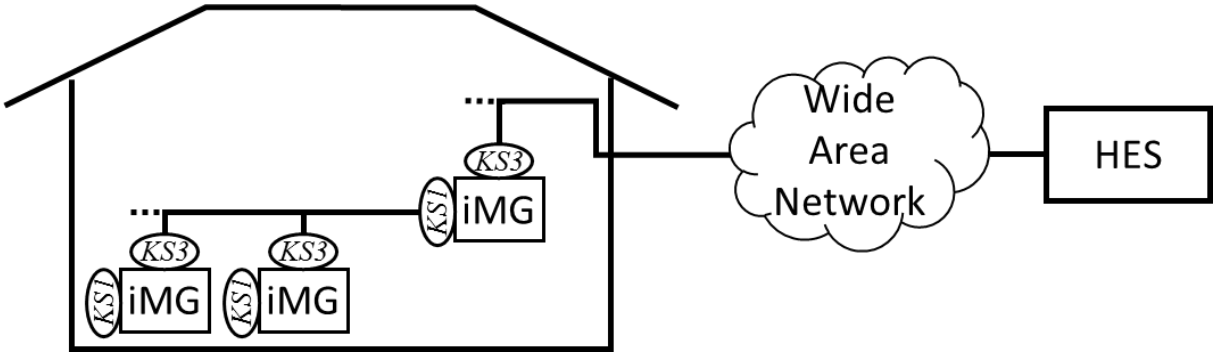

Abbildung 10 Intelligentes Messgerät mit LMN

2.5.3 Intelligentes Messgerät mit kaskadiertem LMN

(1) Ein iMG funktioniert zusätzlich als Gateway. Es hat eine WAN-Verbindung zum HES und verwendet **KS3**. Mindestens ein weiteres iMG ist in seinem LMN über seine **KS3** an das **KS1** des mit dem WAN verbundenen iMG angebunden. Das zweite iMG verfügt über ein eigenes (Sub-)LMN an seiner **KS1** usw. Hier kommt der Schutzbedarf der **KS3**, also immer verschlüsselt, zum Tragen.

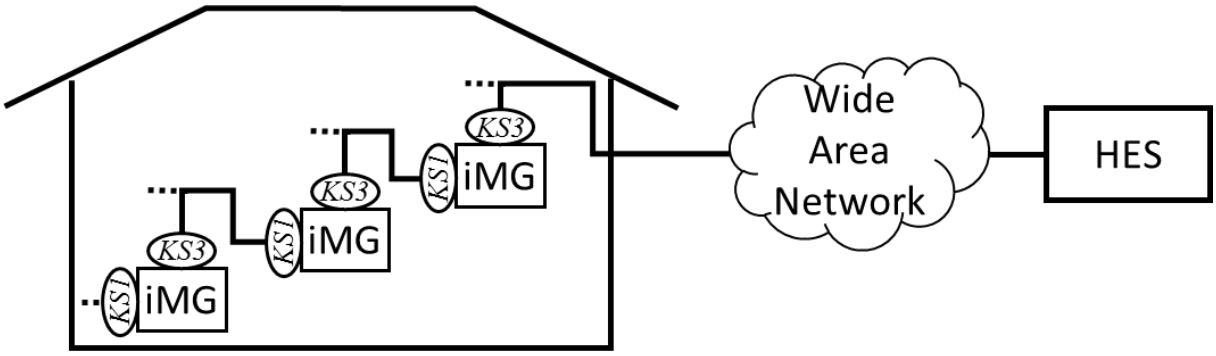

Abbildung 11 Intelligentes Messgerät mit kaskadiertem LMN

2.5.4 Gateway mit LMN

(1) Das Gateway hat eine WAN-Verbindung zum HES und verwendet **KS3**. Die iMG sind parallel in seinem LMN über ihre **KS3** an das **KS1** des mit dem WAN verbundenen iMG angebunden. Hier kommt der Schutzbedarf der **KS3**, also immer verschlüsselt, zum Tragen.

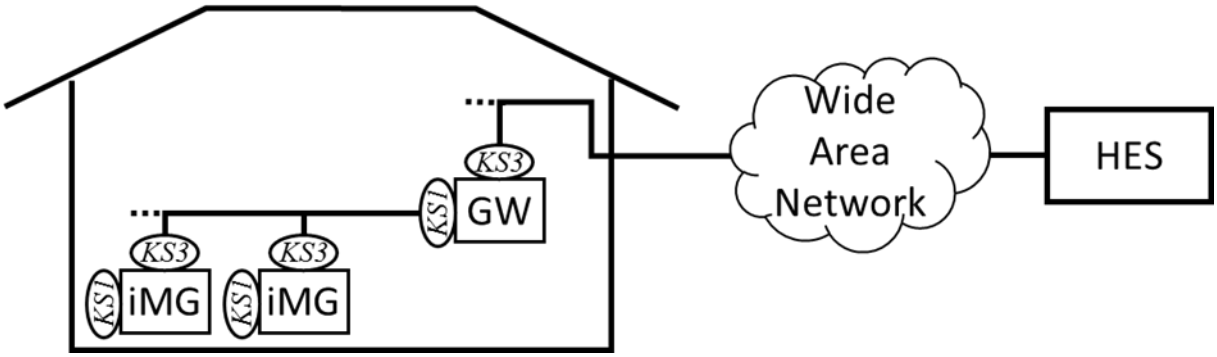

Abbildung 12 Gateway mit LMN

2.5.5 Gateway mit kaskadiertem LMN

(1) Das Gateway hat eine WAN-Verbindung zum HES und verwendet **KS3**. Mindestens ein weiteres iMG ist in seinem LMN über seine **KS3** an das **KS1** des mit dem WAN verbundenen iMG angebunden. Das zweite iMG verfügt über ein eigenes (Sub-)LMN an seiner **KS1** usw. Hier kommt der Schutzbedarf der **KS3**, also immer verschlüsselt, zum Tragen.

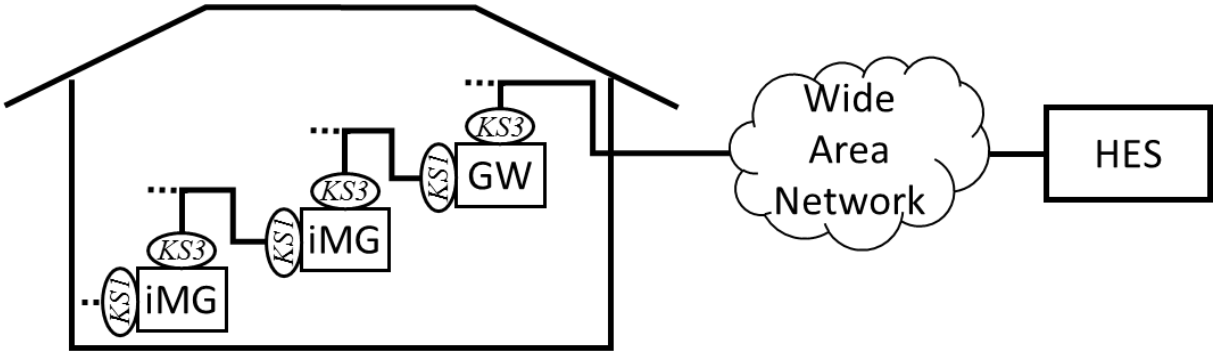

Abbildung 13 Gateway mit kaskadiertem LMN

3. Relevante Schutzobjekte

(1) Die folgenden schützenswerten Objekte ergeben sich aus dem Basisdokument „Mindestanforderungen an das intelligente Messsystem“ [2] sowie aus der Schutzbedarfsanalyse [3]. Die zu erfüllenden Sicherheitsanforderungen sind im Abschnitt 5 spezifiziert.

(2) Die in der Schutzbedarfsanalyse (dort: Abschnitt 4, Tabelle 3) aufgelisteten „untergeordneten Schutzobjekte“ werden in diesem Abschnitt konkretisiert und auf die entsprechenden Hauptkomponenten eines iMS abgebildet.

(3) Der Schutzbedarf ergibt sich jeweils aus der Abwehr unbefugter Zugriffe resultierend in Verlust oder Beeinträchtigung von Integrität, Vertraulichkeit und Verfügbarkeit der Schutzobjekte.

3.1 Intelligentes Messsystem

(1) Ein intelligentes Messsystem besteht mindestens aus intelligenten Messgeräten und einem Head End System.

(2) In der Regel werden jedoch Kommunikationssysteme die Datenübertragung zwischen intelligentem Messgerät und Head End System übernehmen, und das Head End System wird als Sub-System im Zähldatenverarbeitungssystem betrieben. Das Zähldatenverarbeitungssystem beinhaltet daher als Gegenstand dieses Dokuments also die Hauptkomponente „Head End System“ des iMS und das kryptografische Schlüsselmanagement.

(3) Alle Konfigurationen aus den Hauptkomponenten bilden jeweils ein in sich abgeschlossenes System, dessen Funktionen und externe Schnittstellen definiert sind. Ihre Architekturen und Prozesse sind von den Herstellern dokumentiert sowie bezüglich Datensicherheits-Anforderungen spezifiziert und konform zu diesen Anforderungen implementiert.

(4) Aufgrund der Abgeschlossenheit eines solchen Systems wird davon ausgegangen, dass die internen Prozesse konform mit den Anforderungen ablaufen und dass über die externen Schnittstellen nur berechtigte Subjekte gemäss ihren Rollenprofilen Zugriff auf die ihnen zugeordneten Objekte haben können.

(5) Darüber hinaus sind zu schützen:

- die externen Schnittstellen gegen Angriffe hinsichtlich Denial-of-Service, Replay, Buffer Overflow
- die physische Integrität (Manipulationserkennung)
- das verlässliche Aufstarten (z.B. über ein abgesichertes Boot-Verfahren)
- das verlässliche Funktionieren der implementierten Funktionen
- eine verlässliche Selbstdiagnose zur Detektion allfälliger kompromittierender Zugriffe

3.2 Visualisierungsplattform

(1) Die Visualisierungsplattform befindet sich an unterschiedlichen Lokalisierungen mit unterschiedlichen Architekturen und Funktionsumfängen. Sie kann berechtigten Prosumern sowohl lokal am iMG als auch entfernt zur Verfügung stehen. Darüber hinaus ist in der Software-Architektur der Varianten die-

ser Komponente vorgesehen, dass unterschiedliche Datensätze mit verschiedenen Sicherheitsanforderungen bearbeitet werden.

3.2.1 Visualisierung lokal

(1) Die hierfür vom iMG angebotene Schnittstelle authentifiziert berechtigte Subjekte und erlaubt darüber hinaus keine weiteren Eingaben, sondern exportiert die zu visualisierenden Zähldaten als nur-lesbar (read only).

3.2.2 Visualisierung entfernt

(1) Die hierfür vom Datenmanager angebotene Schnittstelle authentifiziert berechtigte Subjekte und erlaubt bidirektionale Kommunikation hinsichtlich Zähldaten als nur-lesbar (read only), CIS-Daten, Tarifierung bzw. anderer, komplexer Kunden-Transaktionen.

3.3 Externe Schnittstellen

3.3.1 Schnittstelle zur lokalen Administration (KS0)

(1) Die Hauptkomponenten iMG und DC können lokal administriert werden.

(2) Wenn ein Administrator eine Hauptkomponente lokal, also mit einer direkten physischen Verbindung, administriert benutzt er die Schnittstelle **KS0**.

(3) Diese Schnittstelle kann exklusiv für diesen Zweck bereit stehen (DC). Sie kann darüber hinaus aber auch eine lokale Zählerablesung unterstützen (iMG bzw. Gateway).

(4) Die Schnittstelle authentifiziert berechtigte Subjekte und erlaubt diesen Zugriffe basierend auf deren Benutzer-Rollen.

(5) Die Kommunikation über diese Schnittstelle erfolgt verschlüsselt.

