IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
Fragen und ergänzende Anmerkungen	Fragen und ergänzende Anmerkungen		Die Marktpartner interagieren mit dem MV und BA über spezifizierte Schnittstellen zur Umsetzung der Marktprozesse. Wie sieht die Interaktion der sonstigen Rollen mit dem System aus? - Gibt es Benutzer-Schnittstellen (User-Interface – UI) für Verwaltungspersonal mit unterschiedlichen Zugriffsrechten? - Welche Funktionen und welcher Datenzugriff soll über diese UIs angeboten werden? - Wenn ja, welche Anforderungen bestehn an diese UIs (UI Guidelines, Accessibility, etc.)?		decarbon1ze GmbH
Fragen und ergänzende Anmerkungen	Fragen und ergänzende Anmerkungen		Wenn die regulierten Marktprozesse über marktrollenspezifische REST-APIs bereitgestellt werden, so ist es kein großer Schritt mehr, für diese APIs jeweils einfache UIs anzubieten. Z.B. zur Inspektion der Daten auf dem Hub für Sachbearbeiter:innen der jeweiligen Marktrolle, und ggfs sogar zum abarbeiten einzelner Prozessschritte. Ist dies geplant?		decarbon1ze GmbH
Fragen und ergänzende Anmerkungen	Fragen und ergänzende Anmerkungen	Umsetzung DSGVO	Unvereinbarkeit mit DSGVO	1.Datenschutz Der beabsichtigte Systemwechsel ist aus datenschutzrechtlicher Sicht nicht zu befürworten. So sind die Anforderungen an einen Schutz personenbezogener Informationen durch einen zentralisierten Hub weder notwendig noch geeignet, um die nach § 52 Absatz 3 MsbG verpflichtend vorgesehene Pseudonymisierung von Last- und Zählerstandsgängen zu gewährleisten; Die Anforderungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit werden in den Erläuterungen der zentralen Prozessvorgaben im Rahmen der Konsultation vom 26.09.2025 unvollständig und damit fehlerhaft wiedergegeben. Es wird zitiert,“ es könne eine alphanumerische Bezeichnung des Ortes der Messung, der Entnahme oder der Einspeisung von Energie genutzt werden, die auch die Voraussetzungen der DSGVO erfüllt. Die Malo ID und MeloID könnten grundsätzlich als solche alphanumerischen Kennzeichen betrachtet werden, wenn die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Betroffenen Person zugeordnet werden können.“	Hausheld AG

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				Zwingende Voraussetzung für eine datenschutzgerechte Verarbeitung bei Pseudonymisierung durch MaLo und MelO bilden damit technisch organisatorische Maßnahmen im Rahmen einer differenzierten Behandlung. Diese Strukturen sind bei den verantwortlichen Akteuren, den Netzbetreibern und Messstellenbetreibern, GWAs fest implementiert und zertifiziert. Offen und kritisch bleibt dies zukünftig. Die BNetzA führt aus: „ Es ist beabsichtigt, dass der MaBIS-Hub durch die vier ÜNB gemeinschaftlich in geeigneter Form betrieben wird.“ Klare Abgrenzungen und Verantwortlichkeiten für die Einrichtung, den Betrieb und insbesondere für eine Kontrolle der geforderten technisch organisatorischen Maßnahmen stehen mit dieser Aussage nicht in Einklang. Für Auftragsverarbeiter gemäß Art. 28 DSGVO führt dies zu Konflikten. Hält ein Auftragsverarbeiter eine Weisung des Verantwortlichen für datenrechtswidrig, hat der Auftragsverarbeiter die Pflicht, den Verantwortlichen über seine Auffassung zu informieren. Je nach Erheblichkeit der datenschutzwidrigen Datenverarbeitung erhöht sich die Hinweisplicht bis hin zu einer Nichtausführung von Weisungen. Die BfDI schränkt ihre Aussage zur vorübergehenden Möglichkeit einer Pseudonymisierung auf Basis von MaLo und MeLo-Id weitergehend ein: „Insgesamt müssen bei der Verarbeitung personenbezogener Daten die Vorgaben der Datenschutzgrundverordnung (DSGVO) eingehalten werden. Insbesondere sind gemäß Art. 5 Abs. 2 DSGVO die zur Verarbeitung der Last- oder Zählerstandgänge berechtigten Stellen für die Einhaltung des Absatzes 1 von Art. 5 DSGVO verantwortlich und müssen dessen Einhaltung nachweisen können.“ Es wird damit erneut auf die Grundsätze der nach der DSGVO zulässigen Datenverarbeitung verwiesen, zu denen die Anforderung an eine „Datensparsamkeit“ gemäß Art 5. Abs. 1 c) gehört.	

