Branchenempfehlung Strommarkt Schweiz

Richtlinien für die Datensicherheit von intelligenten Messsystemen

für Zertifizierung und Betrieb von intelligenten Messsysteme

RL-DSP – CH, Ausgabe 2018

swissmig

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

VSE AES

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 der Erstausgabe (AG Datenschutz/Datensicherheit bei Smart Metering)

Maurus Bachmann	VSGS	
Francis Beyeler	VSE	
Andreas Eilingsfeld	EWZ	
Roman Gmür	Enpuls AG	
Stéphane Henry	Romande Energie SA	
Patrick Inderkum,	e-lynx (ASUT)	
Roland Kiefer	Stadtwerk Winterthur	
Andreas Kölliker	InfoGuard AG	AG-Leiter
Andy Kreuzer	IDS Schweiz AG (swissmig)	
Thomas Mettler	Arbon Energie AG	
Hendrik la Roi	VSE	Sekretär
Tom Ruef	BKW Energie AG	
Yves Senn	Encontrol AG	
David Spale	Avectris AG	
Michael Staudinger	Landis+Gyr AG (ISSS)	

Beratung
Infoguard AG, Baar
VZsecurITy, Laupersdorf

Verantwortung Kommission
Für die Pflege und die Weiterentwicklung des Dokuments zeichnet die VSE-Kommission Energiedaten in Zusammenarbeit mit den Herstellern verantwortlich.

Dieses Dokument ist ein Branchendokument zum Strommarkt. Es gilt als Richtlinie im Sinne von Art. 27 Abs. 4 Stromversorgungsverordnung.

Chronologie

Januar 2016	Arbeitsaufnahme AG Datensicherheit bei Smart Metering
Juni 2016	Veröffentlichung der Schutzbedarfsanalyse des BFE
November 2017	Verabschiedung der Verordnungsrevision zur Energiestrategie 2050 durch den Bundesrat mit neuem Art. 8b StromVV «Datensicherheitsprüfung»
April 2018	Fertigstellung des Dokuments
Mai/Juni 2018	Vernehmlassung in der Branche
24. Oktober 2018	Genehmigung durch den VSE-Vorstand

Das Dokument wurde unter Einbezug und Mithilfe von VSE, Branchenvertretern und Herstellern erarbeitet.

Der VSE verabschiedete das Dokument am 24.10.2018.

Druckschrift Nr. 1045 d, Ausgabe 2018

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungen und Definitionen

BFE	Bundesamt für Energie
CRM	Customer Relationship Management.
DC	Datenkonzentrator
EDM	Energiedaten-Management
EVU	Energieversorgungsunternehmen
HES	Head End System
IKT	Informations- und Kommunikationstechnologie
iMG	intelligentes Messgerät. Ein elektronischer Elektrizitätszähler gemäss StromVV, Art 8a
iMS	intelligentes Messsystem
MDM	Meter Data Management
METAS	Eidgenössisches Institut für Metrologie
SBA	Schutzbedarfsanalyse
SW	Software
VNB	Verteilnetzbetreiber
VSE	Verband Schweizerischer Elektrizitätsunternehmen
WAN	Wide Area Network
ZDVS	Zähldatenverarbeitungssystem. Zähldatenverarbeitungssysteme bieten Funktionen zur Verwaltung der Messgeräte oder der Bearbeitung der von den Messgeräten aufgenommen Rohdaten wie z. B. Geräteparametrierung, Geräteverwaltung oder Zeitreihenverwaltung.

Quellenverzeichnis

	Titel	Herausgeber
[1]	Stromversorgungsverordnung (StromVV) vom 14. März 2008 (mit Anpassungen für den 1.1.2018)	Bund
[2]	Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz; 11/2014	BFE
[3]	Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern; 10/2015	BFE
[4]	Studie «Schutzbedarfsanalyse Smart Metering in der Schweiz» vom Juni 2016	BFE

Vorwort

Beim vorliegenden Dokument handelt es sich um ein Branchendokument des VSE. Es ist Teil eines umfassenden Regelwerkes für die Elektrizitätsversorgung im offenen Strommarkt. Branchendokumente beinhalten branchenweit anerkannte Richtlinien und Empfehlungen zur Nutzung der Strommärkte und der Organisation des Energiegeschäftes, und erfüllen damit die Vorgabe des Stromversorgungsgesetzes (StromVG) sowie der Stromversorgungsverordnung (StromVV) an die Energieversorgungsunternehmen (EVU).