3.3.2 Schnittstelle KS3 (Wide Area Network)

3.3.2.1 iMG Basis-Konfiguration

(1) Über die Schnittstelle KS3 kommuniziert ein iMG über ein Wide Area Network über die Domänengrenzen hinweg mit dem HES (Abbildung 14). Dies umfasst die Übertragung der Zähldaten (für Energieverbrauch, Netz-Status etc.) an den Datenmanager sowie die Administration des iMG (Konfiguration, Updates etc.) durch berechtigte Operatoren beim Datenmanager. Die Kommunikation erfolgt verschlüsselt.

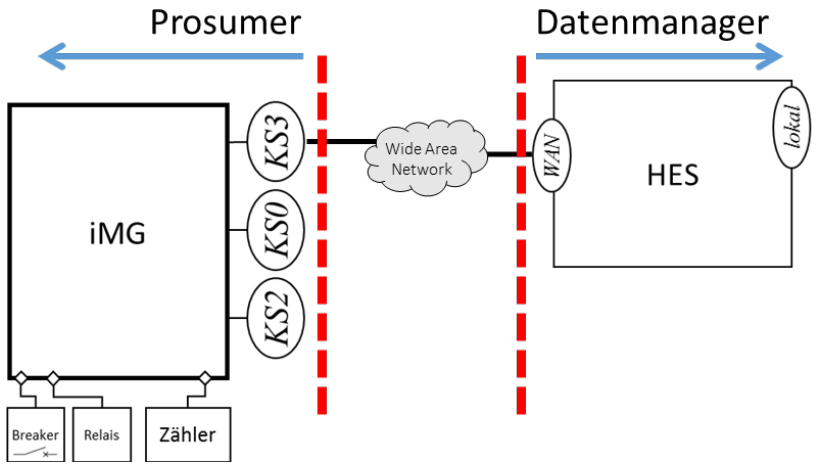

Abbildung 14 Basis-Konfiguration iMG-HES

3.3.2.2 iMG als Gateway

(1) Falls ein iMG mit eigenem Zähler als Gateway eingesetzt wird, werden die Zähldaten der anderen Geräte, die an dessen **KS1** Schnittstelle angebunden sind, sowie diejenigen des Zählers im iMG, entweder direkt oder über einen DC an das HES übertragen (Abbildung 15).

(2) Dieser Fall ist nur zu betrachten, wenn das iMG z.B. die Energiedaten mit dem eingebauten Zähler erfasst und gleichzeitig andere Verbrauchsdaten (Wasser, Wärme, Gas) übermitteln muss. In diesem Fall ist das iMG in der Domäne des Prosumers lokalisiert.

(3) Das iMG als Gateway überträgt seine Zähldaten und Konfigurationsdaten sowie die Zähldaten und die Konfigurationsdaten derjenigen Geräte, die über seine KS1 Schnittstelle angebunden sind, entweder unmittelbar oder über einen DC vom oder an das HES.

(4) Die Schnittstellen der verbundenen Geräte bauen, wenn möglich, mit der KS1 Schnittstelle des iMG abhängig von der Übertragungstechnik und den verwendeten Kommunikationsprotokollen eine verschlüsselte Verbindung auf einer geeigneten Protokollebene auf.

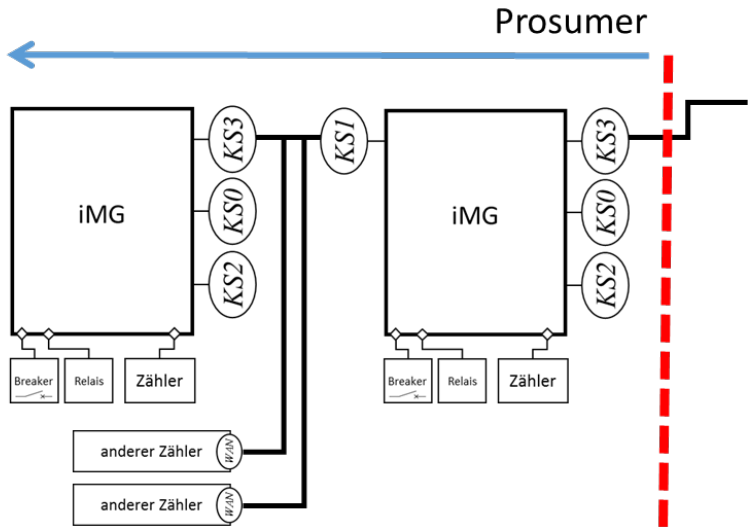

Abbildung 15 Konfiguration des iMG als Gateway

3.3.2.3 Gateway ohne eigenen Zähler

(1) Anstelle eines iMG als Gateway kann dafür ein dediziertes Gateway Gerät benutzt werden. An dieses Gateway können über die **KS1** Schnittstelle verschiedene iMG angeschlossen werden (Abbildung 16).

(2) Je nach Modell kann ein Gateway lokal Zählldaten speichern und weitergeben (vergleichbar mit einem iMG).

(3) Falls keine lokale Bearbeitung der Zählldaten unterstützt wird, entfallen die Anforderungen gem. 3.3.2.2 sowie die Schnittstelle **KS2**.

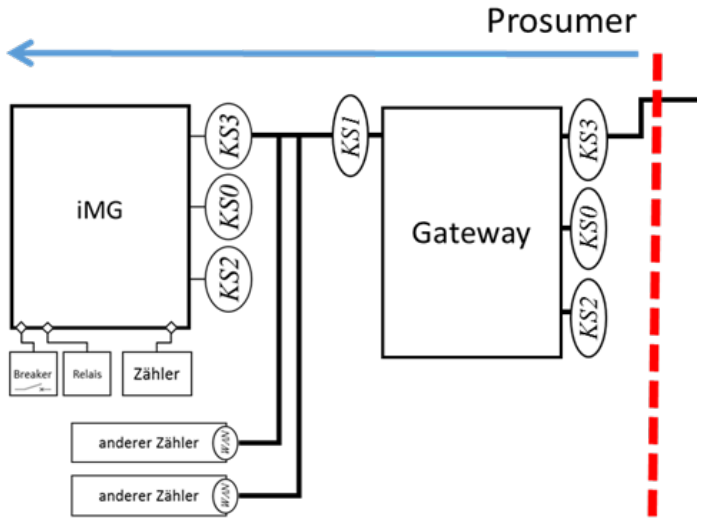

Abbildung 16 Gateway-basierte Architektur in der Prosumer-Umgebung

3.3.2.4 Datenkonzentrator (DC)

(1) Analog gelten die Anforderungen und die Schnittstellen **KS1**, **KS3$_{HK}$** und **KS3$_{HES}$** auch für den DC, der in der Regel nicht in der Domäne des Prosumers lokalisiert ist (in Abbildung 17) bspw. in einer Trafostation), sinngemäss. Die Schnittstelle **KS3$_{HK}$** dient zum Anschluss von iMG über deren **KS3**-Schnittstellen.

(2) Falls ein DC auch über eine **KS1**-Schnittstelle verfügt, so dass am DC auch andere Zähler (keine Hauptkomponenten des iMS) angeschlossen werden können, gelten die Anforderungen an diese Schnittstelle des DC ebenfalls sinngemäss.

(3) Anders als das iMG überträgt der DC jedoch nur die Zähldaten sowie die Konfigurationsdaten anderer Geräte.

(4) Er erlaubt für sich selber eine Administrierung von einem entfernten System aus via seiner **KS3$_{HES}$** Schnittstelle sowie lokal über seine KS0-Schnittstelle.

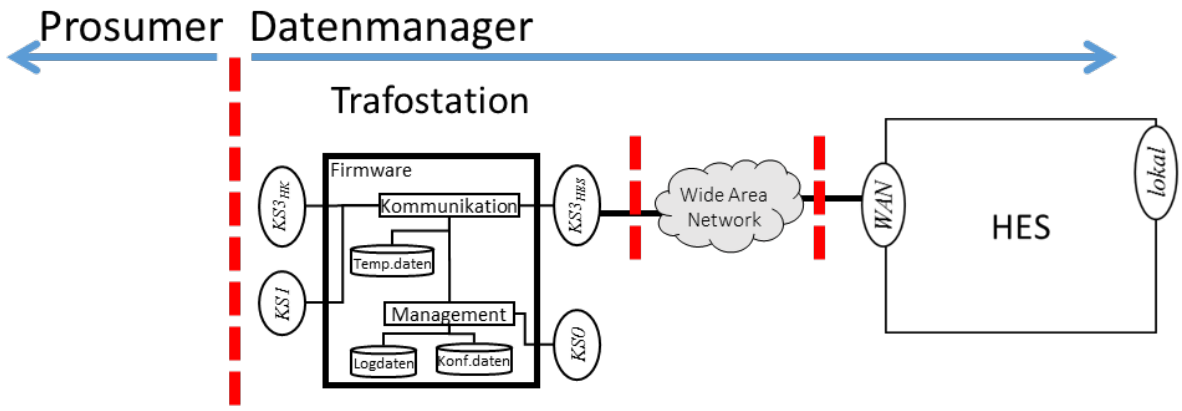

Abbildung 17 Konfiguration des Datenkonzentrators

3.3.3 Schnittstelle KS1 (Local Metrological Network)

(1) Die Schnittstelle dient dem Anschluss weiterer Messgeräte („andere Zähler“, Fremdspartenzähler welche keine Hauptkomponenten des iMS sind) über deren WAN Schnittstellen an eine derjenigen Hauptkomponenten des iMS, die eine Gateway-Funktionalität unterstützen (iMG als Gateway bzw. DC). Sie unterstützt insbesondere Protokolle geringerer Reichweite wie z.B. Powerline Communication (PLC).

(2) Die **KS1**-Schnittstelle erlaubt wenn möglich die Etablierung einer verschlüsselten Verbindung zwischen einem anderen Zähler und der als Gateway agierenden Hauptkomponente und insbesondere keinen Zugriff auf weitere, interne Funktionen des Gateways.

(3) Zähldaten und Konfigurationsdaten der Geräte an der **KS1**-Schnittstelle werden durch das Modul Kommunikation ohne Daten-Bearbeitung, jedoch ggf. mit Protokoll-Umwandlung und Umschlüsselung, übertragen.

(4) Steuerbefehle zum Abruf der Zähldaten aus angeschlossenen Fremdspartenzählern, welche datenschutzkonform implementiert sind (z.B. Tagesverbrauch etc.), sind nur über die Schnittstelle **KS1** an die entsprechenden Zähler übertragbar und können im iMG nicht unbefugt verändert werden.

(5) Steuerbefehle für angeschlossene externe Lastganggeräte sind nur über die Schnittstelle **KS1** übertragbar und können im iMG nicht unbefugt verändert werden. Die Kommunikation erfolgt verschlüsselt.

3.3.4 Schnittstelle KS2 (HAN, Home Area Network)

(1) Ein iMG erlaubt über diese Schnittstelle dem entsprechenden Prosumer oder einem anderen berechtigten Subjekt Zugriff auf eine lokale Visualisierungsplattform.

(2) Die grundsätzlichen Eigenschaften dieser Schnittstelle umfassen die Authentifizierung der Benutzer, an die die Zähldaten übermittelt werden, sowie die Sicherstellung, dass es sich um einen read only Datenexport handelt.

(3) Dem entsprechend ist mindestens eine lokale Anschlussmöglichkeit für ein geeignetes ICT-System (Information and Communication Technology) des Prosumers vorhanden.

3.4 Daten in den Hauptkomponenten

(1) Die grundsätzlichen Bedrohungen durch Verlust von Vertraulichkeit, Integrität und Verfügbarkeit der Daten gelten jeweils in einer spezifischen Form für die entsprechenden Datensätze und können unterschiedliche Auswirkungen haben. Diese reichen von datenschutzrechtlicher Persönlichkeitsverletzung bei Vertraulichkeitsverlust bis hin zu zivil- bzw. strafrechtlichen Konsequenzen bei Verfügbarkeitsverlust, welcher schlimmstenfalls zu einer gefährlichen Betriebssituation führen kann.

(2) In diesem Abschnitt werden die Daten mit Schutzbedarf nach Anwendungsbereichen strukturiert aufgelistet. Die zu erfüllenden Sicherheitsanforderungen sind im Abschnitt 5, Anforderungen an das intelligente Messsystem, spezifiziert.