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				Eine auf die notwendige Datenerhebung minimierte Verarbeitung sehen das Schutzprofil und TR 03109-6 für das SMGW vor. Danach soll die Minimierung der übermittelten Daten und eine tarifgerechte Aggregation der Zählwerte bereits auf dem Gateway erfolgen und hinsichtlich der Datenübermittlung sichergestellt werden, dass Daten nur im erforderlichen Umfang und zu festgelegten Zeitpunkten ausschließlich an die jeweils berechtigte Stelle von einer vertrauenswürdigen Stelle automatisiert eingestellt werden. Der Einsatz des Gateways bildet danach den Stand der Technik ab im Hinblick auf eine mögliche und notwendige Datenminimierung und entspricht der Grundidee einer „Privacy by design“ Eine ungefilterte Weiterleitung aller Daten hingegen, auch diejenigen der Letztverbraucher, deren Tarife eine datensparsame Erhebung bedingen, widerspricht diesem Prinzip. Insgesamt ist festzustellen, dass wesentliche Aspekte der Position der BfDI übergangen werden. Gemäß § 47 Abs. 1 Nr. 13 MsbG kann die BNetzA Entscheidungen treffen im Benehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur datenschutzgerechten weiteren Ausgestaltung des Verfahrens der Zählerstandsgangmessung, einschließlich Vorgaben zur Löschung, Pseudonymisierung und Depseudonymisierung oder Anonymisierung von Messwerten, und zur standardmäßigen Vorgabe der Zählerstandsgangmessung als nicht auf einen Einzelzählpunkt bezogenes Bilanzierungsverfahren für Letztverbraucher mit einem Jahresstromverbrauch unterhalb von 10 000 Kilowattstunden. Herstellung des Benehmens bedeutet nicht Einvernehmen, aber eine über die Anhörung hinausgehende Beteiligung. Dieser Form einer notwendigen Berücksichtigung wird der bloße Hinweis auf einen Teil des Positionspapiers der BfDI nicht gerecht.	

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				2.Datensicherheit Art. 5 Abs. 1 f) schreibt eine Datenverarbeitung vor, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Die BfDI nimmt auf die Vorschrift ausdrücklich Bezug. Ein zentralisierter Betrieb in Form des MaBIS-Hubs gefährdet allerdings auch die Sicherheit der zu schützenden Daten, da die Beachtung des Schutzprofils und eine Verschlüsselung nach TR-03109-6 durch Übermittlung sämtlicher Rohdaten an den MaBIS-Hub in Frage gestellt wird. Die dargestellten Sicherheits- und Resilienz-Konzepte sind nicht erprobt, obgleich der zentralisierte Hub eine erhöhte Angriffsfläche bietet. Mit dem beabsichtigten Single-Point-of-Truth geht damit das Risiko eines Single-Point-of Failure einher. Aufgrund der vorstehenden Bedenken stellt sich abschließend die Frage, ob eine Verhältnismäßigkeitsprüfung durch Abwägung der Datenschutzrisiken im Verhältnis zu verbesserten Erkenntnismöglichkeiten in dem erforderlichen Umfang erfolgt ist.	
Fragen und ergänzende Anmerkungen	Fragen und ergänzende Anmerkungen			Wie werden Verstöße gegeen die IT-Richtlinien identifiziert und protokolliert?	SAP SE
Fragen und ergänzende Anmerkungen	Fragen und ergänzende Anmerkungen			Was sind die Maßnahmenen im Falle eines Verstoß gegen die IT-Richtlinien?	SAP SE
Fragen und ergänzende Anmerkungen	Fragen und ergänzende Anmerkungen		Werden die Kosten für den Aufbau und Betriebs des MaBiS-Hubs über die Netzentgelte umgelegt oder soll es eine eigene Umlage geben? Bei einer Umwälzung der Kosten sollte berücksichtigt werden, dass alle Marktlokationen, erzeugende und verbrauchende, an den Kosten beteiligt werden.	Es wird keine Aussage getroffen, wer die Kosten für den Aufbau und Betriebs des Hubs trägt bzw. wie die Betreibergesellschaft sich refinanziert.	VKU e.V.
Fragen und ergänzende Anmerkungen	Fragen und ergänzende Anmerkungen		Wie wird bei einer zentralisierten Infrastruktur Cybersicherheit gewährleistet? Sind Redundanzen für den Fall eines Cyberangriffs vorgesehen?	Einen potentiellen, digitalen Single Point of Failure für den deutschen Strommarkt zu schaffen, scheint in der aktuellen globalpolitischen Lage ein nicht zu unterschätzendes Risko darzustellen.	VKU e.V.