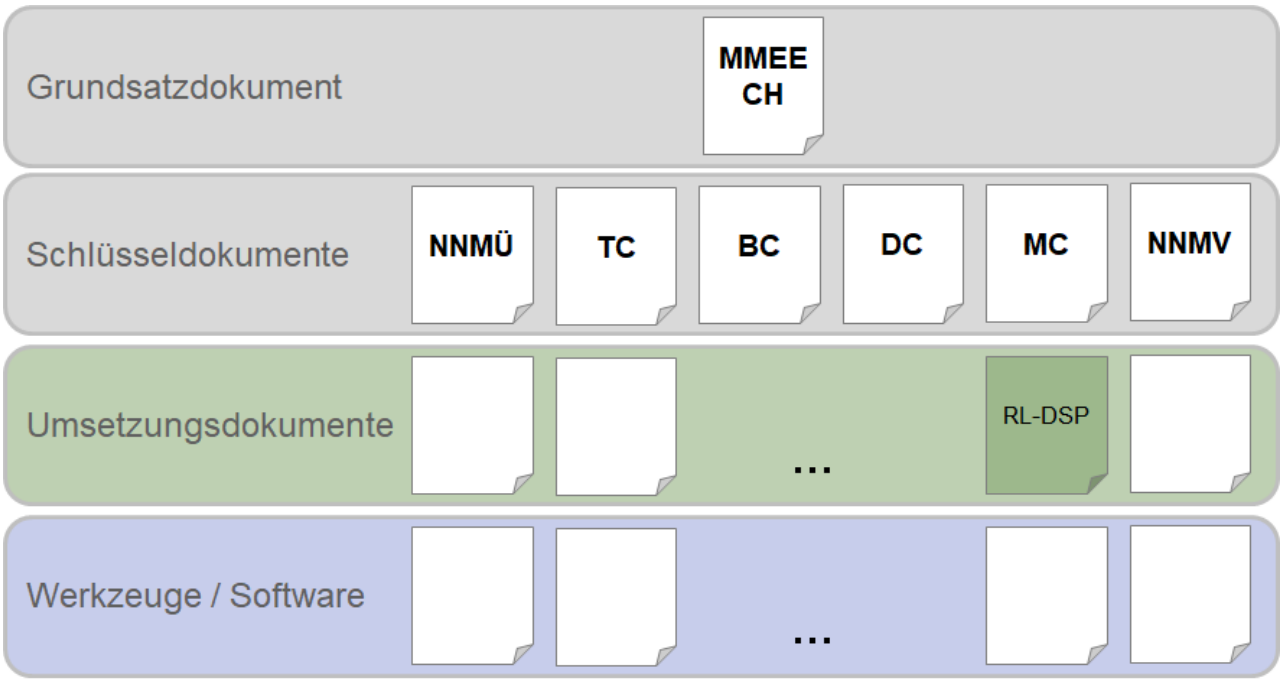
Branchendokumente werden von Branchenexperten im Sinne des Subsidiaritätsprinzips ausgearbeitet, regelmässig aktualisiert und erweitert. Bei den Bestimmungen, welche als Richtlinien im Sinne des StromVV gelten, handelt es sich um Selbstregulierungsnormen.

Die Dokumente sind hierarchisch in vier unterschiedliche Stufen gegliedert

- Grundsatzdokument: Marktmodell elektrische Energie (MMEE)
- Schlüsseldokumente
- Umsetzungsdokumente
- Werkzeuge/Software

Beim vorliegenden Dokument «Richtlinien für die Datensicherheit von intelligenten Messsystemen» handelt es sich um ein Umsetzungsdokument.

Dokumentstruktur



1. Einleitung

1.1 Zweck des Dokumentes

(1) Das vorliegende Branchendokument legt auf der Basis der Schutzbedarfsanalyse (SBA) des BFE [4] Richtlinien und Anforderungen zur Durchführung einer Datensicherheitsprüfung für intelligente Messsysteme bei Endverbrauchern fest.

(2) Das Anliegen der Richtlinien ist, anhand der Risikobewertung in der SBA, prüfbare Sicherheitsanforderungen zu definieren, die eine geeignete Detailtiefe aufweisen und bei einer Überprüfung reproduzierbare Ergebnisse ermöglichen.

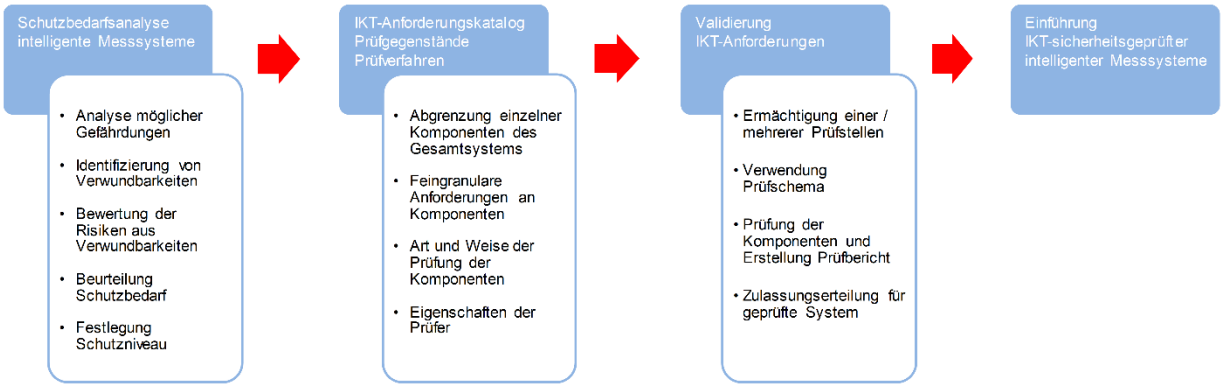


Abbildung 1: Prozessschritte zur Gewährleistung der Datensicherheit intelligenter Messsysteme beim Endverbraucher (Quelle: Ref. [3], Abbildung 8)

