swissmig

Prüfmethodologie
zur
Durchführung der Datensicherheitsprüfung
für
Smart Metering Komponenten
in der Schweiz

Basierend auf der
Schutzbedarfsanalyse des BfE
sowie
den Arbeiten der
swissmig-Arbeitsgruppe „DSsquare“

Version 2.1, 1. Juli 2019

Referenzdokumente

	Titel	Herausgeber
[1]	Anforderungen Datensicherheit / Datenschutz intelligente Messsysteme; V2.0; 02/2017	swissmig
[2]	Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz; 11/2014	BfE
[3]	Studie «Schutzbedarfsanalyse Smart Metering in der Schweiz»; 06/2016	BfE
[4]	Stromversorgungsverordnung vom 14. März 2008 (StromVV)	Der Schweizerische Bundesrat
[5]	Stromversorgungsverordnung (StromVV) Änderung vom 1. November 2017	Der Schweizerische Bundesrat
[6]	Branchenempfehlung Strommarkt Schweiz Richtlinien und Anforderungen zur Durchführung einer Datensicherheitsprüfung, Anhang 1, 2018	VSE

Versionen und Dokumentenhistorie

Version	Datum	Bearbeiter/Änderungen
1.3	13.02.2019	Finale Version mit allen Ergänzungen, verabschiedet im März 2019
2.0	20.03.2019	Offizielle Version
2.1	01.07.2019	Redaktionelle Nachbearbeitung der Passagen 5.2.1.3 b), 5.3.1.3 b) 5.4.1.4 b) gemäss V1.3

INHALT

1 Geltungsbereich

Zu prüfen ist die Erfüllung der Anforderungen an die Hauptkomponenten (HK) intelligentes Messgerät (iMG), Kommunikationssystem (KS; Datenkonzentrator (DC) oder Gateway (GW)) und Head End System (HES) durch den jeweiligen Prüfgegenstand (PG). Ein PG besteht im Minimum aus einem iMG und einem HES und kann auch in einer erweiterten Konfiguration untersucht werden, sofern diese konform mit Abschnitt 2.5 des Anforderungskatalogs ist.

Die funktionalen und architektonischen Anforderungen sind im Abschnitt 5 des Anforderungskatalogs [6] (Branchenempfehlung Strommarkt Schweiz Richtlinien und Anforderungen zur Durchführung einer Datensicherheitsprüfung, Anhang 1)spezifiziert. Für alle HK gilt Abschnitt 5.1 übergreifend.

Komponentenspezifische Anforderungen an zu einem PG gehörende HK sind dort in den Abschnitten 5.2 bis 5.5 spezifiziert.

In Abschnitt 5.6 sind die Anforderungen an Komponenten zur kundenspezifischen Visualisierung von Verbrauchsdaten (Visualisierungsplattform (VP)) spezifiziert. Eine VP ist als externe Komponente kein Teil eines PG, jedoch sind die Anforderungen an die Datensicherheit der Schnittstelle zwischen iMG und VP Teil der Spezifikation in 5.2.

Die für den Betrieb eines PG notwendige Kryptografie wird durch eine organisatorische Komponente „Schlüsselmanagement“ zur Verfügung gestellt. Das korrekte und wirksame Funktionieren der Kryptografie in den HK wird als Komponenteneigenschaft geprüft. Das Schlüsselmanagement wird als organisatorische Unterstützungskomponente gemäss den Anforderungen des Abschnitts 6 begutachtet.

Liste der entsprechenden Abschnitte des Anforderungsdokuments [6]:

- Übergreifende IT-Sicherheitsanforderungen an alle 4 Arten von HK (5.1)
- Komponentenspezifische Anforderungen an
  - iMG (5.2)
  - GW (5.3)
  - DC (5.4)
  - HES (5.5)
  - VP (5.6)
- Schlüsselmanagement, Key Management, KM (6)
- Architektur konform zu 2.5

2 Herstellerdokumentation

Die Hersteller stellen der Prüfstelle eine geeignete Dokumentation zur Verfügung, so dass die Prüfer alle Prüfaspekte ohne Rückfrage untersuchen können. Diese Dokumentation gibt Auskunft über den Prüfgegenstand und wie dieser die entsprechenden Anforderungen hinsichtlich eines vertrauenswürdigen Betriebs erfüllt. Das mit diesen Informationen gewonnene Wissen wird als Grundlage für die Durchführung von Schwachstellenanalysen und Tests verwendet.