3.4.1 Konfigurationsdaten

Firmware

(1) Betriebssystem und Anwendungen in allen Hauptkomponenten; unterliegen einer Versionskontrolle; sind bei Auslieferung installiert und gegen unautorisierte Inbetriebnahme gesichert.
Die Integrität dieser Daten ist Voraussetzung für einen ordnungsgemässen und vertrauenswürdigen Betrieb.

Firmware-Update:

(1) Betriebssystem und Anwendungen in den Hauptkomponenten; unterliegen einer Versionskontrolle; werden in den Hauptkomponenten entsprechend der Versionskontrolle durch autorisierte Benutzer in der Rolle Administrator installiert und in Betrieb genommen.
Die Integrität dieser Daten ist Voraussetzung für einen ordnungsgemässen und vertrauenswürdigen Betrieb.

Zählerkonfigurationsdaten

(1) Daten, die den Betrieb und das Verhalten einer Hauptkomponente bestimmen
Die Integrität dieser Daten ist Voraussetzung für einen ordnungsgemässen und vertrauenswürdigen Betrieb. Unbefugte Änderungen bedrohen z.B. die Verfügbarkeit der Energieleistungen beim Prosumer oder die korrekte Tarifierung.

Zählerzeit

(1) Spezielle Konfigurationsdaten
Die Integrität dieser Daten ist Voraussetzung für eine korrekte Zeitangabe in den Zähldaten, ihre Verfügbarkeit ist für eine durchgängige Zeitschreibung sicher zu stellen.

Schalt-Daten

(1) Spezielle Konfigurationsdaten
Falls die Hauptkomponente iMG eine Unterbrecher-Funktion (Breaker) besitzt, die remote ausgelöst werden kann, ist für diejenigen Daten, die den entsprechenden Prozess lokal auslösen, eine Integritätssicherung in Verbindung mit einer Autorisierung implementiert.

(2) Sinngemäss gilt das für Daten, die Steuerbefehle an andere Relais umfassen, welche z.B. im Sinne einer Rundsteuerung arbeiten.

(3) Schalt-Daten für Breaker müssen eineindeutig für eine dedizierte Einheit übertragen werden und erfordern einen autorisierten Operator beim Datenmanager Ein Broadcast zur gleichzeitigen Auslösung mehrerer Breaker ist nicht zulässig.

(4) Schalt-Daten, die Verbrauchergruppen steuern, können per Broadcast und automatisiert übertragen werden.

Kryptographische Schlüssel

(1) Datensätze, die zur Verschlüsselung (Vertraulichkeit) und Absicherung der Integrität von Daten sowie zur Authentifizierung verwendet werden können
Je nach Anwendungsfall sind mindestens der gemeinsame Schlüssel eines symmetrischen Verschlüsselungsverfahrens bzw. der private Schlüssel eines asymmetrischen Verfahrens gegen Verlust der Vertraulichkeit abzusichern. Der Verlust der Integrität des öffentlichen Schlüssels wird durch ein digitales Zertifikat abgewehrt.

(2) Die Kompromittierung eines Schlüssels darf nicht zur Kompromittierung weiterer führen.

(3) Das Schlüsselmanagement legt die Lebensdauer der Schlüssel fest und sorgt für eine zyklische Erneuerung. Ebenso werden Krypto-Algorithmen, Schlüssellängen und sonstige Verfahren (z.B. Hashfunktionen) regelmässig nach Stand der Technik z.B. hinsichtlich Restlaufzeit und nationaler gesetzlicher Vorgaben überprüft und in Firmware Updates termingerecht implementiert.

Kundendaten:

(1) Datensätze, die Informationen enthalten, die Rückschlüsse auf Personen als Kunden des Netzbetreibers zulassen.
Falls Daten dieses Typs in den Hauptkomponenten existieren, sind diese gegen Verlust der Vertraulichkeit zu schützen, um Persönlichkeitsverletzung auszuschliessen.

3.4.2 Netzrelevante Daten

(1) Status-Informationen, die der Verteilnetzbetreiber zur Steuerung seines Versorgungsnetzes verwendet
Diese Daten stellen momentane Informationen zur Verfügung. Zur Sicherung des ordnungsgemässen Betriebs muss daher die Integrität der Daten sichergestellt sein.

3.4.3 Zähldaten

Lastgang, Registerdaten:

(1) Alle Zähldaten, die Verbrauch und Einspeisung in gegebenen Zeitintervallen im iMG entstehen
Das iMG verfügt über einen integrierten Energiezähler, der an der internen Schnittstelle regelmässig Messwerte übermittelt. Diese sind ab der internen Schnittstelle gegen Integritäts- und Vertraulichkeitsverlust abzusichern. Ein Verlust der Verfügbarkeit dieser Werte muss bemerkt werden, und es erfolgen ein Log-Eintrag sowie eine Signalisierung an den Datenmanager. Anhängig von den Benutzern, an die über die externen Schnittstellen dieser Hauptkomponente Zähldaten weitergegeben werden, bereitet das iMG die vom Zähler übernommenen und bearbeiteten Rohdaten weiter auf. Die exportierten Daten sind ebenfalls gegen Integritäts- und Vertraulichkeitsverlust abzusichern.

Marktinformationen:

(1) In einem iMG befindliche, quantifizierbare Informationen im Sinne der Betrachtungen des Use Case 2 in der SBA [3]
Die Integrität der Marktinformationen ist tendenziell als kritisch einzustufen, da in der Masse (grossflächig) mit falschen Werten ein kritischer Netzzustand hervorgerufen werden könnte. Die Verfügbarkeit und Vertraulichkeit der Marktdaten im hier beschriebenen Sinn ist bezüglich der Versorgungssicherheit unkritisch.

3.4.4 Logdaten

(1) Logdaten sind Daten mit Schutzbedarf. Art und Umfang der zu loggenden Daten sind nicht Gegenstand des vorliegenden Dokuments. Sie sind vielmehr durch die technische Umsetzung eines iMS bzw. einer Hauptkomponente davon sowie durch die Betriebsführung des Datenmanagers bestimmt.

(2) Die Hersteller sind gehalten, den Umfang der zu loggenden Daten den Ansprüchen der Betreiber anzupassen.

4. Auflistung der relevanten Bedrohungen

(1) Die SBA [3] basiert auf einer Betrachtung bestimmter Risikoszenarien (RS). Sie umfasst verschiedene Use Cases und bewertet deren jeweiliges Betriebsrisiko aus Sicht der IT-Sicherheit. Dazu werden 14 Risikoszenarien spezifiziert und Schutzobjekte, Schwachstellen und Bedrohungen benannt. Anhand der Grafiken im Anhang der SBA wird deutlich, dass insbesondere die Domänen „Prosumer“ und „Datenmanager“ für die dort dargestellten Use Cases zentrale Bedeutung haben. Im vorliegenden Dokument erfolgt daher eine Fokussierung auf die entsprechenden Hauptkomponenten eines iMS in den o.g. Domänen.

Folgende Bedrohungen ergeben sich aus der Schutzbedarfsanalyse:

- Modifikation der Daten lokal
- Modifikation der Daten von fern
- Modifikation der Zeiten
- Unberechtigter Datenzugriff lokal
- Unberechtigter Datenzugriff von fern
- Unberechtigter Datenzugriff auf im Gerät gespeicherte, nicht mehr bearbeitete Daten
- Einschränkung der Verfügbarkeit der Daten
- Unberechtigtes Schalten des Breakers
- Unberechtigtes Schalten der Relais im Smart Meter
- Unsicheres Aufstarten

(2) Die in der SBA spezifizierten Bedrohungen lassen sich teilweise unmittelbar auf Verlust der Vertraulichkeit, Integrität und Verfügbarkeit abbilden. Die Differenzierung zwischen „lokal“ und „von fern“ hat hierbei nur insofern Bedeutung, als dass diese Bedrohungen jeweils dieselben Objekte betreffen, jedoch entweder aus mangelnder Widerstandsfähigkeit der Geräte bzw. mangelnder Sicherheit bei der Datenübertragung resultieren. Aus Sicht der Hauptkomponenten ist jeweils dieselbe Schutzfunktionalität zu fordern, jedoch für unterschiedliche externe Schnittstellen entsprechend zu implementieren.

(3) Durch eine Differenzierung nach Integrität, Vertraulichkeit und Verfügbarkeit werden die Bedrohungen wie folgt gruppiert:

Verlust der Integrität	
– Modifikation der Daten lokal – Modifikation der Daten von fern – Modifikation der Zeiten	Dies kann erfolgen durch unbefugten, ändernden Zugriff auf die im Gerät gespeicherten Daten oder während der Datenübertragung.

Verlust der Vertraulichkeit	
– Unberechtigter Datenzugriff lokal – Unberechtigter Datenzugriff von fern – Unberechtigter Datenzugriff auf im Gerät gespeicherte, nicht mehr bearbeitete Daten	Dies kann erfolgen durch unbefugten, lesenden Zugriff auf die im Gerät gespeicherten Daten oder während der Datenübertragung. Insbesondere kann ein möglicher Zugriff auf Speicherbereiche, die für die Bearbeitung schutzbedürftiger Daten vorher verwendet worden sind, zum Verlust der Vertraulichkeit derselben führen.

Verlust der Verfügbarkeit	
– Verlust oder Einschränkung der Verfügbarkeit der Daten	Dies kann resultieren aus unbefugtem Zugriff auf die datenbearbeitenden Prozesse, so dass diese daran gehindert werden, die Daten ordnungsgemäss und reproduzierbar abzuspeichern bzw. zu übertragen.
– Unberechtigtes Schalten des Breakers – Unberechtigtes Schalten der Relais im Smart Meter	Das unbefugte Schalten von Breaker bzw. Relais im Smart Meter führt i.d.R. zum Verlust der Verfügbarkeit der elektrischen Energie am Messpunkt. Voraussetzung dafür ist der unbefugte Zugriff auf diejenigen Teile der Firmware, die die Schalter ansteuern. Diese Art der Bedrohung resultiert je nach Implementation aus Verlust der Vertraulichkeit (z.B. Username/Passwort) oder der Integrität (unbefugte Änderung einer Steuervariablen in der SW)
– Unsicheres Aufstarten	Dies ist eine fundamentale Sicherheitslücke, insofern als die Bedrohung das System im Bootprozess angreift, bevor die Sicherheitsfunktionen als Anwendungen überhaupt aktiv sind. Eingriffe können vom Versuch durch An- und Abschalten in ein Bootmenü zu gelangen bis zum Booten eines fremden Betriebssystems reichen.

5. Anforderungen an das intelligente Messsystem

5.1 Übergreifende Anforderungen

5.1.1 Benutzerrollenmodell

(1) Unter Berücksichtigung der verschiedenen Hauptkomponenten sowie des MDM ergeben sich drei grundsätzliche Klassen für Benutzerrollen:

- Administrator:
  Benutzer, der das System installiert, wartet und betreut. Der Administrator hat deshalb u. a. die Berechtigung zur Änderung der Sicherheits- und Systemkonfiguration.
- Operator:
  Benutzer, der das System im Rahmen der vorgesehenen Nutzung bedient. Dies beinhaltet auch das Recht zur Änderung betriebsrelevanter Einstellungen.
- Data-Display:
  Benutzer, der den Status des Systems abrufen und definierte Betriebsdaten lesen darf, aber nicht berechtigt ist, Änderungen durchzuführen.

(2) Um den Erfordernissen einer „granularen Zugriffskontrolle“ und der komplexen Systemlandschaft der unterschiedlichen Hauptkomponenten des iMS zu entsprechen, müssen aber im Sinne des Need-to-know Prinzips (bzw. auch Need-to-use) mehr Benutzertypen mit zwar jeweils derselben Einstufung aber geeignet konfigurierten, unterschiedlichen Zugriffsrechten verwendet werden.