(3) In Abbildung 1 sind die wichtigen Prozessschritte zur Gewährleistung der Datensicherheit intelligenter Messsysteme aufgezeigt:

- Schutzbedarfsanalyse (SBA)
- Definition Anforderungskatalog (dieses Dokument und seine Anhänge)
- Validierung Sicherheitsanforderungen (durch das METAS)
- Einführung intelligentes Messsystem (durch den Verteilnetzbetreiber)

(4) Zusätzlich zu den Anforderungen für die Durchführung der Datensicherheitsprüfung des iMS, enthält das Branchendokument Empfehlungen, wie ein iMS sicher betrieben werden kann.

1.2 Strukturierung der Dokumente

(1) Das Dokument besteht aus einem Richtliniendokument in dem der Gesamtprozess, sowie die Rollen und Verantwortungen der einzelnen Akteure festgelegt sind. Kapitel 3 gibt eine Übersicht über die Richtlinien für die Zertifizierung eines iMS. Kapitel 4 eine Übersicht über die Empfehlungen für den sicheren Betrieb eines iMS. Die Sicherheitsanforderungen sind in zwei Anhängen zum Dokument beschrieben.

- Anhang 1 «Zertifizierungsanforderungen an iMS für die Datensicherheit» mit Anforderungen für die prüfbare Sicherheit der Komponenten eines iMS (für die Datensicherheitsprüfung gemäss StromVV, Art. 8b)
- Anhang 2 «Betriebliche Anforderungen an iMS für die Datensicherheit» mit Anforderungen und Empfehlungen für Netzbetreiber und Dienstleister zum Betreiben eines iMS. Dieser Anhang ist, unabhängig von der Datensicherheitsprüfung gemäss Art 8b StromVV, als Branchenempfehlung zu verstehen, wie der VNB seine Verantwortung für den sicheren Betrieb eines iMS wahrnehmen kann.

2. Rollen

(1) **Hersteller**: Die Rolle «Hersteller» beinhaltet die Soft- und Hardwarehersteller von Komponenten von intelligenten Messsystemen. Sie liefern Produkte für die iMS aus. Sie sind dafür verantwortlich, die Komponenten des iMS vor deren Markteinführung prüfen zu lassen. Zudem stellen sie sicher, dass die Geräte während der Betriebsphase, z.B. beim Auftreten von neuen Bedrohungen, mittels Software- und Firmware-Updates weiterhin sicher betrieben werden können.

(2) **Verteilnetzbetreiber:** Der Verteilnetzbetreiber ist für die Erbringung des Messwesens (Messstellenbetrieb und Messdienstleistung) verantwortlich. Er ist dafür zuständig, dass nur geprüfte Komponenten zum Einsatz kommen. Zudem ist er für den sicheren Betrieb des iMS verantwortlich. Die Anforderungen für den sicheren Betrieb eines iMS sind für die Rolle des Datenmanagers formuliert. Der Verteilnetzbetreiber kann das Messwesen, in der Rolle des Datenmanagers, selber erbringen oder die entsprechenden Aufgaben an Dritte auslagern.

(3) **Datenmanager**: In der SBA [4] werden unter dem Begriff «Datenmanager» die Rollen «Messstellenbetreiber» und «Messdienstleister» zusammengefasst. Der Messstellenbetreiber ist in der Regel für die Supportprozesse, wie z. B. den Einbau und Betrieb sowie Eichung und Wartung des iMG, verantwortlich. Der Messdienstleister übernimmt üblicherweise das Ab- und Auslesen der Messeinrichtung sowie andere Leistungen für den Endverbraucher, wie z.B. Weiterbearbeitung der Daten, Abrechnung, Kundenbetreuung oder -beratung.

(4) **Prosumer / Endverbraucher**: Der Prosumer ist sowohl Einspeiser als auch Endverbraucher im Stromnetz und befindet sich normalerweise in der Netzebene 5 oder 7, in seltenen Fällen auch in der Netzebene 3.

(5) **Prüfstelle**: Die Prüfstelle ist für die Validierung der Sicherheitsanforderungen verantwortlich. Sie prüft, ob die Datensicherheitsanforderungen vollständig und wirksam umgesetzt worden sind. Die Prüfstelle übermittelt nach Abschluss der Prüfung die Prüfergebnisse in Form eines Prüfberichtes an die Hersteller. In Art. 8b Abs. 3 des StromVV wird das METAS als einzige Prüfstelle erwähnt. Es kann Dritte mit der Erfüllung dieser Aufgabe oder Teilen davon, betrauen.

(6) **Kontrollstelle**: Die Kontrollstelle vergibt an den Hersteller, nach Bewertung des Verfahrens resp. des Prüfberichts, eine produktgebundene Zulassung zum Betrieb – eine sogenannte Zulassungsermächtigung – inklusive Zulassungszeichen (Zertifikat). Das METAS ist gemäss der Formulierung in Art. 8b Abs. 3 des StromVV verantwortlich für die Rolle der Kontrollstelle.