Allgemeines	Allgemeines		Die detaillierten Anforderungen(Kap.2. bis Kap.4.2) sollten durch eine entsprechende transparente Schutzbedarfsanalyse/Risikoanalyse nachvollziehbar begründet werden. Ggf. sind diese Anforderungen für die abzubildenden Prozesse zu hoch.		Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
Allgemeines	Allgemeines		Derzeit sind alle Kommunikationsprozesse als reine Push-Verfahren ausgelegt. Wir möchten darauf hinweisen, dass dies nicht in jedem Fall die technisch optimale Lösung darstellt und potenziell nachteilige technische Implikationen haben kann. Durch API-basierte Kommunikation eröffnen sich zusätzliche Integrationsmöglichkeiten – etwa asynchrone Schnittstellen oder das gezielte Abholen von Daten. Die konkrete technische und konzeptionelle Ausgestaltung der APIs und Datenformate möchten wir im Rahmen der edi@energy aktiv begleiten. Wir sehen eine Chance darin den Übermittlungsbegriff an dieser Stelle weiter zu interpretieren, um an ausgewählten Stellen durch alternative technische Umsetzungen von Push-Prozessen Mehrwerte zu heben, ohne negative Auswirkungen auf die bestehenden Prozess-Abläufe. Gerne bieten wir an in den nächsten Wochen geeignete Prozesse zu identifizieren und zu diskutieren.	Ein reines Push-Verfahren in der herkömmlichen technischen Interpretation kann zu Herausforderungen führen, etwa wenn Zielsysteme der Marktpartner zeitweise nicht erreichbar sind, Daten mehrfach gesendet werden müssen oder eine hohe Zahl gleichzeitiger Übertragungen ausgehend vom M-Hub die Systeme belastet. Außerdem ist die Steuerung und Nachverfolgung solcher Prozesse oft aufwendig. Dadurch steigt die Abhängigkeit von der Verfügbarkeit aller beteiligten Systeme und die Komplexität der Steuerung. Mit dem Einsatz von API-basierter Kommunikation eröffnen sich neue Möglichkeiten, die für die Konzeption des MaBiS-Hubs betrachtet werden sollten: Aus technischer Sicht ist in manchen Prozessen ein alternativer Übermittlungsansatz oft robuster, weil Empfänger selbst steuern können, wann und in welcher Rate sie Daten abrufen. Für den Hub reduziert sich damit die Abhängigkeit von der technischen Verfügbarkeit der Marktpartnersysteme und der technische Aufwand für eine garantierte Nachrichtenzustellung. Zum Beispiel sind hybride Modelle denkbar, bei denen eine kurze Benachrichtigung die Marktpartner auf neue oder geänderte Daten hinweist, die vom Marktpartner dann gezielt, verpflichtend abgeholt werden müssen. Der eigentliche Datenaustausch kann dadurch zeitlich entkoppelt und gezielt vom Empfänger ausgelöst werden. Dieses asynchrone Vorgehen entlastet die Systeme und erhöht die Stabilität, ohne die fachlichen Push-Prozesse grundsätzlich zu verändern. Insgesamt ist es unser Ziel eine nutzenoptimierte und prozessdienliche Konfiguration der Übermittlungsverfahren zu finden.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
Allgemeines	Allgemeines			Der vorgeschlagene Monitoring- und Reporting-Mechanismus, der die BNetzA in regelmäßigen Abständen über die Qualität der Datenverfügbarkeit und des Datenaustausches informieren soll, ist aus unserer Sicht elementar, um eine korrekte, vollständige und fristgerecht verfügbare Datenbasis, insbesondere aus iMS, sicherzustellen. Das Schaffen von Transparenz über den MaBiS-Hub beim Austausch von Stammdaten und insbesondere Bewegungsdaten, ist aus unserer Sicht ein wichtiger Hebel, um Defizite frühzeitig aufzudecken und diese mit qualitätssteigernden Maßnahmen wirksam zu adressieren.	E.ON Energie Deutschland GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