Nicht abschliessende Liste möglicher iMS-Benutzer:

- iMG-Administrator
  kann ein iMG lokal bzw. von Ferne konfigurieren.
- DC-Administrator
  kann einen DC lokal bzw. von Ferne konfigurieren.
- HES-Administrator
  kann ein HES beim Datenmanager konfigurieren.
- Zählerableser
  kann lokal am iMG Zähldaten ablesen sowie die Zählerzeit synchronisieren.
- Operator
  kann die Zähldaten (verbrauchsrelevant bzw. netzrelevant) aus den iMG über das HES von Ferne auslesen.
- Breaker-Manager
  kann einen Breaker von Ferne auslösen.
- Hersteller-Support
  entspricht z.B. einem Techniker des Herstellers, der aus seiner bzw. der Domäne des Datenmanagers heraus auf andere Hauptkomponenten von Ferne zugreift.
- Prosumer lokal
  kann über eine Visualisierungskomponente im iMG Zähldaten nur lesend erfassen.

- Prosumer remote
  kann über eine Visualisierungskomponente Zähldaten vom Datenmanager erhalten und ggf. Einstellungen im CIS des Datenmanagers ändern.

5.1.2 Zugriffskontrolle

a) An denjenigen Schnittstellen der Hauptkomponenten mit Benutzerzugriff, sind bezüglich der schützenswerten Objekte die jeweiligen Zugriffsrechte für alle Rollen definiert.
b) Das anzuwendende Rollenmodell ist vom Hersteller zu definieren.
c) Das Rollenmodell ist durch autorisierte Benutzer erweiterbar.

5.1.3 Identifikation und Authentisierung

a) An den Schnittstellen der Hauptkomponenten mit lokalem Benutzerzugriff ist eine Lösung mit mindestens Benutzername und Passwort implementiert. AM iMG ist ein passwortgeschützer Zugriff auf eine definierte Rolle zulässig.
b) Falls eine Hauptkomponente Telearbeit unterstützt, müssen starke Authentisierungsverfahren (basierend auf „Besitz und Wissen“) implementiert sein. Dies kann bei einem HES sowie für Zugriffe auf eine Hauptkomponente über das HES der Fall sein.
c) Passwörter müssen über verschlüsselte Kanäle ausgetauscht werden.
d) Standard-Passwörter müssen bei Erst-Anmeldung geändert werden.
e) Es muss ein Passwortkomplexitätsprüfung nach Stand der Technik erfolgen.
f) Sollte das Anmeldeverfahren (Log-in) nicht erfolgreich abgeschlossen werden, darf das System keine Auskunft darüber geben, welche Information (Benutzername oder Passwort) nicht korrekt war.
g) Passwörter müssen bei der Eingabe verborgen sein.
h) Passwörter müssen manuell geändert werden können. Der Prozess muss eine Bestätigung dieser Aktion beinhalten. Die Änderung oder ein Versuch einer Änderung führt zu einem Log-Eintrag.
i) Falls Passwörter gespeichert werden, muss dies verschlüsselt erfolgen.

5.1.4 Verschlüsselung

a) Der Datenverkehr zwischen den Hauptkomponenten erfolgt verschlüsselt.
b) Schutzbedürftige Daten dürfen im intelligenten Messsystem nur verschlüsselt gespeichert werden Das System muss die sichere, selektive Löschung bestimmter Daten ermöglichen, beispielsweise durch Überschreiben mit Zufallsdaten.
c) Bei der Auswahl von Verschlüsselungsstandards sind nationale Gesetzgebungen zu berücksichtigen. Es dürfen nur anerkannte Verschlüsselungs-Verfahren und Schlüsselmindestlängen benutzt werden, die nach aktuellem Stand der Technik auch auf absehbare Zeit als sicher gelten. Selbstentwickelte Verschlüsselungs-Algorithmen sind nicht erlaubt. Bei der Implementierung der Verschlüsselungs-Verfahren sollte, wo möglich, auf anerkannte Verschlüsselungs-Bibliotheken zurückgegriffen werden, um Implementierungsfehler zu vermeiden.
d) Die verwendeten Algorithmen müssen angegeben werden.

5.1.5 Lebenszyklus der Hauptkomponenten

(1) Der Lebenszyklus einer Hauptkomponente umfasst mindestens deren Spezifikation, Entwicklung, Auslieferung und Inbetriebnahme sowie ihre sichere Entsorgung. Komponenten, die in Spezifikation

und Entwicklung eine abgeschlossene IT-Sicherheitsfunktionalität aufweisen, können jedoch trotzdem in allen Phasen ihrer Lebenszyklen durch unbefugte Zugriffe kompromittiert werden.

a) Der Hersteller gewährleistet daher in den Phasen, welche von ihm kontrolliert werden, Schutz gegen Verlust oder Beeinträchtigung von Integrität, Vertraulichkeit und Verfügbarkeit seiner Komponenten.
b) Diese Massnahmen sind vom Hersteller dokumentiert und deren Umsetzung kann von den Betreibern seiner Komponenten verifiziert werden.
   Die Betreiber folgen dabei einem prozessualen Ansatz für Erwerb, Entwicklung und Wartung von Systemen mit Vorgaben, die im Betreiberdokument spezifiziert sind. Die Hersteller sind gehalten, den Umfang der zu dokumentierenden Aspekte den Ansprüchen der Betreiber anzupassen.
c) Für den Fall dass sicherheitskritische Schwachstellen während des Betriebs der HK bekannt werden, sind organisatorische Massnahmen zur Bekanntmachung, Dokumentation und Behebung von Fehlern zwischen Herstellern und Betreibern abzustimmen (Flaw Remediation, Schwachstellenbeseitigung).
d) Sicherheit bei der Entwicklung und Unterstützung von Prozessen bzgl. Auslieferung und Inbetriebnahme
e) Falls ein Hersteller Drittprodukte oder Teilkomponenten in seine Produkte integriert, führt er im Sinne von a) Eingangskontrollen durch.

5.2 Anforderungen an das iMG

5.2.1 Anforderungen an den sicheren Betrieb

5.2.1.1 Auslieferung und Erst-Inbetriebnahme

a) Der Hersteller liefert ein iMG grundsätzlich betriebsfertig aus, jedoch in einer geeigneten Konfiguration, so dass eine Erst-Inbetriebnahme mindestens eine Registrierung des Geräts beim Datenmanager erzwingt, bevor das iMG seine vorgesehenen Funktionen freigibt.
b) Die Geräteidentifikation sowie die Versionsnummern der Firmware (ggf. einzelner Komponenten) sind dokumentiert, und das Auslieferungszertifikat und die hierin enthaltenen Daten sind entscheidend.
c) Falls das Gerät bei einer Erst-Inbetriebnahme nicht in diesen Betriebszustand kommt, muss dieses bemerkt werden können, so dass das Gerät zunächst neu konfiguriert werden kann.

5.2.1.2 Sicheres Booten des Gerätes

a) Ein Gerät ist nach der Erst-Inbetriebnahme in der Lage, bei jedem Neustart in den vorgesehenen Betriebsmodus zu kommen. Bootmenüs sind nur für berechtigte Administratoren zugänglich.
b) Booten von externen Datenträgern ist nicht möglich.
c) Stellt das Gerät einen fehlerhaften Wiederanlauf fest, wird eine Fehlermeldung ausgegeben, ggf. ein Alarm an den Datenmanager erzeugt, diese Ereignisse in die Log-Daten übernommen, und das Aufstarten der lokalen Anwendungen im iMG wird verhindert.
d) Das Betriebssystem ist in der Lage, eine Integritätsprüfung an sich selbst durchzuführen. Bei einer fehlerhaften Integritätsprüfung wird eine Fehlermeldung ausgegeben sowie ein Alarm an den Datenmanager erzeugt, diese Ereignisse in die Log-Daten übernommen, und das Aufstarten der Anwendungen im Zähler wird verhindert.

5.2.1.3 Manipulationserkennung

a) Ein Gerät, das im vorgesehenen Betriebsmodus arbeitet, kann erkennen, ob die Integrität des Gehäuses kompromittiert ist. In diesem Fall wird eine Fehlermeldung ausgegeben sowie ein Alarm an den Datenmanager erzeugt.
b) Diese Ereignisse werden in die Log-Daten übernommen.

5.2.1.4 Speicherschutz

a) Das Betriebssystem erlaubt Speicherplatzmanagement, so dass im flüchtigen Speicher des Geräts Adressräume exklusiv für die entsprechenden Anwendungen reserviert sind.
b) Speicherbereiche, in denen Zähldaten bzw. Kryptoschlüssel temporär abgelegt werden, werden nach deren Verwendung durch gezieltes Überschreiben wiederaufbereitet.

5.2.1.5 Logging

a) Alle aus Sicht der Datensicherheit relevanten Systemereignisse werden in die Log-Daten übernommen.
b) Log-Daten dürfen nur durch entsprechend autorisierte Benutzer ausgelesen werden.
c) Log-Daten sind gegen unautorisierte Änderung bzw. Löschung gesichert.
d) Art und Umfang der zu loggenden Daten sind nicht Gegenstand des vorliegenden Dokuments. Sie sind vielmehr durch die technische Umsetzung eines iMS bzw. einer Hauptkomponente davon sowie durch die Betriebsführung des Datenmanagers bestimmt. Im Minimum unterstützt das Logging die in [4] spezifizierten Anforderungen.

   Die Hersteller sind gehalten, den Umfang der zu loggenden Daten den Ansprüchen der Betreiber anzupassen.

5.2.1.6 Firmware Update

a) Nur bei einem Gerät, das im vorgesehenen Betriebsmodus arbeitet, kann ein berechtigter Administrator Updates auslösen.
b) Das Betriebssystem ist in der Lage, eine Integritätsprüfung des Updates durchzuführen (bspw. durch Zwischenspeicherung und Prüfsummentest).
c) Bei einer fehlerhaften Integritätsprüfung werden eine Fehlermeldung ausgegeben, ggf. ein Alarm an den Datenmanager erzeugt, diese Ereignisse in die Log-Daten übernommen und das Update verhindert. Das Betriebssystem ist in einem solchen Fall in der Lage, wieder verlässlich mit der vorhergehenden Softwareversion aufzustarten.
d) Falls eine Authentifizierung der Herkunft eines Updates mithilfe der Informationen und Funktionen gemäss a) und b) nicht möglich ist, ist eine Authentifizierung der Updates mittels einer anderen Funktionalität zu implementieren. Ein erfolgloser Authentifizierungsversuch ist gemäss c) zu verarbeiten.
e) Ein Update des metrologischen Teils des iMG ist nur im Rahmen der Vorgaben der MID (Messgeräterichtlinie 2004/22/EG, engl. Measuring Instruments Directive) und des METAS (Eidgenössisches Institut für Metrologie) zulässig.
f) Der Firmware Update ist nur über die **KS0** und **KS3** möglich.
g) Die Firmware aller Hauptkomponenten muss aktualisiert werden können.