(7) Weitere Marktrollen sind im Dokument «MMEE – CH» aufgelistet.

3. Richtlinien für die Datensicherheitsprüfung von iMS

(1) Im Art 8b des StromVV vom 1. November 2017 wird bestimmt, dass nur iMS eingesetzt werden dürfen, die vorgängig eine Datensicherheitsprüfung durchlaufen haben. Das vorliegende Kapitel beschreibt «die zu prüfende Elemente» (Kapitel 3.1), «die Anforderungen an diese» (Anhang 1), sowie die «Art und Weise der Prüfung» (Kapitel 3.3). In Kapitel 3.2 gibt es eine Übersicht über Ablauf und Rollen der Datensicherheitsprüfung.

3.1 Gültigkeitsbereich des iMS für die Datensicherheitsprüfung

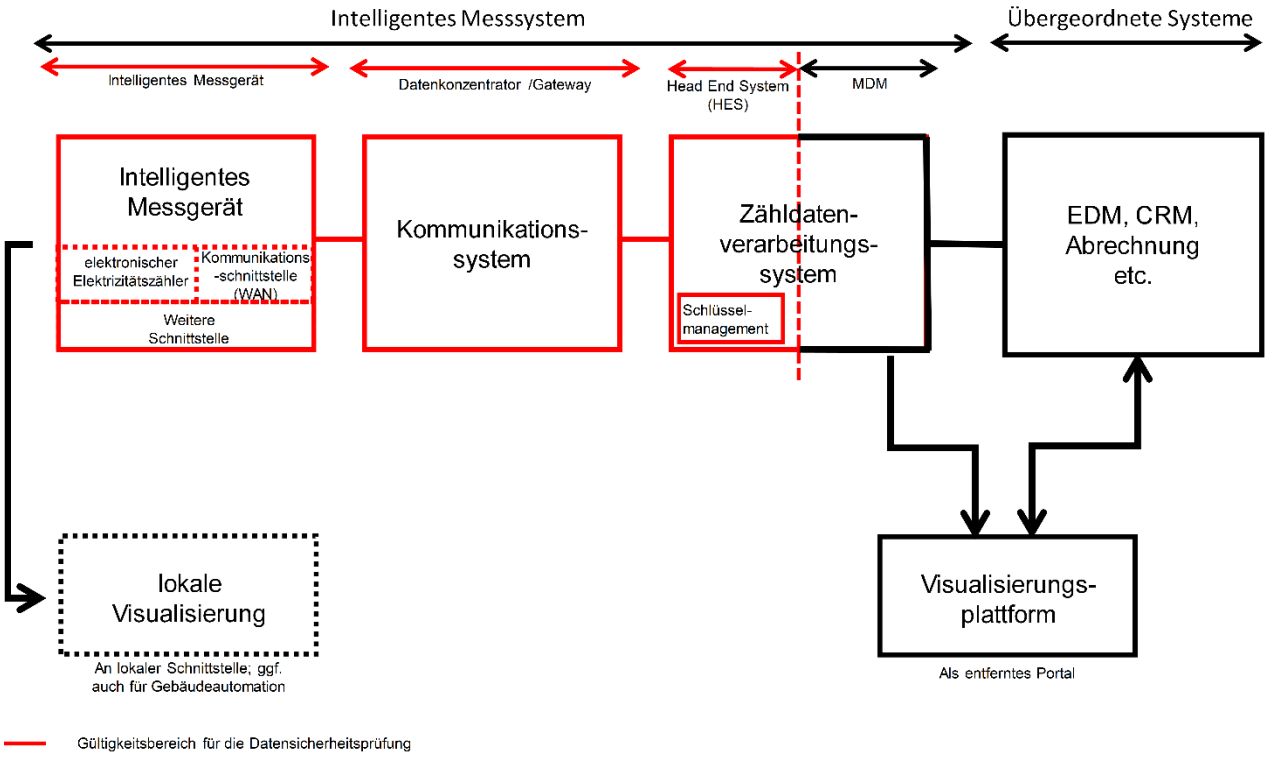


Abbildung 2: Gültigkeitsbereich des iMS für die Datensicherheitsprüfung

(1) Der Gültigkeitsbereich für die Datensicherheitsprüfung des iMS ist in Abbildung 2 (in rot) dargestellt. Sie umfasst drei Hauptkomponenten: das iMG, das Kommunikationssystem und das HES.

(2) Ausgenommen vom Gültigkeitsbereich der Datensicherheitsprüfung sind, wegen ihrer unterschiedlichen Umsetzung, sowohl die lokale Visualisierung, sowie alle dem HES nachgelagerten Systeme (MDM, ZDVS, EDM, CRM, Abrechnungssystem, Visualisierungsplattform usw.). Aus dem gleichen Grund ist die Schnittstelle zwischen HES und MDM nicht Bestandteil der Datensicherheitsprüfung. Die Schnittstelle zur lokalen Visualisierung am iMG ist aber im Gültigkeitsbereich eingeschlossen.