Zu dokumentierende Aspekte:

- Korrespondenzzuordnungen zwischen Sicherheitsrichtlinienmodell und der funktionalen Spezifikation (Prüffeld IT-Sicherheitskonzeption)
- Beschreibung des Entwurfs und der Implementierung zur Erfüllung der entsprechenden Anforderungen (Prüffeld Produktentwicklung, Architektur, Funktionalität)
- Beschreibung der architekturorientierten Merkmale der Sicherheitsfunktionalität (Prüffeld Produktentwicklung, Architektur, Funktionalität)
- Produktdokumentation, Handbücher etc. so dass Administratoren und Anwendern eine vertrauenswürdige Konfiguration des Systems ermöglicht ist (Prüffeld Produktdokumentation)
- Beschreibung, dass im Produktlebenszyklus keine organisatorischen Schwachstellen existieren, über die die Vertrauenswürdigkeit des Produktes kompromittiert werden kann (Prüffeld Produktlebenszyklus)
- Dokumentation der herstellerseitig ausgeführten Tests der implementierten Sicherheitsfunktionen (Optionale Verifikation herstellerseitig)

Durch die Dokumentation der Sicherheitsfunktionalität eines PG müssen zwei Eigenschaften demonstriert werden. Die erste Eigenschaft ist, dass die Sicherheitsfunktionalität korrekt funktioniert (Korrektheit) und die zweite, dass der PG nicht in einer Weise verwendet werden kann, dass die Sicherheitsfunktionalität beschädigt oder umgangen werden kann (Wirksamkeit).

3 Formale Randbedingungen

Zur optimalen Durchführung einer Prüfung muss die Prüfstelle über den Umfang des PG, die darin enthaltenen HK und die Art und Weise, wie die entsprechenden Anforderungen erfüllt werden, in geeigneter Weise informiert werden.

Dem entsprechend existieren Qualitäts-Anforderungen an die Herstellerdokumentation.

Gleichfalls bestehen Qualitäts-Anforderungen an die Prüfstelle, so dass unterschiedliche, jedoch vergleichbare Prüfgegenstände immer gleichwertige Prüfergebnisse erhalten und derselbe Prüfgegenstand bei verschiedenen Prüfungen immer gleichwertige Prüfergebnisse erhält.

Aus diesem Grund werden für die Prüfmethodologie geeignete Ausschnitte der

> *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, April 2017, Version 3.1, Revision 5*

zugrunde gelegt. Die CC stellen als ISO/IEC 15408 eine Grundlage für die standardisierte Prüfung von IT-Sicherheitseigenschaften von IT-Produkten und –Systemen dar und enthalten Prüffelder (Assurance Classes) und darin jeweils Prüfaufgaben (Assurance Components). Je nach Prüftiefe (Umfang und Intensität) der Prüfungen ändern sich die Anzahl und die Umfänge der Assurance Components in einer entsprechenden Assurance Class. In der Anwendung der Common Criteria ergeben sich wiederholt und regelmässig als grundsätzliche Kritikpunkte der unverhältnismässige Aufwand für Dokumentation und Prüfschritte sowie die geringe Flexibilität in der Anwendung.

Für die Konformitätsprüfung eines aus anforderungskonformen HK zusammengesetzten PG ist das Instrument CC untauglich, wohingegen die standardisierte Spezifikation entsprechender Prüfschritte in den Assurance Components bei geeigneter Auswahl extrem hilfreich ist, um die Qualitätsziele der vorliegenden Prüfmethodologie zu erfüllen (insbesondere Vergleichbarkeit und Reproduzierbarkeit).

4 Aspekte der Datensicherheit

Die IT-Sicherheitseigenschaften eines Produkts können auf verschiedene Weisen an unterschiedlichen Stellen seines Lebenszyklus kompromittiert werden. Dies könnte durch mangelhafte Spezifikation bzw. Implementierung der IT-Sicherheitsfunktionen während der Entwicklung des eigentlichen Produkts passieren, jedoch auch durch bereits kompromittierte Komponenten von Zulieferern oder (IT-)Sicherheitslücken in der Entwicklungsabteilung sowie bei der Auslieferung und Inbetriebnahme.

Dem entsprechend umfasst die hinsichtlich Datensicherheit zu betrachtende Umgebung der Prüfgegenstände mehr Aspekte als nur die „out-of-the-box" Version des entsprechenden Produkts.

Diese Prüfmethodologie ist ein State-of-the-art Prüfverfahren und deckt die folgenden Aspekte ab:

1. **IT-Sicherheitskonzeption**
   Auslegeordnung, welche schutzbedürftigen Objekte in einem System existieren, wodurch sie aus Sicht der Datensicherheit bedroht sind (Verlust oder Einschränkung von Vertraulichkeit, Integrität bzw. Verfügbarkeit) und welche Sicherheitsfunktionalitäten dies verhindern sollen
2. **Produktentwicklung, Architektur, Funktionalität**
   Beschreibung der Architektur und der Funktionen eines Systems hinsichtlich einer korrekten Umsetzung gemäss IT-Sicherheitskonzeption
3. **Produktdokumentation**
   Wegleitung, die Betreiber - und insbesondere auch Prüfstellen - in die Lage versetzt, ein System in einen sicheren Betriebszustand zu bringen
4. **Produktlebenszyklus**
   Nachweis, dass alle Systemkomponenten identifizierbar sind und in ihren Lebenszyklen gegen Verlust oder Einschränkung von Vertraulichkeit, Integrität bzw. Verfügbarkeit geschützt sind
5. **Verifikationstests herstellerseitig (QM o.ä.)**
   Nachweis, dass alle sicherheitsrelevanten Systemkomponenten Abnahmetests hinsichtlich Korrektheit und Wirksamkeit durchlaufen haben
6. **Penetrationstests prüfstellenseitig**
   Schwachstellenanalyse durch eine Prüfstelle, um das Vorhandensein potenzieller Schwachstellen zu ermitteln (Korrektheit) bzw. tatsächliche Schwachstellen zu detektieren sowie ein Mass der Widerstandsfähigkeit der Sicherheitsfunktionalität gegen Bedrohungen zu ermitteln (Wirksamkeit)