5.2.2 Schnittstellen

5.2.2.1 Schnittstelle KS0

a) Für den Zugriff auf diese Schnittstelle sind mindestens die Benutzerrollen «iMG-Administrator» sowie «Zählerableser», sowie «Operator_lokal» gemäss den entsprechenden Zugriffsrechten verfügbar.
b) Die Authentifizierung erfolgt mindestens über Benutzername und Passwort.
c) Die Schnittstelle erlaubt der Rolle «Zählerableser» einen nur-lesenden Zugriff auf die zur lokalen Ablesung vorgesehenen Zähldaten sowie die Synchronisierung der Zählerzeit.
d) Die Schnittstelle erlaubt der Rolle „Operator_lokal“ einen nur-lesenden Zugriff auf die zur Fernübertragung vorgesehenen Zähldaten und auf die netzrelevanten Daten sowie den lokalen Zugriff auf Breaker und Relais.
e) Für den Zugriff auf die Breaker-Funktion ist eine zweistufige Authentifizierung vorzusehen. Falls dies konstruktiv nicht möglich sein sollte, ist die Funktion grundsätzlich gesperrt und muss für den Zugriff durch den «Operator_lokal» vom HES aus freigeschaltet werden. Die Sperrung wird grundsätzlich nach dem Zugriff des «Operator_lokal» sofort wieder aktiviert.
f) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des iMG möglich.
g) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
h) Eine unbefugte Störung der Schnittstelle hat keinen Einfluss auf den metrologischen Teil oder auf die anderen Schnittstellen.
i) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.2.2.2 Schnittstelle KS3

a) Das iMG verbindet sich über diese Schnittstelle nur mit der entsprechenden WAN-Schnittstelle des HES oder mit der **$KS3_{HK}$**-Schnittstelle des DC und der **KS1** des Gateways.
b) Die Kommunikation erfolgt verschlüsselt auf einer geeigneten Protokollebene. Die verwendeten Algorithmen werden regelmässig auf Stand der Technik geprüft bzw. bei bekannt gewordener Kompromittierung zeitnah ausgetauscht.
c) Für den Zugriff über diese Schnittstelle sind mindestens die Benutzerrollen «iMG-Administrator» sowie «Operator_tele» gemäss den entsprechenden Zugriffsrechten verfügbar.
d) Falls das iMG Telearbeit unterstützt, sollten wo möglich zweistufige Authentisierungsverfahren (basierend auf „Besitz und Wissen“) implementiert sein. Dies kann für Zugriffe auf das iMG über das HES der Fall sein.
e) Die Schnittstelle erlaubt der Rolle «Operator_tele» beim Datenmanager einen nur-lesenden Zugriff auf die zur Fernübertragung vorgesehenen Zähldaten und insbesondere auf die netzrelevanten Daten, sowie den Zugriff auf Breaker und Relais.
f) Für den Zugriff auf die Breaker-Funktion ist eine zweistufige Authentifizierung vorzusehen.
g) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des iMG möglich. Das Modul Kommunikation separiert den Datenverkehr von und zu den über **KS1** bzw. **$KS3_{HK}$** angeschlossenen Geräten.
h) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
i) Eine Störung der Schnittstelle hat keinen Einfluss auf den metrologischen Teil oder auf die anderen Schnittstellen.
j) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.2.2.3 Schnittstelle KS2

a) Für den Zugriff auf diese Schnittstelle ist mindestens die Benutzerrolle Prosumer gemäss den entsprechenden Zugriffsrechten verfügbar.
b) Die Authentifizierung erfolgt mindestens über Benutzername und Passwort.
c) Die Schnittstelle erlaubt der Rolle Prosumer einen nur-lesenden Zugriff auf die zur Visualisierung vorgesehenen Zähldaten.
d) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des iMG möglich.
e) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
f) Eine Störung der Schnittstelle hat keinen Einfluss auf den metrologischen Teil oder auf die anderen Schnittstellen.
g) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an das MDM System aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.2.2.4 Schnittstelle KS1

a) Das iMG verbindet sich über diese Schnittstelle nur mit der entsprechenden WAN-Schnittstelle anderer intelligenter Messgeräte im LMN.
b) Die Kommunikation erfolgt wenn möglich verschlüsselt auf einer geeigneten Protokollebene. Die verwendeten Algorithmen werden regelmässig auf Stand der Technik geprüft bzw. bei bekannt gewordener Kompromittierung zeitnah ausgetauscht.
c) Für den Zugriff auf diese Schnittstelle sind keine Benutzerrollen verfügbar. Der iMG-Administrator konfiguriert die Verbindungen
d) Zähldaten der Geräte an der KS1-Schnittstelle werden durch das Modul Kommunikation nur via **KS3** ohne Daten-Bearbeitung im iMG, jedoch ggf. mit Protokoll-Umwandlung und Umschlüsselung, übertragen.
e) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des iMG möglich.
f) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
g) Eine Störung der Schnittstelle hat keinen Einfluss auf den metrologischen Teil oder auf die anderen Schnittstellen.
h) Unbefugte Zugriffsversuche und andere Störungen, welche die entsprechende Hauptkomponente im Rahmen der an der Schnittstelle verwendeten Protokolle detektieren kann, lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.2.3 Spezifische Anforderungen

5.2.3.1 Verwendung der Verschlüsselung

a) Jedes Gerät erhält einen individuellen Auslieferungsschlüssel. Dieser wird bei der Erst-Inbetriebnahme nach erfolgreicher Registrierung durch einen neuen Schlüssel ersetzt.
b) Beim Wechsel eines iMG (z.B. Ausbau für die Eichung) kann der Auslieferungsschlüssel wieder aktiviert werden.
c) Die Verschlüsselung ist mit einer zum Zeitpunkt der Auslieferung als sicher geltenden Technologie realisiert.
d) Die Verschlüsselungstechnologie ist update-fähig.
e) Die Kryptoschlüssel werden in allen Geräten und Systemen gegen unbefugten Zugriff geschützt.

5.2.3.2 Zeiteinstellungen

a) Für den Zugriff auf dieses Objekt über die Schnittstelle KS0 werden die Benutzerrollen iMG-Administrator und Zählerableser gemäss den entsprechenden Zugriffsrechten verwendet.
b) Die Authentifizierung erfolgt mindestens über Benutzername und Passwort.
c) Die Änderung der Zeiteinstellung im iMG löst eine Meldung an den Datenmanager aus und wird in die Log-Daten übernommen.
d) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an das MDM System aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.2.3.3 Breaker

a) Der Breaker im iMG kann nur von einem berechtigten Benutzer am HES, am GW, am iMG via KS0 oder durch Regeln, die im iMG hinterlegt sind, ausgelöst werden. Für das Zurücksetzen eines ausgelösten Breakers muss dieser entsprechend freigeschaltet werden.
b) Eine Breaker-Funktion muss für jeden Breaker einzeln ausgelöst werden.
c) Ein Steuerbefehl, welcher mehrere Breaker gleichzeitig anspricht, ist ausgeschlossen.
d) Der Breaker muss nach dem Freischaltbefehl lokal am Gerät selber wieder eingeschaltet werden.

5.2.3.3.1 Steuer-Relais

a) Ein Steuer-Relais kann nur von einem berechtigten Benutzer am HES, am GW, am iMG via KS0 oder durch Regeln, die im iMG hinterlegt sind, ausgelöst werden.
b) Mehrere Steuer-Relais können mittels eines Broadcast angesteuert werden.

5.3 Anforderungen an das Gateway als Kommunikationssystem

5.3.1 Anforderungen an den sicheren Betrieb

5.3.1.1 Auslieferung und Erst-Inbetriebnahme

a) Der Hersteller liefert ein Gateway grundsätzlich betriebsfertig aus, jedoch in einer geeigneten Konfiguration, so dass eine Erst-Inbetriebnahme mindestens eine Registrierung des Geräts beim Datenmanager erzwingt, bevor das Gateway seine vorgesehenen Funktionen freigibt.
b) Die Geräteidentifikation sowie die Versionsnummern der Firmware (ggf. einzelner Komponenten) sind dokumentiert, und das individuelle Auslieferungszertifikat und die hierin enthaltenen Daten sind entscheidend.
c) Falls das Gerät bei einer Erst-Inbetriebnahme nicht in diesen Betriebszustand kommt, muss dieses bemerkt werden können, so dass das Gerät zunächst neu konfiguriert werden kann.

5.3.1.2 Sicheres Booten des Gerätes

a) Ein Gerät ist nach der Erst-Inbetriebnahme in der Lage, bei jedem Neustart in den vorgesehenen Betriebsmodus zu kommen. Bootmenüs sind nur für berechtigte Administratoren zugänglich.
b) Booten von externen Datenträgern ist nicht möglich.
c) Stellt das Gerät einen fehlerhaften Wiederanlauf fest, wird eine Fehlermeldung ausgegeben, ggf. ein Alarm an den Datenmanager erzeugt, diese Ereignisse in die Log-Daten übernommen, und das Aufstarten der lokalen Anwendungen im Gateway wird verhindert.

d) Das Betriebssystem ist in der Lage, eine Integritätsprüfung an sich selbst durchzuführen. Bei einer fehlerhaften Integritätsprüfung wird eine Fehlermeldung ausgegeben sowie ein Alarm an den Datenmanager erzeugt, diese Ereignisse in die Log-Daten übernommen, und das Aufstarten der Anwendungen im Zähler wird verhindert.

5.3.1.3 Manipulationserkennung

a) Ein Gerät, das im vorgesehenen Betriebsmodus arbeitet, kann erkennen, ob die Integrität des Gehäuses kompromittiert ist. In diesem Fall wird eine Fehlermeldung ausgegeben sowie ein Alarm an den Datenmanager erzeugt.
b) Diese Ereignisse werden in die Log-Daten übernommen.

5.3.1.4 Speicherschutz

a) Das Betriebssystem erlaubt Speicherplatzmanagement, so dass im flüchtigen Speicher des Geräts Adressräume exklusiv für die entsprechenden Anwendungen reserviert sind.
b) Speicherbereiche, in denen Zähldaten bzw. Kryptoschlüssel temporär abgelegt werden, werden nach deren Verwendung durch gezieltes Überschreiben wiederaufbereitet.

5.3.1.5 Logging

a) Alle aus Sicht der Datensicherheit relevanten Systemereignisse werden in die Log-Daten übernommen.
b) Log-Daten dürfen nur durch entsprechend autorisierte Benutzer ausgelesen werden.
c) Log-Daten sind gegen unautorisierte Änderung bzw. Löschung gesichert.
d) Art und Umfang der zu loggenden Daten sind nicht Gegenstand des vorliegenden Dokuments. Sie sind vielmehr durch die technische Umsetzung eines iMS bzw. einer Hauptkomponente davon sowie durch die Betriebsführung des Datenmanagers bestimmt. Im Minimum unterstützt das Logging die in [4] spezifizierten Anforderungen.

5.3.1.6 Firmware Update

a) Nur bei einem Gerät, das im vorgesehenen Betriebsmodus arbeitet, kann ein berechtigter Administrator Updates auslösen.
b) Das Betriebssystem ist in der Lage, eine Integritätsprüfung des Updates durchzuführen (bspw. durch Zwischenspeicherung und Prüfsummentest).
c) Bei einer fehlerhaften Integritätsprüfung wird eine Fehlermeldung ausgegeben, ggf. ein Alarm an den Datenmanager erzeugt, diese Ereignisse in die Log-Daten übernommen und das Update verhindert. Das Betriebssystem ist in einem solchen Fall in der Lage, wieder verlässlich mit der vorhergehenden Softwareversion aufzustarten.
d) Falls eine Authentifizierung der Herkunft eines Updates mithilfe der Informationen und Funktionen gemäss a) und b) nicht möglich ist, ist eine Authentifizierung der Updates mittels einer anderen Funktionalität zu implementieren. Ein erfolgloser Authentifizierungsversuch ist gemäss c) zu verarbeiten.
e) Die Firmware aller Hauptkomponenten muss aktualisiert werden können.