3.2 Ablauf der Datensicherheitsprüfung – Schritt für Schritt

(1) Die folgenden Schritte[1] beschreiben die Abwicklung einer Datensicherheitsprüfung, die in der Abbildung 3 veranschaulicht wird. Die Beschreibung dieses Ablaufs basiert auf der oben ausgeführten Rollenverteilung der jeweiligen Akteure, konkretisiert aber ihre Aufgaben wo nötig.

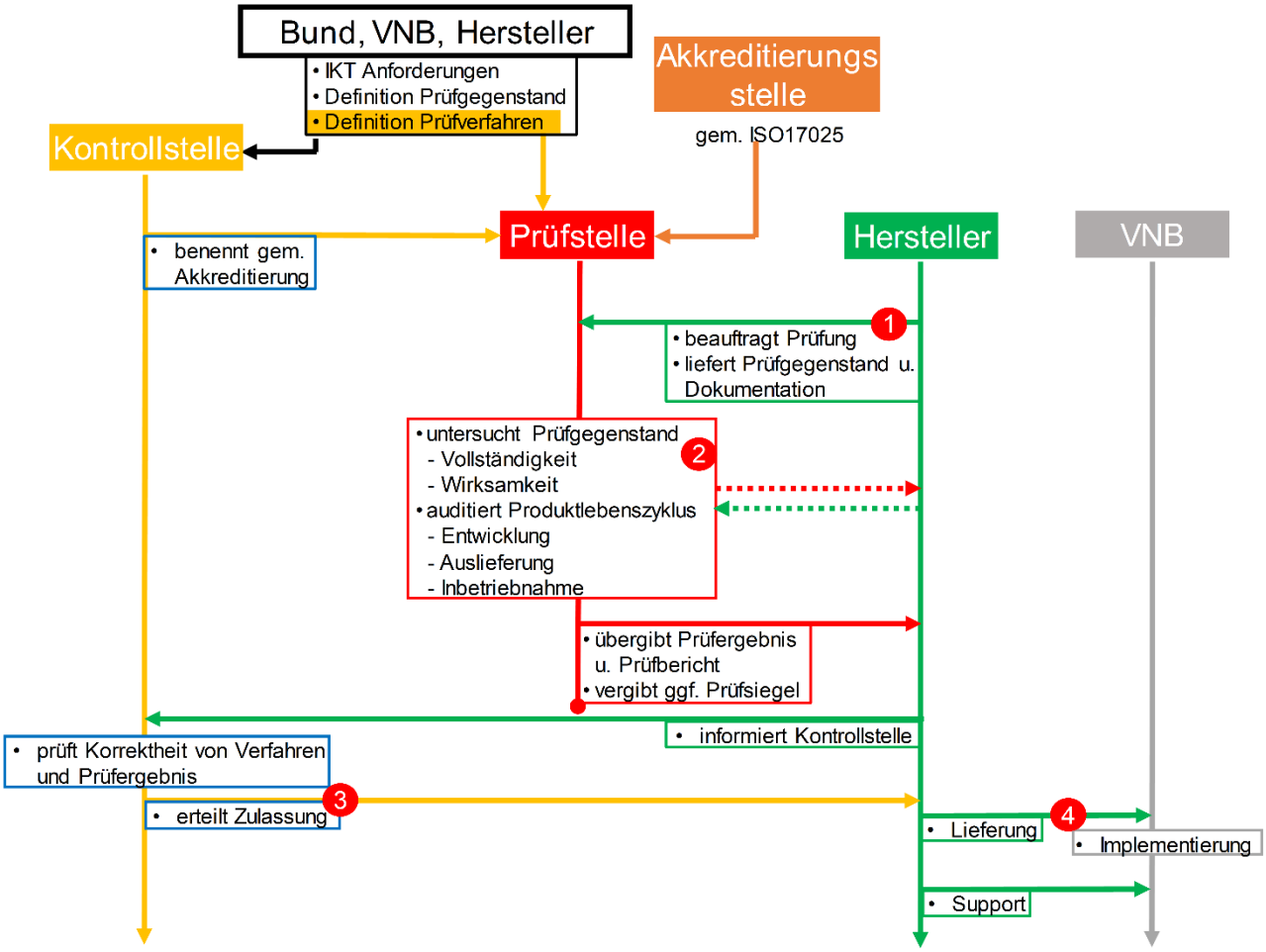


Abbildung 3: Ablauf der IKT-Sicherheitsvalidierung (Quelle: Ref. [3], Abbildung 10)

Schritt 1: Prüfauftrag des Herstellers für Produkt an Prüfstelle

(2) Eine akkreditierte Prüfstelle wird vom Hersteller (oder z.B. vom Betreiber, der als «Sponsor» für die Kostenübernahme der Prüfung auftritt) beauftragt, ein iMS hinsichtlich Datensicherheitsprüfung und auf Basis des bekannten Anforderungskataloges, zu untersuchen. Prüfgegenstände sind Teil eines iMS; ihre erforderlichen Sicherheitsfunktionalitäten werden detailliert im Anforderungskatalog (siehe Anhang 1: «Zertifizierungsanforderungen an iMS für die Datensicherheit») festgelegt.
Der Hersteller stellt sein Produkt, die dazu gehörende und notwendige technische Dokumentation sowie weitere Informationen über sicherheitsrelevante Prozesse (gem. Anforderungskatalog) der Prüfstelle zur Verfügung. Zu diesem Lieferumfang gehören u.a. die Produktidentifikation (z.B. Seriennummer; Versionsstand aus einem Konfigurationskontrollsystem etc.), die Produktdokumentation so-