Anders als bei Produkt- oder System-Evaluationen gemäss Common Criteria, wo durch ein spezielles Security Target bzw. ein spezielles Protection Profile der Prüfgegenstand festgeschrieben wird, weist das vorliegende Verfahren insbesondere diesbezüglich eine hohe Flexibilität auf. Die möglichen Prüfgegenstände sind Kombinationen aus iMG, KS und HES, so dass durch eine Konformitätsprüfung sichergestellt werden kann, dass alle möglichen Kombinationen in demselben Grad den IT-Sicherheitsanforderungen des Anforderungskatalogs entsprechen.

Gemäss den Vorgaben des Artikels 8 der Stromversorgungsverordnung muss für alle eingesetzten Elemente nachgewiesen werden, dass diese diejenigen Datensicherheits-Anforderungen erfüllen, welche sich aus der schweizerischen Schutzbedarfsanalyse (Version 2016) ergeben. Die hierin untersuchten Risikoszenarien sind dadurch gekennzeichnet, dass in ihnen jeweils als zentraler Vertrauensanker die Umgebung des iMS bei Prosumer und Datenmanager zugrunde liegt. Dem entsprechend wurden für die Hauptkomponenten (HK) eines intelligenten Messsystems (iMS) basierend auf der SBA die schutzbedürftigen Objekte und die identifizierten Bedrohungen spezifiziert und daraus generische Anforderungen an die Systemarchitektur und die Funktionalität abgeleitet.

Diese Generizität muss jedoch für die entsprechenden Prüfgegenstände durch die jeweiligen Hersteller mit Hilfe zusätzlicher Dokumentation konkretisiert werden, so dass eine Prüfstelle anhand dieser konkret vorliegenden Dokumentation sowie dem Prüfgegenstand bewerten kann, ob die Anforderungen aus dem Anforderungskatalog erfüllt sind.

Insgesamt ergeben sich zur Abdeckung der obigen Aspekte verschiedene Aufgaben für Hersteller und Prüfstellen, welche im Folgenden beschrieben werden.

Die Aufgaben umfassen neben der Übergabe des Prüfgegenstands an die Prüfer verschiedene Dokumentationen (Liefergegenstände) seitens des Herstellers, welche prüfungsrelevante, vertrauliche Informationen für die Prüfer liefern, um eine maximale Effizienz bei gleichzeitig minimer Prüfdauer zu gewährleisten.

Die Untersuchungen der Prüfstelle folgen mindestens teilweise und -wo angegeben - standardisierten Vorgaben (Aufgaben) und resultieren in einer schriftlichen Berichterstattung, welche Grundlage für den Zertifizierungsprozess beim METAS ist.

Die vorgegebenen Prüffelder decken die in Abschnitt 4 formulierten Aspekte der Datensicherheit auf unterschiedliche Weisen, jedoch ganzheitlich ab.

Übersicht Liefergegenstände und Aufgaben

Aspekt der Datensicherheit	Herstelleraufgabe	Prüfstellenaufgabe
IT-Sicherheitskonzeption	Dokumentation erstellen	• ASE_OBJ.2 (IT-Sicherheitskonzeption) • ASE_TSS.2 (Lokalisierung und Zuordnung Sicherheitsfunktionalität)
Produktentwicklung, Architektur, Funktionalität	Prüflisten vervollständigen	• ADV_ARC.1 (Architekturbeschrieb) • ADV_FSP.1 (Funktionsbeschrieb) basierend auf Prüflisten entsprechend den Hauptkomponenten im Prüfgegenstand
Produktdokumentation	Handbücher mit hinreichendem Detaillierungsgrad erstellen	Verwenden und Defizite zurückmelden
Produktlebenszyklus	Dokumentation mindestens gemäss 5.1.5 und 5.x.1.1 erstellen	Diese grundlegenden Anforderungen werden unter „Produktentwicklung, Architektur, Funktionalität“ berücksichtigt. Allfällige Defizite werden zurückgemeldet und ggf. wird ein Audit durchgeführt.
Verifikationstests herstellerseitig	Testdokumentation bezüglich IT-Sicherheitsfunktionalität erstellen	Verwendung zur Vorbereitung der Penetrationstests
Penetrationstests prüfstellenseitig	Prüfgegenstand zur Verfügung stellen	• AVA_VAN.3 (Fokussierte Schwachstellenanalyse)

5 Prüfmethodologie

Grundsätzliche Massgabe für alle Prüfschritte ist die Erzielung von Vergleichbarkeit und Reproduzierbarkeit der Prüfergebnisse.

Zu diesem Zweck muss das Prüfprotokoll alle Prüfschritte der jeweiligen nachfolgenden Prüffelder unmissverständlich nachvollziehbar dokumentieren.