5.3.2 Schnittstellen

5.3.2.1 **Schnittstelle KS0**

a) Für den Zugriff auf diese Schnittstelle sind mindestens die Benutzerrollen «Gateway-Administrator» sowie «Zählerableser» sowie «Operator_lokal» gemäss den entsprechenden Zugriffsrechten verfügbar.
b) Die Authentifizierung erfolgt mindestens über Benutzername und Passwort.
c) Die Schnittstelle erlaubt der Rolle «Zählerableser» einen nur-lesenden Zugriff auf die zur lokalen Ablesung vorgesehenen Zähldaten sowie die Synchronisierung der Gatewayzeit.
d) Die Schnittstelle erlaubt der Rolle «Operator_lokal» einen nur-lesenden Zugriff auf die zur Fern-über-tragung vorgesehenen Zähldaten und auf die netzrelevanten Daten sowie den Zugriff auf Breaker und Relais in den angeschlossenen iMG
e) Für den Zugriff auf die Breaker-Funktion ist eine zweistufige Authentifizierung vorzusehen. Falls dies konstruktiv nicht möglich sein sollte, ist die Funktion grundsätzlich gesperrt und muss für den Zugriff durch den «Operator_lokal» vom HES aus freigeschaltet werden. Die Sperrung wird grundsätzlich nach dem Zugriff des «Operator_lokal» sofort wieder aktiviert.
f) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des Gateway möglich.
g) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
h) Eine unbefugte Störung der Schnittstelle hat keinen Einfluss auf die anderen Schnittstellen.
i) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.3.2.2 Schnittstelle KS3

a) Der Gateway verbindet sich über diese Schnittstelle nur mit der entsprechenden WAN-Schnittstelle des HES.
b) Die Kommunikation erfolgt verschlüsselt auf einer geeigneten Protokollebene. Die verwendeten Algorithmen werden regelmässig auf Stand der Technik geprüft bzw. bei bekannt gewordener Kompromittierung zeitnah ausgetauscht.
c) Für den Zugriff über diese Schnittstelle sind mindestens die Benutzerrollen «Gateway-Administrator» sowie «Operator_tele» gemäss den entsprechenden Zugriffsrechten verfügbar.
d) Falls das Gateway Telearbeit unterstützt, sollten wo möglich zweistufige Authentisierungsverfahren (basierend auf „Besitz und Wissen“) implementiert sein. Dies kann für Zugriffe auf das Gateway über das HES der Fall sein.
e) Telearbeit z.B. für Wartungszwecke der Hersteller mit „trivialen“ Authentisierungsverfahren ist nicht zulässig.
f) Die Schnittstelle erlaubt der Rolle «Operator_tele» beim Datenmanager einen nur-lesenden Zugriff auf die zur Fernübertragung vorgesehenen Zähldaten sowie den Zugriff auf Breaker und Relais in den angeschlossenen iMG.
g) Für den Zugriff auf die Breaker-Funktion ist eine zweistufige Authentifizierung vorzusehen.
h) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des Gateway möglich. Das Modul Kommunikation separiert den Datenverkehr von und zu den über **KS1** bzw. **KS3** angeschlossenen Geräten.
i) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
j) Eine Störung der Schnittstelle hat keinen Einfluss auf die anderen Schnittstellen.
k) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.3.2.3 Schnittstelle KS2

a) Für den Zugriff auf diese Schnittstelle ist mindestens die Benutzerrolle Prosumer gemäss den entsprechenden Zugriffsrechten verfügbar.
b) Falls das Gateway Zähldaten verschiedener Kunden bearbeitet, muss seine Datenhaltung mandantentauglich sein und darf verschiedenen Kunden in der Benutzerrolle „Prosumer lokal“ ausschliesslich Zugriff auf ihre entsprechenden Daten erlauben.
c) Die Authentifizierung erfolgt mindestens über Benutzername und Passwort.
d) Die Schnittstelle erlaubt der Rolle Prosumer einen nur-lesenden Zugriff auf die zur Visualisierung vorgesehenen Zähldaten.
e) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des Gateway möglich.
f) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
g) Eine Störung der Schnittstelle hat keinen Einfluss auf die anderen Schnittstellen.
h) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an das MDM System aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.3.2.4 Schnittstelle KS1

a) Der Gateway verbindet sich über diese Schnittstelle nur mit der entsprechenden WAN-Schnittstelle anderer intelligenter Messgeräte.
b) Die Kommunikation erfolgt wenn möglich verschlüsselt auf einer geeigneten Protokollebene. Die verwendeten Algorithmen werden regelmässig auf Stand der Technik geprüft bzw. bei bekannt gewordener Kompromittierung zeitnah ausgetauscht.
c) Für den Zugriff auf diese Schnittstelle sind keine Benutzerrollen verfügbar. Der Gateway-Administrator konfiguriert die Verbindungen
d) Zähldaten der Geräte an der **KS1**-Schnittstelle werden durch das Modul Kommunikation nur via **KS3** ohne Daten-Bearbeitung im Gateway, jedoch ggf. mit Protokoll-Umwandlung und Umschlüsselung bzw. mit Zwischenspeicherung, übertragen.
e) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des Gateway möglich.
f) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
g) Eine Störung der Schnittstelle hat keinen Einfluss auf die anderen Schnittstellen.
h) Unbefugte Zugriffsversuche und andere Störungen, welche die entsprechende Hauptkomponente im Rahmen der an der Schnittstelle verwendeten Protokolle detektieren kann, lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.3.3 Spezifische Anforderungen

5.3.3.1 Verwendung der Verschlüsselung

a) Jedes Gerät erhält einen individuellen Auslieferungsschlüssel. Dieser wird bei der Erst-Inbetriebnahme nach erfolgreicher Registrierung durch einen neuen Schlüssel ersetzt.
b) Beim Wechsel eines Gateway kann der Auslieferungsschlüssel wieder aktiviert werden.
c) Die Verschlüsselung ist mit einer zum Zeitpunkt der Auslieferung als sicher geltenden Technologie realisiert.
d) Die Verschlüsselungstechnologie ist update-fähig.
e) Die Kryptoschlüssel werden in allen Geräten und Systemen gegen unbefugten Zugriff geschützt.
f) Es benötigt eine Schnittstelle zum PKI System, falls dieses nicht eine integrierte Lösung ist.

5.3.3.2 Zeiteinstellungen

a) Für den Zugriff auf dieses Objekt über die Schnittstelle **KS0** werden die Benutzerrollen Gateway-Administrator oder – falls vorhanden – Zählerableser gemäss den entsprechenden Zugriffsrechten verwendet.
b) Die Authentifizierung erfolgt mindestens über Benutzername und Passwort.
c) Die Änderung der Zeiteinstellung im Gateway löst eine Meldung an den Datenmanager aus und wird in die Log-Daten übernommen.
d) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an das MDM System aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.4 Anforderungen an den Datenkonzentrator als Kommunikationssystem

5.4.1 Anforderungen an den sicheren Betrieb

5.4.1.1 Auslieferung und Erst-Inbetriebnahme

a) Der Hersteller liefert einen DC grundsätzlich betriebsfertig aus, jedoch in einer geeigneten Konfiguration, so dass eine Erst-Inbetriebnahme mindestens eine Registrierung des Geräts beim Datenmanager erzwingt, bevor der DC seine vorgesehenen Funktionen freigibt.
b) Die Geräteidentifikation sowie die Versionsnummern der Firmware (ggf. einzelner Komponenten) sind dokumentiert, und falls ein Auslieferungszertifikat verwendet wird, sind die hierin enthaltenen Daten entscheidend.
c) Falls das Gerät bei einer Erst-Inbetriebnahme nicht in diesen Betriebszustand kommt, muss dieses bemerkt werden können, so dass das Gerät zunächst neu konfiguriert werden kann.

5.4.1.2 Sicheres Booten

a) Ein Gerät ist nach der Erst-Inbetriebnahme in der Lage, bei jedem Neustart in den vorgesehenen Betriebsmodus zu kommen. Bootmenüs sind nur für berechtigte Administratoren zugänglich.
b) Booten von externen Datenträgern ist nicht möglich.
c) Stellt das Gerät einen fehlerhaften Wiederanlauf fest, wird eine Fehlermeldung ausgegeben, ggf. ein Alarm an den Datenmanager erzeugt, diese Ereignisse in die Log-Daten übernommen, und das Aufstarten der lokalen Anwendungen im DC wird verhindert.
d) Das Betriebssystem ist in der Lage, eine Integritätsprüfung an sich selbst durchzuführen. Bei einer fehlerhaften Integritätsprüfung wird eine Fehlermeldung ausgegeben sowie ein Alarm an den Datenmanager erzeugt, diese Ereignisse in die Log-Daten übernommen, und das Aufstarten der Anwendungen im Zähler wird verhindert.

5.4.1.3 Sicherer Start der MDM-Anwendungen

a) Die MDM-Anwendungen sind nach der Erst-Inbetriebnahme in der Lage, bei jedem Neustart in den vorgesehenen, durch Konfigurationseinstellungen definierten Betriebsmodus zu kommen.
b) Stellt die Anwendung einen fehlerhaften Wiederanlauf fest, wird eine Fehlermeldung ausgegeben, ggf. ein Alarm an den Datenmanager erzeugt, und diese Ereignisse werden in die Log-Daten übernommen.
c) Die MDM-Anwendung ist in der Lage, eine Integritätsprüfung an sich selbst durchzuführen. Bei einer fehlerhaften Integritätsprüfung wird eine Fehlermeldung ausgegeben, ggf. ein Alarm an den Datenmanager erzeugt, und diese Ereignisse werden in die Log-Daten übernommen.

5.4.1.4 Manipulationserkennung

a) Ein Gerät, das im vorgesehenen Betriebsmodus arbeitet, kann erkennen, ob die Integrität des Gehäuses kompromittiert ist. In diesem Fall wird eine Fehlermeldung ausgegeben sowie ein Alarm an den Datenmanager erzeugt.
b) Diese Ereignisse werden in die Log-Daten übernommen.

5.4.1.5 Speicherschutz

a) Das Betriebssystem erlaubt Speicherplatzmanagement, so dass im flüchtigen Speicher des Geräts Adressräume exklusiv für die entsprechenden Anwendungen reserviert sind.
b) Speicherbereiche, in denen Zähldaten bzw. Kryptoschlüssel temporär abgelegt werden, werden nach deren Verwendung durch gezieltes Überschreiben wiederaufbereitet.

5.4.1.6 Logging

a) Alle aus Sicht der Datensicherheit relevanten Systemereignisse werden in die Log-Daten übernommen.
b) Log-Daten dürfen nur durch entsprechend autorisierte Benutzer ausgelesen werden.
c) Log-Daten sind gegen unautorisierte Änderung bzw. Löschung gesichert.
d) Art und Umfang der zu loggenden Daten sind nicht Gegenstand des vorliegenden Dokuments. Sie sind vielmehr durch die technische Umsetzung eines iMS bzw. einer Hauptkomponente davon sowie durch die Betriebsführung des Datenmanagers bestimmt. Im Minimum unterstützt das Logging die in [4] spezifizierten Anforderungen.

   Die Hersteller sind gehalten, den Umfang der zu loggenden Daten den Ansprüchen der Betreiber anzupassen.

5.4.1.7 Firmware Update

a) Nur bei einem Gerät, das im vorgesehenen Betriebsmodus arbeitet, kann ein berechtigter Administrator Updates auslösen.
b) Das Betriebssystem ist in der Lage, eine Integritätsprüfung des Updates durchzuführen (bspw. durch Zwischenspeicherung und Prüfsummentest).
c) Bei einer fehlerhaften Integritätsprüfung werden eine Fehlermeldung ausgegeben, ggf. ein Alarm an den Datenmanager erzeugt, diese Ereignisse in die Log-Daten übernommen und das Update verhindert. Das Betriebssystem ist in einem solchen Fall in der Lage, wieder verlässlich mit der vorhergehenden Softwareversion aufzustarten.
d) Falls eine Authentifizierung der Herkunft eines Updates mithilfe der Informationen und Funktionen gemäss a) und b) nicht möglich ist, ist eine Authentifizierung der Updates mittels einer anderen Funktionalität zu implementieren. Ein erfolgloser Authentifizierungsversuch ist gemäss c) zu verarbeiten.
e) Die Firmware aller Hauptkomponenten muss aktualisiert werden können.

5.4.2 Schnittstellen

a) Beim DC entfallen die Anforderungen des iMG hinsichtlich

- der lokalen Zählerablesung an der Schnittstelle **KS0** und
- der Visualisierungsschnittstelle **KS2**.

b) Grundsätzlich ist das Einsatzszenario des DC die Zusammenfassung der Datenkommunikation mehrerer iMG zum entsprechenden Datenmanager. Zu diesem Zweck werden die Schnittstellen **$KS3_{HK}$** und **$KS3_{HES}$** verwendet. Falls der DC in einer Konfiguration verwendet wird, die es erlaubt auch andere Zähler in einem LMN anzubinden, wird dafür die Schnittstelle **KS1** verwendet.