Allgemeines	Allgemeines	nicht vorhanden	Mit der aktuellen Konsultation zum MaBiS-Hub (Fokuspunkt Messwertverarbeitung und Pseudonymisierung) werden die technologischen Potenziale, die eine Hub-Architektur grundsätzlich bietet, nur ansatzweise genutzt. Die Optimierungsmöglichkeiten durch Nutzung von unterschiedlichen API-Techniken, Shared Data & Shared Services werden in dem Ansatz kaum berücksichtigt. Somit ist auch nur ein geringerer Mehrwert für die Branche erkennbar, was zur Akzeptanz des MaBiS-Hubs und seines weiteren Ausbaus im Markt nicht beiträgt. In unseren Konsultationsbeiträgen – insbesondere in der IT-Leitlinie – zeigen wir daher den notwendigen Anpassungsbedarf auf. Das beiliegende Dokument „Entwurf_Pull-Verfahren_Use_Case_Aufbereitung_und_Übermittlung_von_Werten“ illustriert exemplarisch, wie das API-basierte PULL-Verfahren den Prozess der Informationsbereitstellung effizienter und flexibler gestalten kann. Wir regen die BNetzA daher an, im Rahmen der Festlegung zur Umsetzung der Use Cases sowie bei der Ausgestaltung der Datenhaltung mehr technologische Offenheit und Flexibilität zuzulassen.	Mit der Umsetzung des MaBiS-Hubs (Teil 1) ist die Neuausrichtung der Marktkommunikation nicht beendet. Wir sehen den MaBiS-Hub als Einstieg in die Neukonzeption der Marktkommunikation und dieses sollte nicht durch technologische Einschränkungen verbaut werden. Ebenso sehen wir, wie die gesamte Branche, die Notwendikgeit eines langfristigen Lösungskonzepts und nicht die kurzfristige Beseitigung von Problemen.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
Allgemeines	Allgemeines	nicht vorhanden	In den IT-Leitlinien und auch anderen Dokumenten zum MaBiS-Hub werden die üblichen Zuständigkeiten zwischen Eigentümer/Gesamtverantwortlicher, Betreiber und operative Rollen der Funktionseinheiten des MaBiS-Hubs nicht definiert. Wir sehen dies als dringend erforderlich an, da damit die Verantwortungsbereiche und Aufgaben abgegrenzt werden müssen. Definitionen Eigentümer/Gesamtverantwortlicher: Eigentümer bzw. Gesamtverantwortlicher des MaBiS-Hubs muss eine juristische Person oder gemeinschaftlich gegründete Branchen-Gesellschaft o. ä. sein, welche gesamtheitlich für den Hub haftet. Sie ist u. a. zuständig für die Beauftragungen an den Betreiber des Hubs. Betreiber: Der Betreiber wird durch den Eigentümer/ Gesamtverantwortlichen beauftragt und ist zuständig für den technischen Betrieb und die Organisation des Hubs, d. h. er ist z. B. für die Bereitstellung von Servern, Datenbanken, Software sowie deren Pflege zuständig (beispielhafte Aufzählung) Operative Rollen der Funktionseinheiten: Die in den Funktionseinheiten hinterlegten Rollen, welche durch Unternehmen der Branche wahrgenommen werden können.	Im Gegensatz zu einigen anderen Mitgliedern der Branche vertreten wir die Auffassung, dass Eigentümer/Gesamtverantwortlicher, Betreiber und operative Rollen der Funktionseinheiten nicht zwangsläufig identisch sein müssen. Nach der momentanen Vorlage ist unsere Einschätzung der Rollen wie folgt: • Wahrung von Neutralität und Marktunabhängigkeit o Der Eigentümer bzw. Gesamtverantwortliche des MaBiS-Hubs (z. B. eine neutrale Instanz oder reglementierte Gesellschaft) trägt die Gesamtverantwortung für das regelwerkskonforme Funktionieren des MaBiS-Hubs. o Der technische Betreiber hingegen muss den Betrieb, Wartung und Sicherheit der IT-Infrastruktur bereitstellen. o Durch klare Trennung werden Interessenskonflikte mit Marktrollen (BKV, NB, LF) vermieden. • Haftung und Governance o Der Eigentümer bzw. Gesamtverantwortliche ist für die inhaltliche, fachliche und regulatorische Steuerung zuständig (Definition von Prozessen gemäß BNetzA-Vorgaben, Datenmodelle, Marktregeln) o Der Betreiber trägt die operative Verantwortung für die Verfügbarkeit, IT-Sicherheit und Systempflege. Diese Trennung ermöglicht eindeutige Haftungs- und Eskalationspfade im Störungs- oder Sicherheitsfall. • Sicherstellung von Compliance und Aufsichtsfähigkeit o Durch die organisatorische Trennung wird gewährleistet, dass Audits, Zertifizierungen und Prüfungen (z. B. durch BNetzA, Wirtschaftsprüfer, ISO-Auditoren) unabhängig durchgeführt werden können. o Die Regel- und Aufsichtsfunktion des Eigentümers bzw. Gesamtverantwortlichen bleibt dadurch unangetastet, während der Betreiber den technischen Nachweis der Einhaltung führt. • Vermeidung von Vendor-Lock-In und Sicherung der Nachhaltigkeit o Eigentum und Betreiberleistungen dürfen nicht untrennbar gekoppelt sein. o Der Eigentümer bzw. Gesamtverantwortliche muss in der Lage sein, den Betrieb des MaBiS-Hubs an einen anderen qualifizierten Betreiber zu übergeben, ohne Eigentums- oder Datenhoheitsverlust.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