5.1 Prüffeld IT-Sicherheitskonzeption

Diese beinhaltet eine prägnante Aussage über die beabsichtigte Reaktion auf eine angenommene Bedrohung schutzbedürftiger Objekte. Die Bewertung ist erforderlich, um nachzuweisen, dass die Sicherheitsfunktionalität Bedrohungen ausreichend und vollständig abdeckt, dass die Aufteilung dieses Problems zwischen dem Prüfgegenstand und seiner Einsatzumgebung klar definiert ist (Korrektheit der Implementierung der Sicherheitsfunktionalitäten).

Herstelleraufgabe:

Erstellung einer Spezifikation, die beinhaltet

- welche schutzbedürftigen Objekte im jeweiligen System als Teil eines Prüfgegenstands bearbeitet werden bzw. welche wegfallen (basierend auf Objekte-Bedrohungs-Matrix)
- welchen Bedrohungen als Ergebnis davon durch welche Sicherheitsfunktionalität begegnet wird (Bedrohung-Sicherheitsfunktionalitäts-Matrix; dezidierte Beschreibung für jeden in der für eine zu prüfende HK spezifischen Matrix durch ein „x“ indizierten Zusammenhang)
- welche Sicherheitsfunktionalität innerhalb des System bzw. in dessen Betriebsumgebung lokalisiert ist oder ob sie durch organisatorische Vorgaben realisiert werden muss (bspw. Schlüsselmanagement)
- Definition des Prüfgegenstands (In der der Prüfstelle vorliegenden Systemarchitektur eines iMS sind dies diejenigen Hauptkomponenten, welche noch kein Sicherheitszertifikat haben.)
- Eindeutige und nachvollziehbare Identifikation und Dokumentation für alle zu prüfenden Komponenten

Bedrohungen: / Schutzwürdige Objekte	B1: Unberechtigte Modifikation der Daten lokal	B2: Unberechtigte Modifikation der Daten von fern	B3: Unberechtigte Modifikation der Zeiten	B4: Unberechtigter Datenzugriff lokal	B5: Unberechtigter Datenzugriff von fern	B6: Unberechtigter Datenzugriff auf im Gerät gespeicherte	B7: Verlust oder Einschränkung der Verfügbarkeit der Daten	B8: Unberechtigtes Schalten des Breakers	B9: Unberechtigtes Schalten des Relais	B10: Unsicheres Aufstarten
O1: Messdatenverarbeitungssystem	x	x		x	x		x	x	x	
O2: Visualisierungsplattform	x	x		x	x		x			
O3: KS0 lokale Schnittstelle	x			x				x	x	
O4: KS3 Schnittstelle WAN		x			x	x	x	x	x	
O5: KS2 Schnittstelle HAN	x			x			x			
O6: KS1 Schnittstelle LMN	x			x			x			
O7: Krypto Schlüssel				x	x					
O8: Firmware Update	x	x								x
O9: Firmware	x	x						x	x	x
O10: Zählerkonfiguration	x	x								
O11: Zählerzeit			x							
O12: Netzrelevante Daten	x	x					x	x	x	
O13: Lastgang und Registerdaten	x	x		x	x	x				
O14: Alle Daten im Smart Meter	x	x		x	x	x				

Prüfstellenaufgabe:

- Anwendung der Prüfaspekte der Common Criteria hinsichtlich Übereinstimmung von Konzeption und Implementierung
- Dokumentation der durchgeführten Prüfungen und deren Ergebnisse in einem Bericht, welcher Teil des Prüfprotokolls ist
- Indikation, unter welchen Prüfaspekten herstellerseitige Verbesserungen notwendig waren

Prüfaspekte

- ASE_OBJ.2 (IT-Sicherheitskonzeption)
- ASE_TSS.2 (Lokalisierung und Zuordnung Sicherheitsfunktionalität)

Aus CC:

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Developer action elements:

ASE_TSS.2.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

ASE_TSS.2.1C The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.2.2C The TOE summary specification shall describe how the TOE protects itself against interference and logical tampering.

ASE_TSS.2.3C The TOE summary specification shall describe how the TOE protects itself against bypass.

Evaluator action elements:

ASE_TSS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.2.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

Glossar:

SFR Security Functional Requirement

TOE Target of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

5.2 Prüffeld Produktentwicklung, Architektur, Funktionalität

Im Anforderungsdokument (Branchenempfehlung Strommarkt Schweiz Richtlinien und Anforderungen zur Durchführung einer Datensicherheitsprüfung, Anhang 1, [6)] wurden für die Hauptkomponenten eines iMS generische IT-Sicherheitsfunktionalitäten und –architekturen spezifiziert, so dass die schutzbedürftigen Objekte aus der SBA in geeigneter Weise gegen angenommene Bedrohungen geschützt sind.
Ein Prüfgegenstand, bestehend aus HK, stellt eine konkrete Implementierung der Hersteller dar, welche in der Umsetzung dieser Funktionalitäten frei sind.
Daher muss in der Herstellerdokumentation die Entsprechung der spezifischen Implementierungen im Prüfgegenstand zu den generischen funktionalen und architektonischen Ansätzen im Anforderungsdokument dargestellt werden. (Korrektheit der Implementierung der Sicherheitsfunktionalitäten)
Zu diesem Zweck werden Prüflisten (sh. „Anhang Prüflistenmodule“ in diesem Dokument) bezogen auf Hauptkomponenten verwendet, die für einen konkreten Prüfgegenstand geeignet zusammengefasst sind (Jeweils das Modul „Übergreifende Anforderungen in Verbindung mit einem Modul „HK“).
Die Verwendung der Formatierung der Prüfmodule ist nicht zwingend, eine Veränderung der Inhalte ist nicht zulässig.