5.4.2.1 Schnittstelle KS0

a) Für den Zugriff auf diese Schnittstelle ist die Benutzerrolle DC-Administrator gemäss den entsprechenden Zugriffsrechten verfügbar.
b) Die Authentifizierung erfolgt mindestens über Benutzername und Passwort.
c) Die Schnittstelle erlaubt der Rolle Zählerableser einen nur-lesenden Zugriff auf die zur lokalen Ablesung vorgesehenen Zähldaten sowie die Synchronisierung der Zählerzeit.
d) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des DC möglich.
e) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
f) Eine unbefugte Störung der Schnittstelle hat keinen Einfluss auf die anderen Schnittstellen.
g) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.4.2.2 Schnittstelle KS3

a) Der DC verbindet sich über diese Schnittstelle nur mit den entsprechenden WAN-Schnittstellen der iMG und des HES.
b) Die Kommunikation erfolgt verschlüsselt auf einer geeigneten Protokollebene. Die verwendeten Algorithmen werden regelmässig auf Stand der Technik geprüft bzw. bei bekannt gewordener Kompromittierung zeitnah ausgetauscht.
c) Für den Zugriff über diese Schnittstelle sind mindestens die Benutzerrollen DC-Administrator sowie Operator gemäss den entsprechenden Zugriffsrechten verfügbar.
d) Für Telearbeit sollten wo möglich zweistufige Authentisierungsverfahren (basierend auf „Besitz und Wissen“) implementiert sein. Dies kann für Zugriffe auf den DC über das HES der Fall sein.
e) Telearbeit z.B. für Wartungszwecke der Hersteller mit „trivialen“ Authentisierungsverfahren ist nicht zulässig.
f) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des DC möglich.
g) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
h) Eine Störung der Schnittstelle hat keinen Einfluss auf die anderen Schnittstellen.
i) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.4.2.3 Schnittstelle KS1

a) Der DC verbindet sich über diese Schnittstelle nur mit der entsprechenden WAN-Schnittstelle anderer Messgeräte im LMN.
b) Die Kommunikation erfolgt wenn möglich verschlüsselt auf einer geeigneten Protokollebene. Die verwendeten Algorithmen werden regelmässig auf Stand der Technik geprüft bzw. bei bekannt gewordener Kompromittierung zeitnah ausgetauscht.
c) Für den Zugriff auf diese Schnittstelle sind keine Benutzerrollen verfügbar. Der DC-Administrator konfiguriert die Verbindungen

d) Zähldaten der Geräte an der **KS1**-Schnittstelle werden durch das Modul Kommunikation nur via **KS3** ohne Daten-Bearbeitung im DC, jedoch ggf. mit Protokoll-Umwandlung und Umschlüsselung, übertragen.
e) Über die Schnittstelle ist keine Verbindung auf andere Schnittstellen des DC möglich.
f) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
g) Eine Störung der Schnittstelle hat keinen Einfluss auf die anderen Schnittstellen.
h) Unbefugte Zugriffsversuche und andere Störungen, welche die entsprechende Hauptkomponente im Rahmen der an der Schnittstelle verwendeten Protokolle detektieren kann, lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.4.3 Spezifische Anforderungen

5.4.3.1 Verwendung der Verschlüsselung

a) Jedes Gerät erhält einen individuellen Auslieferungsschlüssel. Dieser wird bei der Erst-Inbetriebnahme nach erfolgreicher Registrierung durch einen neuen Schlüssel ersetzt.
b) Beim Wechsel eines DC kann der Auslieferungsschlüssel wieder aktiviert werden.
c) Die Verschlüsselung ist mit einer zum Zeitpunkt der Auslieferung als sicher geltenden Technologie realisiert.
d) Die Verschlüsselungstechnologie ist update-fähig.
e) Die Kryptoschlüssel werden in allen Geräten und Systemen gegen unbefugten Zugriff geschützt.

5.4.3.2 Zeiteinstellungen

a) Für den Zugriff auf dieses Objekt über die Schnittstelle KS0 wird die Benutzerrolle DC-Administrator gemäss den entsprechenden Zugriffsrechten verwendet.
b) Die Authentifizierung erfolgt mindestens über Benutzername und Passwort.
c) Die Änderung der Zeiteinstellung im DC löst eine Meldung an den Datenmanager aus und wird in die Log-Daten übernommen.
d) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an das MDM System aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.5 Anforderungen an das HES

(1) Das Head End System ist eine Hauptkomponente des iMS im Sinne der Definition in Abschnitt 2.3. Über sie greifen verschiedene Rollen und auch automatisierte Prozesse des MDM beim Datenmanager auf Hauptkomponenten des iMS zu.

a) Dem entsprechend gelten für diese, den Rollen beim Datenmanager angebotenen, externen Schnittstellen Sicherheitsanforderungen auf demselben Niveau wie bei den anderen Hauptkomponenten.

(2) Eine herausragende Bedeutung hat die WAN-Schnittstelle des HES. Sie verbindet die Hauptkomponente HES mit den anderen (iMG bzw. DC) über Datenfernübertragung.

b) Daher muss diese Verbindung das Sicherheitsniveau der Hauptkomponenten aufweisen.

(3) Das HES verfügt über die externe Schnittstelle WAN und ggf. mehrere unterschiedliche lokale externe Schnittstellen:

- zur lokalen und entfernten Systemkonfiguration (regulärer Betrieb; Mensch-Maschine Schnittstelle; MMI (Man Machine Interface))
- zur automatisierten Datenübertragung vom iMS zum Datenmanager (regulärer Betrieb; API o.ä.)
- für Sonstiges (z.B. Support-Techniker des Herstellers o.ä.).

c) Die lokalen externen Schnittstellen müssen dasselbe Sicherheitsniveau der Hauptkomponenten aufweisen.

(4) Abhängig vom Lieferumfang der Hersteller umfasst das HES mindestens die HES-Anwendung, kann aber auch als eigenständiges System aus HW, Betriebssystem und Anwendung bestehen.

5.5.1 Anforderungen an den sicheren Betrieb

5.5.1.1 Auslieferung und Erst-Inbetriebnahme

(1) Die Versionsnummern und Softwarelizenzen der SW (ggf. einzelner Komponenten) sind dokumentiert.

5.5.1.2 Sicheres Booten

a) Das Betriebssystem der Rechnerplattform des HES ist nach der Erst-Inbetriebnahme in der Lage, bei jedem Neustart in den vorgesehenen Betriebsmodus zu kommen.
b) Bootmenüs sind nur durch berechtigte Administratoren zugänglich.
c) Booten von externen Datenträgern ist nicht möglich.
d) Stellt das System einen fehlerhaften Wiederanlauf fest, werden eine Fehlermeldung ausgegeben sowie ein Alarm an den Datenmanager erzeugt und diese Ereignisse in die Log-Daten übernommen.

5.5.1.3 Sicherer Start der Anwendung HES

a) Die HES-Anwendung ist nach der Erst-Inbetriebnahme in der Lage, bei jedem Neustart in den vorgesehenen Betriebsmodus zu gelangen.
b) Stellt die Anwendung einen fehlerhaften Wiederanlauf fest, werden eine Fehlermeldung ausgegeben und ein Alarm an den Datenmanager erzeugt, und diese Ereignisse werden in die Log-Daten übernommen.
c) Die HES-Anwendung ist in der Lage, eine Integritätsprüfung an sich selbst durchzuführen. Bei einer fehlerhaften Integritätsprüfung werden eine Fehlermeldung ausgegeben sowie ein Alarm an den Datenmanager erzeugt, und diese Ereignisse werden in die Log-Daten übernommen.

5.5.1.4 Speicherschutz

a) Das Betriebssystem der Computerplattform der HES-Anwendung erlaubt Speicherplatzmanagement, so dass im flüchtigen Speicher dieses Rechners Adressräume exklusiv für die entsprechenden Anwendungen reserviert sind.
b) Speicherbereiche, in denen Zähldaten bzw. Kryptoschlüssel temporär abgelegt werden, werden nach deren Verwendung durch gezieltes Überschreiben wiederaufbereitet.

5.5.1.5 Sicheres Löschen

a) Daten mit Schutzbedarf, die auf Datenträgern gespeichert wurden, werden durch ein Verfahren nach Stand der Technik (BSI (D), DoD (USA) o.ä.) physikalisch durch mehrfaches Überschreiben mit Zufallsdaten unlesbar gemacht. Persistente Datenträger (z.B. CD-ROM) werden gemäss diesen Anforderungen unlesbar gemacht.

5.5.1.6 Logging

a) Alle aus Sicht der Datensicherheit relevanten Systemereignisse werden in die Log-Daten übernommen.
b) Log-Daten dürfen nur durch entsprechend autorisierte Benutzer ausgelesen werden.
c) Log-Daten sind gegen unautorisierte Änderung bzw. Löschung gesichert.
d) Art und Umfang der zu loggenden Daten sind nicht Gegenstand des vorliegenden Dokuments. Sie sind vielmehr durch die technische Umsetzung eines iMS bzw. einer Hauptkomponente davon sowie durch die Betriebsführung des Datenmanagers bestimmt. Im Minimum unterstützt das Logging die in [4] spezifizierten Anforderungen.

   Die Hersteller sind gehalten, den Umfang der zu loggenden Daten den Ansprüchen der Betreiber anzupassen.

5.5.1.7 Firmware Update

a) Für das Update einer HES-Anwendung werden Systemadministratoren-Rechte (keine im vorliegenden Dokument betrachtete Rolle) an der entsprechenden Rechnerplattform benötigt.

5.5.2 Schnittstellen

5.5.2.1 Schnittstelle WAN

a) Das HES verbindet sich über diese Schnittstelle nur mit der entsprechenden **KS3**-Schnittstelle des iMG oder des DC bzw. Gateway.
b) Die Kommunikation erfolgt verschlüsselt auf einer geeigneten Protokollebene. Die verwendeten Algorithmen werden regelmässig auf Stand der Technik geprüft bzw. bei bekannt gewordener Kompromittierung zeitnah ausgetauscht.
c) Für den Zugriff auf diese Schnittstelle sind keine Benutzerrollen definiert.
d) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
e) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.5.2.2 Lokale Schnittstellen des HES

5.5.2.2.1 Mensch-Maschine

a) Für den Zugriff auf diese Schnittstellen sind mindestens die Benutzerrollen „Administrator“ und „Operator“ verfügbar.
b) Die Einstellung der granularen Zugriffsrechte für HES-Administrator, iMG-Administrator, DC-Administrator, Operator, Breaker-Manager und Hersteller-Support ist gemäss der entsprechenden Topologie vorzunehmen.

c) Die Authentifizierung erfolgt mindestens über Benutzername und Passwort. Falls eine Hauptkomponente Telearbeit unterstützt, müssen starke Authentisierungsverfahren (basierend auf „Besitz und Wissen“) implementiert sein.
d) Die Schnittstelle ist gehärtet gegen Angriffe wie z.B. Denial-of-Service, Replay, Buffer Overflow etc.
e) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an den Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.

5.5.2.2.2 Maschine-Maschine (iMS-MDM)

a) Da die Ausprägung der Architektur des MDM je nach Hersteller sehr unterschiedlich ist, sind die folgenden Punkte als Empfehlung zu verstehen.
b) Diese Schnittstelle dient der automatisierten Übertragung der Zähldaten aus dem iMS zum HES des Daten-managers. Als externer Schnittstelle des HES besteht die grundsätzliche Anforderung darin, unbefugten Zugriff auf das HES zu verhindern.
c) Dem entsprechend sind für den Zugriff auf diese Schnittstelle keine Benutzerrollen definiert.
d) Je nach Ausprägung der Schnittstelle werden die Zähldaten in einem konfigurierbaren Format exportiert. Die Übertragung findet in der Domäne des Datenmanagers statt. Die vom iMS übertragenen Daten sind daher aus Sicht der Datensicherheit und des Datenschutzes durch die Schutzfunktionen der die Daten weiterbearbeitenden Systeme für die weitere Übertragung und Bearbeitung abgesichert.