Allgemeines	Allgemeines	nicht vorhanden	Hinweis (bitte neu aufnehmen): In den IT Leitlinien muss ein Kapitel 1.2 zu den Betreiberanforderungen ergänzt werden. Anforderung: Der Betrieb des MaBiS-Hubs ist durch einen benannten, nachweislich qualifizierten Betreiber sicherzustellen, der den technischen, organisatorischen und regulatorischen Anforderungen des Energiemarktes entspricht. • Es ist ein Betreibervertrag mit definierten Service-Level-Agreements, Securitiy-Level-Agreements und Verfügbarkeitskennzahlen zu etablieren. • Der Betreiber muss über ein nach ITIL aufgebautes Betriebsmodell verfügen (Incident-, Change-, Problem-, Release-Management) • Ein Notfallmanagement und Wiederanlaufverfahren sind nach BSI-Standard 100-4/ ISO 22301 umzusetzen. • Der Betreiber hat regelmäßig Compliance- und Penetrationstests durchzuführen und deren Ergebnisse der Aufsicht (z. B. BNetzA) vorzulegen.	• Gewährleistung einer klaren Verantwortlichkeit für den sicheren, hochverfügbaren und regelkonformen Betrieb. • Sicherstellung, dass der Betreiber über geeignete Zertifizierungen und Nachweise (z. B. ISO 27001, ISO 20000, BSI-Grundschutz, KRITIS-Nachweis) verfügt. • Vermeidung von Interessenkonflikten durch organisatorische Trennung von Marktrollen (z. B. Bilankreisverantwortliche, BIKO, "Datenbereitsteller") • Sicherstellung einer Betriebstransparenz gegenüber Aufsicht und beteiligten Marktakteuren.	E.ON Netze
Allgemeines	Allgemeines	nicht vorhanden	Hinweis (bitte neu aufnehmen): In den IT-Leitlinien werden verschiedene Überwachungsmechanismen, KPI's und Reports angesprochen. Es fehlen Kontrollinstanzen, die als Empfänger dieser Kontrollmechanismen dienen könnten.	In den IT-Leitlinien soll auf die Etablierung einer Art technisch-inhaltlichen Aufsichtsrat mit Spezialisten für Sicherheit, Betrieb, Prozesse, Marktpartnervertreter hingewiesen werden.	E.ON Netze
Allgemeines	Allgemeines	--	Wir schlagen vor, dass der Betreiber des MaBiS-Hub die Möglichkeit hat, den Nachrichteneingang in den Hub zu stoppen (ggf. nur für ein oder mehrere Marktpartner), wenn diesem ein Fehlverhalten auffällt.	Wir empfehlen einen solchen "Not-Stopp" aufgrund aktueller Geschehnisse. Zum Beispiel könnte ein Marktpartner versehentlich/aufgrund IT-technischer Probleme/Fehlentwicklungen innerhalb kürzester Zeit eine Vielzahl an z.B. Lastgangdaten an den Hub übermitteln, ohne dass diese eine Relevanz für den Hub hätten. Diese nicht begründete Massen an Daten könnte im Hub zu Performance-Problemen führen und der Eingang von Nachrichten (allen Nachrichten, bestimmten Nachrichtentypen (z.B. MSCONS) sollte für den entsprechenden Marktparnter bis zur Behebung des Fehlverhaltens vom MaBiS-Hub-Betreiber gestoppt werden können.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
Allgemeines	Allgemeines		Die vorgelegten IT-Leitlinien für den MaBiS-Hub sind insgesamt sehr gelungen. Sie spiegeln ein modernes und tragfähiges Architekturverständnis wider, indem sie auf offene Programmiersprachen, etablierte Standards und technologieneutrale Grundsätze setzen. Dies ist ausdrücklich zu begrüßen, da offene Standards eine langfristige Wartbarkeit, Interoperabilität und Anbieterunabhängigkeit des entstehenden Systems sicherstellen. Aus technischer Sicht fehlt den Leitlinien jedoch eine klare Hervorhebung eines ressourcenorientierten Architekturansatzes, wie er in modernen Plattformen eingesetzt wird. Ein solcher Ansatz ist die Grundlage für Skalierbarkeit, Modularität und Integrationsfähigkeit des MaBiS-Hub und sollte daher explizit adressiert werden. Im Folgenden werden die Elemente der Leitlinien herausgearbeitet, die für eine RESTful, ressourcenorientierte Implementierung sprechen und damit technologische, organisatorische und regulatorische Vorteile bieten.		Hochfrequenz Unternehmensberatung GmbH