[1] In der originalen Abbildung in Ref. [3] ist zusätzlich der Schritt 5 «Monitoring des Betriebs und Stichproben» abgebildet. Für die Prüfung des Betriebs gibt es derzeit keine gesetzliche Grundlage. Deshalb wurde sie in dieser Abbildung weggelassen.

wie alle, die IKT-Sicherheitsfunktionalitäten umfassenden technischen Spezifikationen. Darüber hinaus werden die sicherheitsrelevanten Prozesse im Lebenszyklus eines Prüfgegenstandes vom Hersteller für die Prüfstelle dokumentiert (Sicherheit in der Entwicklung, bei der Auslieferung, bei der Inbetriebnahme, Updatefunktionalitäten).

Schritt 2: Produkt an Prüfstelle

(3) Die Prüfung läuft – ggf. interaktiv – zwischen Prüfstelle und Hersteller ab. Die Prüfschritte, die im Prüfschema für die einzelnen Prüfgegenstände aufgeführt sind, werden Schritt für Schritt, anhand der vom Hersteller gelieferten Unterlagen ausgeführt, und die im Anforderungskatalog definierten Sicherheitsfunktionalitäten überprüft. Während der Prüfung unterstützt der Hersteller die Prüfstelle durch zusätzliche Informationen, welche in begründeten Fällen von der Prüfstelle angefordert werden können. Die Prüfstelle ermittelt so die Vollständigkeit und Wirksamkeit der Sicherheitsfunktionalitäten. Zudem auditiert die Prüfstelle den Produktlebenszyklus dahingehend, dass sie die Entwicklung, Auslieferung, Inbetriebnahme und Updatefunktionalitäten soweit möglich überprüft. Dies kann, z. B. auf Basis dokumentierter Prozesse, erfolgen. Die Prüfung kann bei festgestellten Mängeln auch Revisionszyklen des Prüfgegenstandes durch den Hersteller zur Behebung zulassen. Die Prüfstelle übermittelt nach Abschluss der Prüfung das Ergebnis in Form eines Prüfberichtes an den Hersteller.

Schritt 3: Prüfung durch Kontrollstelle und Zulassungsermächtigung

(4) Die Kontrollstelle erhält den Prüfbericht vom Hersteller des iMS und nimmt das betreffende Produkt in ein Verzeichnis auf. Sie prüft den Bericht hinsichtlich der Korrektheit des Verfahrens und der Ergebnisse. Bei Unregelmässigkeiten oder defizitären Prüfungen veranlasst sie Nachbesserungen oder Prüfungen bei einer anderen Prüfstelle. Die Kontrollstelle vergibt nach Bewertung des Verfahrens, resp. des Prüfberichts, eine produktgebundene Zulassung zum Betrieb – eine sogenannte Zulassungsermächtigung – inklusive Zulassungszeichen.

Schritt 4: Produktlieferung und Inbetriebnahme

(5) Der Hersteller liefert ein von der Kontrollstelle zugelassenes Produkt an den Betreiber, der es gemäss den sicherheitsrelevanten Vorgaben aus der Datensicherheitsprüfung in seiner Betriebsumgebung installiert. Das Prüfsiegel und die Zulassung der Kontrollstelle erlauben Transparenz für die vom Regulator durchgeführte Kostenprüfung, und sichern so die Anrechenbarkeit.