Herstelleraufgabe:

Vervollständigung der Prüflisten, so dass
- alle Hauptkomponenten des Prüfgegenstands erfasst sind
- allen Anforderungen aus dem Anforderungskatalog (WAS) eine Beschreibung der konkreten Implementierung (WIE) und der Lokalisierung der Implementierung (WO) gegenübergestellt ist
- Referenzierung der jeweiligen Anforderung auf den entsprechenden mit „x“ indizierten Zusammenhang in der Bedrohung-Sicherheitsfunktionalitäts-Matrix

Prüfstellenaufgabe:
- Anwendung der Prüfaspekte der Common Criteria hinsichtlich Übereinstimmung von Konzeption und Implementierung
- Eintrag der Prüfergebnisse in die Prüfliste, welche so zu an das Prüfprotokoll anzuhängen ist
- Dokumentation der durchgeführten Prüfungen und deren Ergebnisse in einem Bericht, welcher Teil des Prüfprotokolls ist
- Indikation, unter welchen Prüfaspekten herstellerseitige Verbesserungen notwendig waren

Prüfaspekte

- ADV_ARC.1 (Architekturbeschrieb)
- ADV_FSP.1 (Funktionsbeschrieb)

Aus CC:
Developer action elements:
ADV_FSP.1.1D The developer shall provide a functional specification.
ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.
Content and presentation elements:
ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.
ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
Evaluator action elements:
ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Developer action elements:
ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.
ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.
Content and presentation elements:
ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.
ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

Glossar:
SFR Security Functional Requirement
TOE Target of Evaluation
TSF TOE Security Functionality
TSFI TSF Interface

5.3 Prüffeld Produktdokumentation

Der Hersteller liefert umfassende und geeignete Produktdokumentation, so dass alle Betreiber - also auch Prüfstellen während der Prüfung - durch umfassende Dokumentation und hier insbesondere hinsichtlich der IT-Sicherheitsvorgaben an die Betriebsumgebung und die Betreiber (Administratoren, Operatoren etc.; u.a. Rollenmodell) angeleitet werden bzw. in die Lage versetzt sind, einen der jeweiligen Anforderungsliste entsprechenden, sicheren Betriebszustand herzustellen.

Herstelleraufgabe:

- Handbücher liefern bezüglich
  administrativer Aspekte
  - Auslieferung
  - Installation
  - Management
  - Betrieb

und

  operativer Aspekte
  - Benutzer

etc.

Prüfstellenaufgabe:

- Rückmeldungen an die Hersteller falls während der Prüfung Defizite in der Dokumentation erkannt wurden
- Dokumentation der Fundstellen in einem Bericht, welcher Teil des Prüfprotokolls ist

5.4 Prüffeld Produktlebenszyklus

Der Lebenszyklus einer Hauptkomponente umfasst mindestens deren Spezifikation, Entwicklung, Auslieferung und Inbetriebnahme sowie ggf. 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.

Herstelleraufgabe:

1. Erfüllung der Anforderungen 5.1.5 „Lebenszyklus“ sowie 5.x.1.1 , $x \in [2; 3;4; 5]$, „Auslieferung und Erst-Inbetriebnahme“

ggf.

2. Bei schweren, in der Prüfung erkannten Defiziten Nachprüfung in Form eines Audits in Zusammenarbeit mit der Prüfstelle
3. Dokumentation hinsichtlich der verbesserten Defizite aktualisieren

Prüfstellenaufgabe:

1. Prüfung der Erfüllung der Anforderungen 5.1.5 sowie 5.x.1.1

ggf.

2. Bei schweren, in der Prüfung erkannten Defiziten Nachprüfung in Form eines Audits in Zusammenarbeit mit dem Hersteller

5.5 Optionale Verifikationstests herstellerseitig

Nachweis, dass alle sicherheitsrelevanten Systemkomponenten Abnahmetests hinsichtlich Korrektheit und Wirksamkeit durchlaufen haben. Dies hilft der Prüfstelle, ihre Penetrationstests zu planen und kann den Aufwand einer Prüfung minimieren.

Herstelleraufgabe:

- Testplanung erstellen, Testen und Testdokumentation erstellen

Prüfstellenaufgabe:

- Nützliche Vorarbeiten des Herstellers mit dem Ziel der Aufwandsminimierung in Prüfvorgang wiederverwenden

5.6 Prüffeld Penetrationstests prüfstellenseitig

Schwachstellenanalyse durch eine Prüfstelle, um das Vorhandensein potenzieller Schwachstellen zu ermitteln (Korrektheit) bzw. tatsächliche Schwachstellen zu detektieren sowie ein Mass der Widerstandsfähigkeit der Sicherheitsfunktionalität gegen Bedrohungen zu ermitteln (Wirksamkeit der Sicherheitsfunktionalitäten).