Allgemeines	Allgemeines		Bei der Liste der IT-Anforderungen ist z.T. die Kombination der einzeln erfüllbaren Anforderungen kritisch zu bewerten, beispielsweise die ACID-Forderung zusammen mit horizontal skalierbaren Systemen.	Wir empfehlen dringend einen Workshop mit IT-Dienstleistern bzgl. der gleichzeitig erfüllbaren Anforderungen. Wie stehen dazu gerne zur Verfügung.	KISTERS AG
Allgemeines	Allgemeines		Die Anforderungen an die IT-Infrastruktur sind sehr hoch. Es stellt sich die Frage des Kostenrahmens für den Aufbau und Betrieb der notwendigen IT-Infrastruktur. Die notwendige Dimensionierung der IT-Infrastruktur des MaBiS-Hub sollte anhand der IT-Leitlinien, der Zentralisation der Datenspeicherung, Prozessabwicklung sowie der Backup-Vorgaben vorab bestimmt werden und mit belastbaren Zahlen beziffert werden. Nur so sind valide Aussagen zur Umsetzbarkeit des Aufbaus sowie Betriebs in einem akzeptablen Kostenrahmen möglich.	Eine Erlös- bzw. Kostenobergrenze wäre dringend angeraten, um Ineffizienzen und Überdimensionierung zu verhindern.	VKU e.V.
Abkürzungen und Definitionen	Abkürzungen und Definitionen	• ACID-Prinzipien als Systemgrundlage	• ACID-Prinzipien als Systemgrundlage. Bitte ACID in das Abkürzungsverzeichnis übernehmen.	ACID fehlt im Abkürzungsverzeichnis	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.	Übergreifende Anforderungen	Der Messwertverarbeiter und der Bilanzierungs- und Aggregierungsverantwortliche des MaBiS-Hub halten ihre Daten separat und kommunizieren diese nur über Schnittstellen und die festgelegten Prozesse	Änderung: Um eine Doppelte Datenhaltung innerhalb des MaBiS-Hub zu minimieren, greifen der Messwertverarbeiter und der Bilanzierungs- und Aggregierungsverantwortliche trotz Aufgabentrennung auf die gleichen Daten zu.	Eine Doppelte Datenhaltung bedeutet doppelte Kosten in z.B. Wartung, Datenbanken und Archivierung innerhalb einer MaBiS-Hub Instanz und dies ist nicht Zielführend. Eine Trennung der Verantwortung kann auch mit einem Rechtekonzept sichergestellt werden. Dadurch werden aufwendige Synchronisationen zwischen BA und MV vermieden was nur unnötig Ressourcen braucht. Außerdem besteht bei redundanter Datenhaltung immer das Risiko von inhaltlichen Abweichungen. Diese zu monitoren und zu beheben wäre eine zusätzliche Aufgabe. Vorstellbar wäre: MV: MELO/MALO-Stammdaten und MELO/MALO-Messwerte BA: Bilanzierungsrelevante MALO-Stammdaten und MaBiS-SZR Die beiden Marktrollen würden z.B. auf die gleichen MALO-Messwerte zugreifen und hätten keine Schiefstände	Arvato Systems Digital GmbH
1.	Übergreifende Anforderungen	erster Aufzählungspunkt: • Der MaBiS-Hub ist von technischer Seite so zu dimensionieren, dass er perspektivisch die anwachsende Anzahl von Stamm-und Abrechnungsdaten (siehe Anhang) als auch die von der Bundesnetzagentur festgelegten prozessualen Anforderungen performant abbilden kann	Wir begrüßen die zukunftsorientierte Ausrichtung bzgl. Skalierbarkeit und Performance. Dies erachten wir als elementar für eine erfolgreiche Zukunft des MaBiS-Hubs. Dabei ist bitte zu beachten: Es gilt neben der Anzahl von Stamm- und Abrechnungsdaten auch die steigende Anzahl an Werten zu berücksichtigen (z.B. aufgrund iMS-Rollout bei Marktlokationen, die nicht bereits zuvor mit 1/4-h bilanziert wurden oder z.B. die steigenden Anforderungen aus Gesetzen (Energy-Sharing, MiSpeL)). Dabei gilt es unserer Ansicht nach, zwischen MV und BA zu unterscheiden. Im Allgemeinen unterliegt der MV einer höheren Anzahl an zu verarbeitenden Stamm-/Abrechnungsdaten sowie der Verarbeitung von Einzelwerten als der BA. Des Weiteren sind die Auswirkungen von ACID auf die Skalierbarkeit und zukunftsfähige Performance zu berücksichtigen. Überlegungen zu einer rollierenden Abrechnung im BA und die Abbildung unterschiedlicher Bilanzierungsverfahren sollten bereits perspektivisch berücksichtigt werden.	Ausreichende Berücksichtigung aller Faktoren, die auf die Skalierbarkeit und Performance wirken können. Hinweis: Den genannten Anhang konnten wir nicht finden.	BDEW