3.3 Art und Weise der Datensicherheitsprüfung

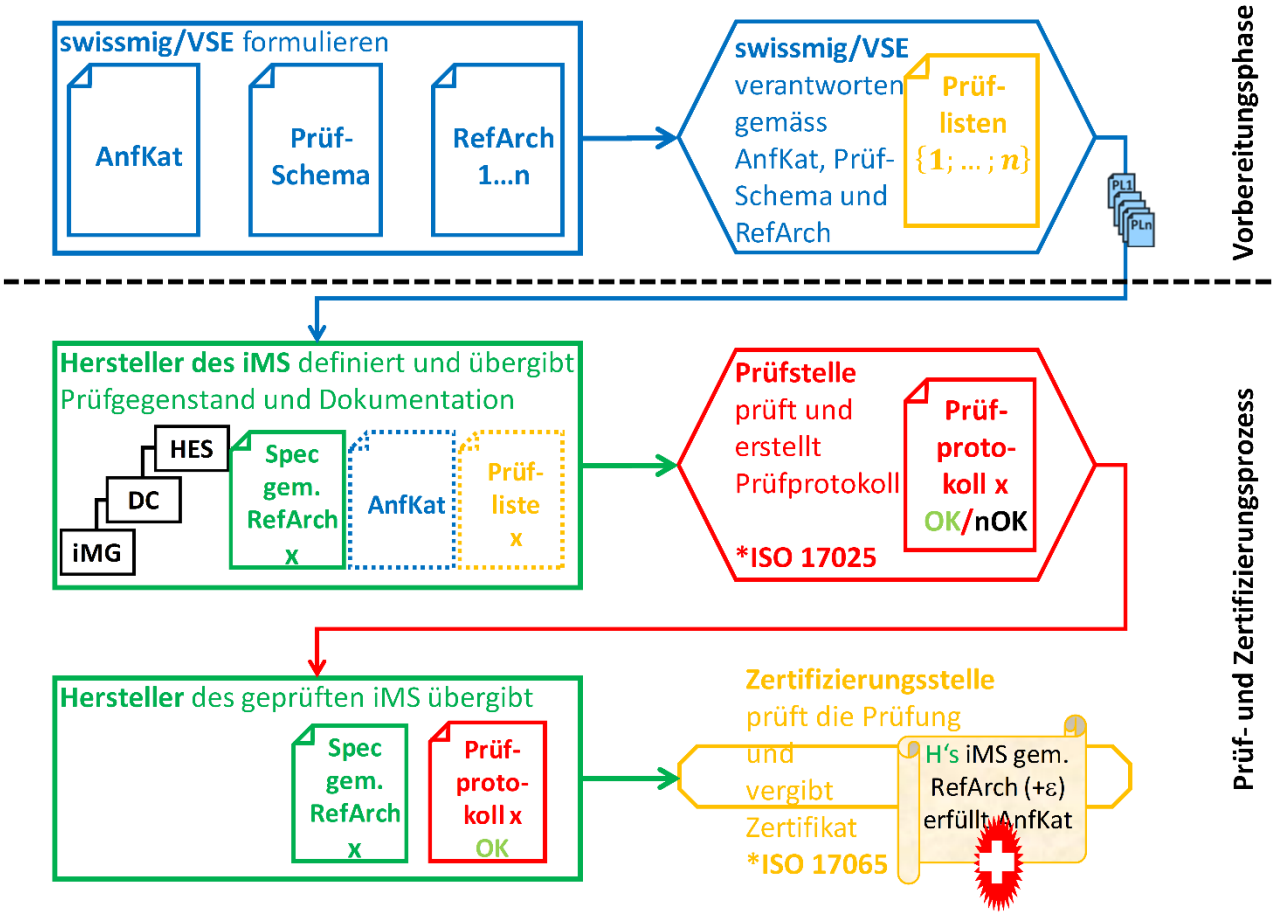


Abbildung 4: Prüfschema mit den Verantwortungsbereichen der involvierten Akteure

(1) Die Datensicherheitsprüfung basiert auf diesen Richtlinien, die aus einem Anforderungskatalog, dem Prüfschema und den Prüflisten besteht. Mit Hilfe dieser Vorgaben legt der Hersteller der Prüfstelle dar, wie er die Anforderungen mit seinen Produkten umgesetzt hat.

(2) Die Prüfstelle prüft die vorgelegten Produkte und fasst ihre Befunde in einem Prüfprotokoll zusammen. Nach bestandener Datensicherheitsprüfung, vergibt die Kontrollstelle die Produktzulassung aufgrund des Prüfprotokolls.

3.3.1 Interoperabilität bei der Datensicherheitsprüfung

(1) Alle Elemente eines iMS müssen nach StromVV, Art 8b, eine Datensicherheitsprüfung bestehen und zertifiziert sein. Die Zertifizierung bezüglich Datensicherheit erfolgt auf der Basis einzelner Elemente. Bei Hinzufügung eines neuen Elementes in einem iMS, erfordert dies die Zertifizierung des neuen Elements. Sicherheitsrelevante Fehlerkorrekturen an bereits zertifizierten Elementen erfordern spätestens nach einem (1) Jahr eine Nachzertifizierung. Die Nachzertifizierung ist auf Stufe Hersteller durchzuführen. Somit erfüllt ein iMS bestehend aus zertifizierten Elementen, welches durch ein neues, zertifiziertes Element (eines anderen Herstellers) erweitert wird weiterhin Art 8b der StromVV (Datensicherheitsprüfung).

4. Der sichere Betrieb eines iMS

(1) Der Einsatz von sicheren und geprüften Schutzobjekten genügt nicht, um den Risiken der SBA zu begegnen. Die Datenmanager müssen zusätzlich sicherstellen, dass die Geräte nach der Inbetriebnahme so betrieben werden, wie es in der Datensicherheitsprüfung beabsichtigt wurde.
Anhang 2: «Betriebliche Anforderungen an iMS für die Datensicherheit» enthält dazu Anforderungen, die sicherstellen, dass auch beim Betreiben eines iMS die Datensicherheit gewährleistet werden kann.

(2) Kapitel 4.1 zeigt welche Systemkomponenten beim Betreiben eines iMS involviert sind. Für diesen Gültigkeitsbereich ist die Datensicherheit zu gewährleisten.