Herstelleraufgabe:

- Prüfgegenstand zur Verfügung stellen (also ein iMS bestehend aus der/den zu prüfenden HK und bereits geprüften HK)

Prüfstellenaufgabe:

- Anwendung der Prüfvorschriften der Common Criteria hinsichtlich Penetrationstests, um zu bestätigen, dass die potenziellen Schwachstellen in der Betriebsumgebung für den PG nicht ausgenutzt werden können. Penetrationstests werden von der Prüfstelle durchgeführt, wobei ein Angriffspotenzial von **Enhanced-Basic** angenommen wird.
- Dokumentation der durchgeführten Prüfungen und deren Ergebnisse in einem Bericht, welcher Teil des Prüfprotokolls ist
- Nachweis, dass alle mit „x“ indizierten Zusammenhänge in der Bedrohung-Sicherheitsfunktionalitäts-Matrix getestet wurden
- Indikation, unter welchen Prüfaspekten herstellerseitige Verbesserungen notwendig waren

Obligatorisch zu dokumentierende Aspekte:
- Prüfer
- Prüfgegenstand (Seriennummer / Hardware- Softwareversion)
- Vorgehensweise
- Systemkonfiguration
- Eingesetzte Tools (mit Versionsbezeichnungen)
- verwendete Rollen / Schnittstellen
- Ergebnisse

Prüfaspekte

- AVA_VAN.3 (Fokussierte Schwachstellenanalyse)

Aus CC:
Developer action elements:
AVA_VAN.3.1D The developer shall provide the TOE for testing.
Content and presentation elements:
AVA_VAN.3.1C The TOE shall be suitable for testing.
Evaluator action elements:
AVA_VAN.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.3.3E The evaluator shall perform an independent, focused vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.
AVA_VAN.3.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

6 Erläuterungen

6.1 Rollen

Hersteller:

- Stellt Prüfgegenstände mit vorgegebenen IT-Sicherheitseigenschaften her
- Liefert hinreichende Dokumentation an die Prüfstelle

Prüfstelle:

- Weist ihre Qualifikation durch ein ISO17025-äquivalentes QM-System sowie die Expertise ihrer Prüfer hinsichtlich IT-Sicherheitsprüfungen gegenüber dem METAS nach
- Verifiziert, dass für einen gegebenen Prüfgegenstand die richtigen IT-Sicherheitseigenschaften implementiert sind und dass diese wirksam sind
- Erstellt ein Prüfprotokoll als Grundlage für die nachfolgende Zertifizierung

Zertifizierungsstelle METAS:

- Verifiziert und zertifiziert, dass für einen gegebenen Prüfgegenstand durch eine regelkonforme Prüfung die Erfüllung der vorgegebenen IT-Sicherheitseigenschaften nachgewiesen wurde

6.2 Dokumentenhierarchie

Anforderungsliste:

- Beschreibung derjenigen IT-Sicherheitseigenschaften, die ein Prüfgegenstand aufweisen muss;
- Beschreibung der verschiedenen Prüfgegenstände und der möglichen unterschiedlichen Architekturen, die damit realisierbar sind;
- generische (also für alle Prüfgegenstände grundlegende) Beschreibung
- erstellt durch die Swissmig-Arbeitsgruppe „DSsquare“
- abgeleitet aus der schweizerischen Schutzbedarfsanalyse (2016) für die ein iMS in der Prosumer- bzw. Datenmanager-Umgebung
- veröffentlicht durch VSE als [6]

Prüfschema:

- Beschreibung aller Schritte des Prüf- und Zertifizierungsverfahrens;
- Spezifikation der Rollen der Teilnehmer des Verfahrens
- Beschreibung der im Minimum benötigten Prüfumgebungen bei den Prüfstellen;

Prüfmethodologie

- Spezifikation der von den Prüfstellen zu untersuchenden Aspekte (CC Assurance Components, Prüfliste(n), etc.)
- Spezifikation der von den Herstellern für eine Prüfung zu liefernden Dokumentationen
- Spezifikation der von den Prüfstellen zu erstellenden Prüfdokumentation

Prüfliste:

- Als Teil der Prüfmethodologie:
  - Abbildung der Ergebnisse der SBA (Objekte und Bedrohungen) auf dedizierte Anforderungen
  - generische Zuordnung der Anforderungen an zu prüfende HK
  - generische Spezifikation der Anforderungen an unterstützende Systeme als Teile des iMS, welche keine HK sind
- Als Teil der Prüfdokumentation:
  - vom Hersteller zu erläuternde Aspekte hinsichtlich der Erfüllung der Anforderungen
  - von der Prüfstelle zu bewertende Erfüllung einzelner Anforderungen

Prüfprotokoll

- Dokumentation aller durchgeführten Prüfungen und deren Ergebnisse durch die Prüfstelle
- Indikation, unter welchen Prüfaspekten herstellerseitige Verbesserungen notwendig waren
- dient als Grundlage zur Zertifizierung

6.3 Liefergegenstände

Prüfgegenstand:
Diejenige Kombination von Einzelkomponenten aus [iMG; KS; HES], für welche eine Zertifizierung angestrebt wird