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.	Übergreifende Anforderungen	erster Aufzählungspunkt: • Der MaBiS-Hub ist von technischer Seite so zu dimensionieren, dass er perspektivisch die anwachsende Anzahl von Stamm-und Abrechnungsdaten (siehe Anhang) als auch die von der Bundesnetzagentur festgelegten prozessualen Anforderungen performant abbilden kann	Wir begrüßen die zukunftsorientierte Ausrichtung bzgl. Skalierbarkeit und Performance. Dies erachten wir als elemantar für eine erfolgreiche Zukunft des MaBiS-Hubs an. Dabei ist bitte zu beachten: Es gilt neben der Anzahl von Stamm- und Abrechnungsdaten auch die steigende Anzahl an Werten zu berücksichtigen (z.B. aufgrund iMS-Rollout bei Marktlokationen, die nicht bereits zuvor mit 1/4-h bilanziert wurden oder z.B. die steigenden Anforderungen aus Gesetzen (Energy-Sharing, Mispel)). Dabei gilt es unserer Ansicht nach zwischen MV und BA zu unterscheiden. Im Allgemeinen unterliegt der MV einer höheren Anzahl an zu verarbeitendenden Stamm-/Abrechnungsdaten sowie Verarbeitung von Einzelwerten als der BA. Des Weiteren sind die Auswirkungen von ACID auf die Skalierbarkeit und zukunftsfähige Performance zu berücksichtigen. Überlegungen zu einer rollierenden Abrechnung im BA und die Abbildung unterschiedlicher Bilanzierungsverfahren sollte bereits perspektivisch berücksichtigt werden.	Ausreichende Berücksichtigung aller Faktoren, die auf die Skalierbarkeit und Performance wirken können. Hinweis: den genannten Anhang konnten wir nicht finden.	Bielefelder Netz GmbH
1.	Übergreifende Anforderungen	Der Messwertverarbeiter und der Bilanzierungs- und Aggregierungsverantwortliche des MaBiS-Hub halten ihre Daten separat und kommunizieren diese nur über Schnittstellen und die festgelegten Prozesse	Die beiden Rollen werden innerhalb des Hubs als jeweils eigener Service mit eigenen Schnittstellen und Datenräumen etabliert, um Unabhängigkeit zu gewährleisten. Die jeweiligen prozessualen/fachlichen Verantwortlichkeiten der Services sind durch die GPKE, WIM und MaBiS klar vorgegeben. Dieser modulare Ansatz erlaubt einen separaten Betrieb und ermöglicht auch singuläre Weiterentwicklung, Wartung, Testbarkeit und Skalierung. Insgesamt ist so sichergestellt, dass die beiden Services klar voneinander abgetrennt sind und eigenständig einsatzfähig sind. Die Ausgestaltung, der Datenhaltung und notwendigen internen Kommunikation zwischen den Services soll dem Hub-Betreiber obliegen, solange die beiden Marktrollen MV und BA gemeinsam durch diesen gehalten werden. Dies gilt ebenso für die Abwicklung von Prozessschritten bei denen eine Kommunikation zwischen den Services ("mit sich selbst") notwendig ist. Die Kommunikation mit externen Systemen wird für beide Services jeweils über die der EDI@Energy freigegebenen API-Schnittstellen realisiert, welche dem üblichen Versionsmanagement unterliegen.	Dies ermöglicht es, die Funktionalitäten einerseits voneinander unabhängig abschließend hinsichtlich ihrer prozessualen und format-/schnittstellentechnischen Vorgaben zu beschreiben und ermöglicht trotzdem bei Personenidentität ein im Interesse des Marktes optimierten Systembetrieb.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.	