4.1 Gültigkeitsbereich für den sicheren Betrieb eines iMS

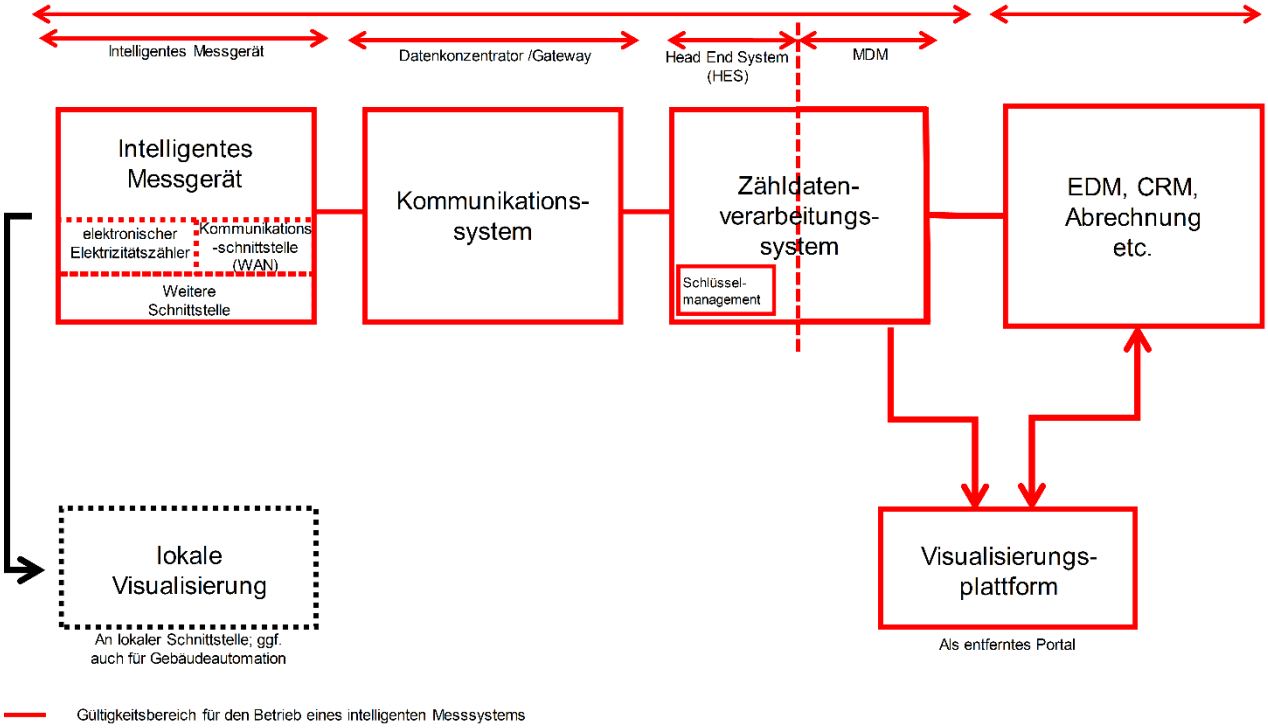


Abbildung 5: Gültigkeitsbereich für den sicheren Betrieb eines iMS

(1) Abbildung 5 zeigt (in rot) den Gültigkeitsbereich für den Betrieb eines iMS. Sie umfasst neben den Hauptkomponenten iMG, Kommunikationssystem und HES der Datensicherheitsprüfung, auch alle dem HES nachgelagerten Systeme (MDM, ZDVS, EDM, CRM, Abrechnungssystem, Visualisierungsplattform usw.). Die Schnittstellen zur lokalen Visualisierung am iMG und zwischen HES und MDM sind eingeschlossen. Die lokale Visualisierung selber ist nicht im Einflussbereich des Datenmanagers und deshalb vom Gültigkeitsbereich ausgenommen.

4.2 Sicherheitsprüfung für den Betrieb eines iMS

(1) Die Anforderungen im Anhang 2: «Betriebliche Anforderungen an iMS für die Datensicherheit» sind sehr umfassend: Sie enthalten z.B. Anforderungen zum Asset-Management, zur Zugriffskontrolle, zur Kryptographie, zur Betriebs- und Kommunikationssicherheit, zum Management von sicherheitsrelevanten Vorfällen, zur Entwicklung und Wartung und zur Regelkonformität (Compliance). Die Auswahl der Anforderungen kann aufgrund der eigenen Risikobewertung des Datenmanagers erfolgen.

(2) Der Anforderungskatalog enthält Anforderungen und Empfehlungen, wie ein iMS sicher betrieben werden kann. Die Einhaltung der Anforderungen stellt sicher, dass der Datenmanager das iMS so betreibt, wie dies bei der Durchführung der Datensicherheitsprüfung gefordert wird.

(3) Die Umsetzung der Anforderungen unterstützt den Datenmanager in seiner Verantwortung für den sicheren Betrieb eines iMS. Mit einem periodischen Datensicherheitsaudit auf der Basis des vorgelegten Anforderungskatalogs kann der Datenmanager die Datensicherheit des Anlagenbetriebs zudem überprüfen und stetig verbessern. Die Durchführung von Sicherheitsaudits wird deshalb empfohlen.

5. Anhang 1: Zertifizierungsanforderungen an iMS für die Datensicherheit

6. Anhang 2: Betriebliche Anforderungen an iMS für die Datensicherheit