Herstellerdokumentation:
Vom Hersteller der Prüfstelle vorzulegende Dokumentation, die die IT-Sicherheitsaspekte, welche gemäss der Prüfliste durch die Prüfstelle untersucht werden, beschreibt

Prüfprotokoll:
Zusammenfassung der Prüfergebnisse der Prüfstelle gemäss Prüfliste für einen gegebenen Prüfgegenstand; dient als Grundlage für den anschliessenden Zertifizierungsprozess

7 Prüflistenmodule

Im Folgenden sind die Anforderungen aus [6] (Branchenempfehlung Strommarkt Schweiz Richtlinien und Anforderungen zur Durchführung einer Datensicherheitsprüfung, Anhang 1) nach Themen und Prüfobjekten strukturiert aufgeführt. Die Nummerierung der einzelnen Anforderungen ist diejenige aus [6].

- Übergreifende Anforderungen
  - Abschnitt 5.1 (wie in [6])
  - gelten für alle Hauptkomponenten (HK) eines intelligenten Messsystems (iMS)
  - umfassen in dieser Darstellung vier Blätter nummeriert mit römischen Zahlen
- Anforderungen an das intelligente Messgerät (iMG)
  - Abschnitt 5.2 (wie in [6])
  - umfassen in dieser Darstellung elf Blätter nummeriert mit römischen Zahlen
- Anforderungen an das Gateway (GW) als Kommunikationssystem (KS)
  - Abschnitt 5.3 (wie in [6])
  - umfassen in dieser Darstellung zehn Blätter nummeriert mit römischen Zahlen
- Anforderungen an den Datenkonzentrator (DC) als Kommunikationssystem (KS)
  - Abschnitt 5.4 (wie in [6])
  - umfassen in dieser Darstellung acht Blätter nummeriert mit römischen Zahlen
- Anforderungen an das Head End System (HES)
  - Abschnitt 5.5 (wie in [6])
  - umfassen in dieser Darstellung neun Blätter nummeriert mit römischen Zahlen
- Anforderungen hinsichtlich des lokalen Anschlusses einer Visualisierungsplattform (VP)
  - Abschnitt 5.6 (wie in [6])
  - umfassen in dieser Darstellung ein Blatt nummeriert mit römischen Zahlen
- Anforderungen an das Schlüsselmanagement (KM)
  - Abschnitt 6 (wie in [6])
  - umfassen in dieser Darstellung zwei Blätter nummeriert mit römischen Zahlen

5.1 Übergreifende Anforderungen

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 passwortgeschützter 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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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.				
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 Gesetzgebun-				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
gen zu berücksichtigen. Es dürfen nur anerkannte Verschlüsselungs-Verfahren und Schlüsselmindestlängen benutzt wer-den, 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				
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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforde-rung er-füllt j/n	Bemerkung
c) Für den Fall dass sicherheitskritische Schwachstellen während des Betriebs der HK bekannt werden, sind organisatorische Mas-snahmen zur Bekanntmachung, Dokumenta-tion und Behebung von Feh-lern zwischen Herstellern und Betreibern abzustimmen (Flaw Remediation, Schwachstellenbeseiti-gung).				
d) Sicherheit bei der Entwicklung und Unterstützung von Prozessen bzgl. Auslie-ferung und Inbetriebnahme (auditfähig zu do-kumentieren)				
e) Falls ein Hersteller Drittprodukte o-der Teilkomponenten in seine Produkte inte-griert, führt er im Sinne von a) Eingangskon-trollen durch.				
f) Falls eine sichere Entsorgung der Komponenten erforderlich ist, verpflichtet der Hersteller seine Kunden dazu, den Ver-bleib der Komponenten inklusive deren Ver-nichtung zu dokumentieren bzw. diese ohne fehlende Einzelkomponenten zurückzuge-ben.				

5.2 Anforderungen an das intelligente Messgerät (iMG)

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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. 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				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 (Messgeräte-richtlinie 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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 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 iMG 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 den metrologischen Teil oder 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.				
5.2.2.2 Schnittstelle KS3				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 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“ beim Datenmanager einen nurlesenden Zugriff auf die zur Fernübertragung vorgesehenen Zähldaten und insbesondere auf die netzrelevanten Daten.				
f) 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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 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.				
5.2.2.3 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				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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.				
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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 über das HES und von einem berechtigten Benutzer oder durch Regeln, die im iMG hinterlegt sind, ausgelöst werden. Ebenso muss für das Zurücksetzen eines ausgelösten Breakers 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 über das HES und von einem berechtigten Benutzer oder durch Regeln, die im iMG hinterlegt sind, ausgelöst werden.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforde-rung er-füllt j/n	Bemerkung
b) Mehrere Steuer-Relais können mit-tels eines Broadcast angesteuert werden.				