5.5.3 Spezifische Anforderungen

a) Der HES-Administrator konfiguriert das HES.
b) iMG-Administrator und DC- (bzw. Gateway-)Administrator konfigurieren die entsprechenden Hauptkomponenten des iMS aus dem Bereich des Datenmanagers heraus.
c) Der Operator kann zusätzlich zur automatisierten Datenübertragung gezielt auf Zähldaten in bestimmten iMG zugreifen.
d) Der Breaker-Manager löst die Breaker in den iMG aus der Domäne des Datenmanagers heraus aus bzw. bereitet das Rücksetzen vor.
e) Der Hersteller-Support konfiguriert die entsprechenden Hauptkomponenten aus der Domäne des Datenmanagers heraus nur dann, wenn diese sich nicht im operativen Betrieb befinden.
f) Grundsätzlich werden die Hauptkomponenten im regelmässigen Betrieb ausschliesslich durch die entsprechenden Benutzerrollen des Datenmanagers konfiguriert.
g) Das HES kann Meldungen anderer Hauptkomponenten regelbasiert an entsprechende Benutzer beim Datenmanager weiterzuleiten.

5.5.4 Allgemeine Anforderungen

5.5.4.1 Betriebsumgebung

a) Je nach Lieferumfang des HES (SW oder Appliance (HW und SW)) gemäss Abschnitt 5.5 ist eine vertrauenswürdige Betriebsumgebung durch den Datenmanager sicherzustellen. Dies umfasst die Konfiguration der Rechnerplattform, die Übernahme der HES-spezifischen Benutzerrollen sowie die geeigneten Zuordnungen der entsprechenden Benutzerrollen des Datenmanagers.
b) Es liegt in der Verantwortung des Datenmanagers, sicherzustellen, dass Wartungszugriffe durch die Hersteller auf die entfernten Hauptkomponenten dasselbe Sicherheitsniveau aufweisen wie

diejenigen Wartungszugriffe aus der Domäne des Datenmanagers aufweisen (idealer Weise: Zweifaktorauthentisierung an einem HES und durchgehend verschlüsselte Verbindung zur entfernten Hauptkomponente).

5.5.4.2 MDM / EDM

a) Wenn das HES Zähldaten automatisiert exportiert, müssen die entsprechenden Schnittstellen zu EDM-Systemen unterstützt werden.
b) Dies darf nicht zu einer Kompromittierung des Sicherheitsniveaus des HES führen.

5.6 Anforderungen an die Visualisierungsplattform

5.6.1 Endkundenschnittstelle (Visualisierungsplattform lokal)

5.6.1.1 Identifikation und Authentisierung

a) Am iMG ist mindestens eine Lösung mit Benutzername und Passwort implementiert. Diese kann für eine Selbstregistrierung des Prosumers ausgelegt sein.

5.6.1.2 Zugriffskontrolle

a) An der Schnittstelle sind bezüglich der Rolle Prosumer für alle schützenswerten Objekte Zugriffsrechte definiert.

5.6.1.3 Trennung der Schnittstellen

a) Die Schnittstelle zur Visualisierungsplattform muss von den anderen Schnittstellen des iMG getrennt sein.
b) Die Zähldaten zur Visualisierung werden vom iMG geeignet aufbereitet, und die Rolle Prosumer hat nur lesenden Zugriff auf die zu visualisierenden Daten.

5.6.2 Visualisierungsplattform entfernt

5.6.2.1 Identifikation und Authentisierung

a) Für alle Zugriffe auf die Visualisierungsplattform authentisiert sich der Prosumer gegenüber dem entsprechenden System des Datenmanagers. Wenn möglich sollte ein zweistufiges Authentisierungsverfahren (basierend auf „Besitz und Wissen“) implementiert sein.

5.6.2.2 Zugriffskontrolle

a) An der Schnittstelle, sind bezüglich der Rolle Prosumer für alle schützenswerten Objekte Zugriffsrechte definiert.

5.6.2.3 Verschlüsselung

a) Die Kommunikation zwischen Prosumer und entfernter Visualisierung erfolgt Ende-zu-Ende-verschlüsselt.

5.6.2.4 Architektur

a) Die Daten werden aus dem MDM bezogen und es muss eine sichere Übertragung zwischen dem MDM (one-way) bzw. einer Komponente der übergeordneten Systeme (bi-direktional) und der entfernten Visualisierungsplattform eingerichtet werden.

5.6.2.5 Entfernte Visualisierungsplattform

(1) Die entfernte Visualisierungsplattform bietet dem Prosumer ggf. einen interaktiven Zugang zu seinem Vertragspartner. Ein Teil der Funktionalität besteht jedoch in der Visualisierung von Verbrauchsdaten.

a) Die Personalisierung dieser Daten für entsprechend autorisierte Prosumer erfolgt im ZDVS, jedoch nicht durch das HES oder eine andere Hauptkomponente.
b) Dem entsprechend muss die Integrität der prosumerbezogenen Daten ab HES sichergestellt sein.
c) Gleichzeitig muss die Visualisierung der Daten prosumerbezogen vertraulich erfolgen.
d) Eine unautorisierte Änderung der visualisierten Verbrauchsdaten (z.B. durch den Prosumer) ist ausgeschlossen.

6. Anforderungen an das Schlüsselmanagement

(1) Die Hauptkomponenten des iMS sowie auch andere Zähler verwenden kryptografische Schlüssel zur Absicherung verschiedener Prozesse. Aktuell und auf absehbare Zeit verfügen viele dieser Geräte nicht über hinreichend Rechenleistung bzw. Speicherplatz für komplexe kryptografische Anwendungen bzw. umfangreiches Schlüsselmanagement. Dem entsprechend müssen sie mit entsprechenden, geeigneten Schlüsseln auf eine andere Weise ausgestattet werden. Und insbesondere muss die Gesamtheit der in einem iMS befindlichen Schlüssel durch ein Schlüsselmanagement verwaltet werden. Dies wird ausserhalb des Prüfgegenstands „HES“, jedoch im ZDVS stattfinden. Somit ergeben sich die folgenden Mindestanforderungen. Abhängig von der jeweiligen, produktspezifischen Architektur erfolgt eine Prüfung nicht gegen eine generische Vorgabe sondern basierend auf den Informationen der Hersteller zu den folgenden Aspekten.

a) Das Schlüsselmanagement deckt den gesamten Lebenszyklus aller kryptografischen Schlüssel im Gesamtsystem ab:

   - Generierung
   - Verteilung
   - Sperrung
   - PKI für zertifikatsbasierte Kryptografie

b) Es ist auf geeignete Weise gegen unautorisierte Zugriffe geschützt.
c) Vor-installiertes Schlüsselmaterial auf Hauptkomponenten dient ausschliesslich der Inbetriebnahme, darf im Betrieb nicht angewendet werden und wird bei der Inbetriebnahme durch operativ anzuwendende Schlüssel ersetzt.
d) Die Verwendung trivialer Schlüssel ist nicht zulässig.
e) Die Verwendung von Gruppenschlüsseln ist nicht zulässig ausser bei Broadcast.
f) Die Benutzerrollen für das Schlüsselmanagement sind vom entsprechenden Hersteller zusätzlich zu denen in Abschnitt 5.1.1 zu definieren. Das Einbringen von Schlüsseln kann via Fernwartung bzw. lokal an den Geräten erfolgen. Geeignete Sicherheitsfunktionen zum Schutz gegen unautorisierten Zugriff auf Schlüsselmaterial sind implementiert.
g) Kryptografische Algorithmen und Schlüssellängen entsprechen jeweils dem Stand der Technik. Die Lebensdauer ist ebenfalls definiert, und es existiert ein verbindlicher Zeitplan für updates bzw. upgrades. Bei bekannt werdender Kompromittierung von Algorithmen oder Schlüssellängen erfolgen updates bzw. upgrades zeitnah.
h) Die Generierung kryptografischer Schlüssel erfolgt durch Komponenten auf aktuellem Stand der Technik.

Glossar

Beispiel Bundesverwaltung: Schlüssel und Algorithmen für „INTERN“, Stand Juli 2017; Quelle: Informatikstrategieorgan des Bundes (ISB)

Bereich	Anwendung / Protokoll	Algorithmus /	Mindest-Werte	Bemerkungen
Verschlüsselung	symmetrisch	AES	128 bit	Transportverschlüsselung: Galois Counter Mode GCM Lokal: Cipher Block Chaining Modus CBC Stromverschlüsselung: Counter Mode CTR
	asymmetrisch	RSA, ElGamal	2048 bit	ECC
Hashfunktionen		SHA-2, SHA-3	H-Wert 256 bit	SHA-1 und MD5 nicht zulässig
Datenauthentifizierung	chiffriert und authentifiziert	AES im GCM		
	nur authentifiziert	HMAC mit SHA-2 oder SHA-3		Keyed-Hash Message Authentication Code
Elektronische Signatur		RSA, DSA	2048 bit	starke Schlüsselpaare wichtig
		ECDSA	256 bit	
Schlüsselaustausch	Diffie-Hellmann Ephemeral (DHE)	Perfect Forward Secrecy (PFS)	2048 bit	PFS gegen Replay Attacks
Transport Layer Security (TLS)	Schlüsselaustausch	DHE	2048 bit	
		ECDHE	256 bit	
	Datenübertragung	Authenticated Encryption with Additional Data (AEAD)		z.B. AES im GCM Secure Sockets Layer (SSL) nur in begründeten Ausnahmen
Secure Shell (SSH)	Schlüsselaustausch DH mit Group-Exchange			Version 2 Version 1 nur in begründeten Ausnahmen CTR und GCM CBC nur in begründeten Ausnahmen
VPN	IPsec (Internet Protocol Security)	Internet Key Exchange (IKE)		Schlüsselaustausch IKEv2 IKEv1 nur in begründeten Ausnahmen Pre-shared Keys 20 Zeichen inkl. Sonderzeichen
	OpenVPN			TLS-basiert
WLAN	WPA2			WPA und WEP nur in begründeten Ausnahmen Wi-Fi Protected Setup (WPS) nicht zulässig
Bluetooth				mindestens die Version 2.1 im Security Mode 4 Bluetooth LE3 (ab v4.0) im Security Mode 1 Level 3 „Just Works“ für das Pairing nicht zulässig (M-i-t-m Angriff)

Abkürzungen und Definitionen

API	Programmierschnittstelle (englisch application programming interface)
AT	Österreich
BFE	Bundesamt für Energie
Breaker	Unterbrecherkontakt im iMG
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIS	Customer Information System;
D	Deutschland
DC	Datenkonzentrator
DMS	Distribution Management System
DoD	United States Department of Defense
DSsquare	DS steht für Datenschutz sowie Datensicherheit; square engl. u.a. für ordentlich
EDM	Energiedaten-Management
HAN	Home Area Network
HES	Head End System
HT	Hoch-Tarif
HW	Hardware
I&A	Identifikation und Authentisierung
ICT	Information and Communication Technology
iMG	intelligentes Messgerät
iMS	intelligentes Messsystem
IPsec	Internet Protocol Security durch Verschlüsselung gesicherte Kommunikation über IP-Netze wie das Internet
ISMS	Information Security Management System
IT	Informationstechnik
LAN	Local Area Network
LMN	Local Metrological Network
Log	Kurzform von Logging; dient für die Aufzeichnung und Nachvollziehbarkeit von Fehlerzuständen etc.
mandantentauglich	Informationstechnik, die auf derselben Plattform oder demselben Software-System mehrere Mandanten, also Kunden oder Auftraggeber, bedienen kann, ohne dass diese gegenseitigen Einblick in ihre Daten, Benutzerverwaltung und Ähnliches haben
MDM	Meter Data Management; in diesem Dokument: Zähldatenverarbeitung jenseits der Hauptkomponente HES des iMS
METAS	Eidgenössisches Institut für Metrologie
MID	Measuring Instruments Directive (Messgeräterichtlinie 2004/22/EG)
NT	Nieder-Tarif
PKI	Public Key Infrastructure (für Anwendungen asymmetrischer Verschlüsselung)
PLC	Powerline Communication
Relais	Steuerkontakt im iMG
RS	Risikoszenario; Risk Scenario
SBA	Schutzbedarfsanalyse
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP
TLS	Transport Layer Security (TLS, deutsch Transportschichtsicherheit; früher: Secure Sockets Layer, SSL)
UK	United Kingdom
VNB	Verteilnetzbetreiber

VSE	Verband Schweizerischer Elektrizitätsunternehmen
WAN	Wide Area Network
WLAN	drahtloses lokales Netzwerk – Wireless LAN