5.3 Anforderungen an das Gateway (GW) als Kommunikationssystem (KS)

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 Daten-manager erzwingt, bevor das Gateway 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.				
5.3.1.2 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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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. Die Hersteller sind gehalten, den Umfang der zu loggenden Daten den Ansprüchen der Betreiber anzupassen.				
5.3.1.6 Firmware Update				
a) Nur bei einem Gerät, das im vorgesehenen Betriebsmodus arbeitet, kann ein				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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.				
5.3.2 Schnittstellen				
5.3.2.1 Schnittstelle KS0				
a) Für den Zugriff auf diese Schnittstelle sind mindestens die Benutzerrollen Gateway-Administrator sowie Zählerableser gemäss den entsprechenden Zugriffsrechten verfügbar.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 Gateway 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.				
5.3.2.2 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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
c) Für den Zugriff über diese Schnittstelle sind mindestens die Benutzerrollen Gateway-Administrator sowie Operator 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“ beim Datenmanager einen nurlesenden Zugriff auf die zur Fernübertragung vorgesehenen Zähldaten.				
g) 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.				
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 die anderen Schnittstellen.				
j) Unbefugte Zugriffsversuche und andere Störungen lösen einen Alarm an den				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforde-rung er-füllt j/n	Bemerkung
Datenmanager aus, und diese Ereignisse werden in die Log-Daten übernommen.				
5.3.2.3 Schnittstelle KS2				
a) Für den Zugriff auf diese Schnitt-stelle ist mindestens die Benutzerrolle Pro-sumer gemäss den entsprechenden Zugriffs-rechten verfügbar.				
b) Falls das Gateway Zähldaten ver-schiedener Kunden bearbeitet, muss seine Datenhaltung mandantentauglich sein und darf verschiedenen Kunden in der Benutzer-rolle „Prosumer lokal“ ausschliesslich Zugriff auf ihre entsprechenden Daten erlauben.				
c) Die Authentifizierung erfolgt minde-stens 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 Ver-bindung auf andere Schnittstellen des Gate-way 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 Schnittstel-len.				
h) Unbefugte Zugriffsversuche und an-dere Störungen lösen einen Alarm an das				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 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.				
5.3.3.2 Zeiteinstellungen				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforde-rung er-füllt j/n	Bemerkung
a) Für den Zugriff auf dieses Objekt über die Schnittstelle KS0 werden die Benut-zerrollen Gateway-Administrator oder – falls vorhanden – Zählerableser gemäss den ent-sprechenden Zugriffsrechten verwendet.				
b) Die Authentifizierung erfolgt mindes-tens über Benutzername und Passwort.				
c) Die Änderung der Zeiteinstellung im Gateway löst eine Meldung an den Daten-manager aus und wird in die Log-Daten übernommen.				
d) Unbefugte Zugriffsversuche und an-dere Störungen lösen einen Alarm an das MDM System aus, und diese Ereignisse wer-den in die Log-Daten übernommen.				

5.4 Anforderungen an den Datenkonzentrator (DC) als Kommunikationssystem (KS)

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 aus-				

gegeben, 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. 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 vorher-gehenden 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				
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 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 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 Head End System (HES)

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
Generelle Anforderungen an die externen Schnittstellen des HES (KONKRETISIERT IN 5.5.2)				
a) Die den Benutzer-Rollen beim Datenmanager angebotenen externen Schnittstellen erfüllen die Sicherheitsanforderungen bezüglich Benutzerrollen auf demselben Niveau wie die Schnittstellen der anderen Hauptkomponenten.				
b) Die Schnittstelle, die zur Kommunikation mit anderen Hauptkomponenten dient, sowie die Datenübertragung über diese Verbindung müssen dasselbe Sicherheitsniveau wie das der Hauptkomponenten haben.				
c) Die Schnittstellen des HES •zur lokalen und entfernten Systemkonfiguration, •zur automatisierten Datenübertragung vom iMS zum Datenmanager, •für Sonstiges, müssen dasselbe Sicherheitsniveau der Schnittstellen der Hauptkomponenten aufweisen.				
5.5.1 Anforderungen an den sicheren Betrieb				
5.5.1.1 Auslieferung und Erst-Inbetriebnahme				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
a) 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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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. Die Hersteller sind gehalten, den Umfang der zu loggenden Daten den Ansprüchen der Betreiber anzupassen.				
5.5.1.7 Firmware Update				
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				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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) Da die Ausprägung der Architektur des MDM je nach Hersteller sehr unterschiedlich ist, sind die folgenden Punkte als **Empfehlung** zu verstehen. 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. Dem entsprechend sind für den Zugriff auf diese Schnittstelle keine Benutzerrollen definiert. 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				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 AUSSCHLIESSLICH das HES.				
b) iMG-Administrator und DC- (bzw. Gateway-)Administrator konfigurieren AUSSCHLIESSLICH 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				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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 heraus 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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforde-rung er-füllt j/n	Bemerkung
b) Dies darf nicht zu einer Kompromit-tierung des Sicherheitsniveaus des HES füh-ren.				

5.6 Anforderungen hinsichtlich des lokalen Anschlusses einer Visualisierungsplattform (VP)

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
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.				

6 Anforderungen an das Schlüsselmanagement (KM)

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
a) Das Schlüsselmanagement deckt den gesamten Lebenszyklus aller kryptografischen Schlüssel im Gesamtsystem eines iMS 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.				

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforde-rung er-füllt j/n	Bemerkung
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.				