Übergreifende Anforderungen	• Der Messwertverarbeiter und der Bilanzierungs- und Aggregierungsverantwortliche des MaBiS-Hub halten ihre Daten separat und kommunizieren diese nur über Schnittstellen und die festgelegten Prozesse	Bitte Satz ändern: • Der Messwertverarbeiter und der Bilanzierungs- und Aggregierungsverantwortliche des MaBiS-Hubs kommunizieren nur über Schnittstellen und die festgelegten Prozesse Unser Verständnis des Originaltextes der BNetzA: • Die Datenhaltung (also Speicherung, Verwaltung und Verantwortung) liegt im MaBiS-Hub, und zwar getrennt nach den Rollen/ Funktionseinheiten MV und BA. • Die Daten verbleiben in der Hoheit dieser beiden Rollen mit teilweise denselben Daten. Dies ergibt sich aus folgender Rollenlogik: • Der MV erzeugt, empfängt, validiert Messwerte und speichert sie in seinem System • Der BA benötigt diese Messwerte (zeitreihenbasiert), um daraus Bilanzkreissummen zu bilden und muss sie daher ebenfalls in seinem System halten, um Aggregation, Plausibilisierung, Abrechnung etc. durchzuführen -> Beide Rollen arbeiten also auf denselben fachlichen Daten, aber aus unterschiedlichen Blickwinkeln. -> Da keine gemeinsame Datenbasis existiert, führt das automatisch zu Datenkopien. Wir stimmen ausdrücklich zu, dass die Kommunikation zwischen den Funktionseinheiten MV und BA über Schnittstellen und die festgelegten Prozesse zu erfolgen hat. Dies ist aus unserer Sicht unabdingbar für die Transparenz und Nachvollziehbarkeit durch die Marktpartner. Wir halten es für falsch, dass BA und MV separate Datenhaltung betreiben.	Der entscheidende Mehrwert eines Data Hubs im Energiermarkt entsteht dadurch, dass er zentral eindeutige Daten den Marktpartnern verfügbar macht. Das hier angedeutete Konzept unterschiedlicher, scheinbar auch doppelter Datenhaltung innerhalb des Hubs, widerspricht dem Grundgedanken eines Data Hubs und ist daher abzulehnen, da nicht der gewünschte Mehrwert und die zwingend erforderliche Zukunftsfähigkeit gewährleistet wird. Wir können keinen Nutzen für separate Datenhaltung innerhalb des MaBiS-Hubs erkennen. Im Einzelnen: Redundanz entsteht, weil MV und BA zum Teil dieselben Daten jeweils in eigenen separaten Datenbanken in den Funktionseinheiten speichern, verarbeiten und historisieren, statt auf eine gemeinsam bereitgestellte, versionsgeführte Datenbasis im MaBiS-Hub zuzugreifen (z. B. Shared Data). Dadurch ist der MaBiS-Hub kein „Single Point of Truth“. Dadurch hebt sich der MaBiS-Hub in seinem Datenhaltungskonzept deutlich von denen in den anderen europäischen Ländern ab, die ihre Daten nur einmal zentral halten. Des weiteren erschwert diese Art der Datenhaltung erheblich den weiteren Ausbau des MaBiS-Hubs um weitere Funktionseinheiten, da diese wiederum eigene Datenhaltung haben müssten, obwohl sie nahezu dieselben Daten nutzen. Weiter sehen wir in dem Konzept erhebliche Schwierigkeiten für einen zukünftigen Datenaustausch in Datenökosystemen. Auch die Einbindung des Kunden hinsichtlich Sicht auf seine Daten gemäß der EU-RL wird erschwert. Durch diese Art der Datenhaltung generieren wir im Hub dieselbe Komplexität und Fehleranfälligkeit bzgl. der korrekten Datennutzung, wie wir sie heute schon in den Systemen der Marktpartner vorliegen haben und verhindern wollten.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				Im Übrigen sehen wir es nach wie vor als sinnvoll an, nicht alle Daten (auch historische) dauerhaft in einem Hub zu halten. Wir sehen weiterhin den Vorteil in einer dezentralen Datenhaltung bei den verantwortlichen Marktpartnern, wo die Daten jederzeit abrufbar vorliegen. Das Argument, dass der Markt dies nicht leisten könnte, kann nicht gelten, da die Prozesse auch in dem vorliegenden Konzept eine Datenbereitstellung nahezu in Echtzeit durch die Marktpartner vorsieht. Hinweis: Der MaBiS-Hub sollte als zentrale Austausch- und Integrationsplattform für energiewirtschaftliche Bilanzierungs- und Aggregationsprozesse dienen. Er ist als dezentral föderiertes System zu betreiben: Daten bleiben bei ihren Eigentümern, werden über offene Standards geteilt, sind nachvollziehbar gekennzeichnet und EU-rechtskonform verarbeitet. • Ein dezentral föderierter MaBiS-Hub ist fachlich geboten (Datenhoheit), regulatorisch zukunftssicher (Data Act seit 12.09.2025 umzusetzen) und technisch sinnvoll (Interoperabilität, Resilienz). Eine föderierte Governance ersetzt eine zentrale Steuerung durch gemeinsame Regeln und verifzierbare Nachweise und schafft so Vertrauen, Austauschfähgkeit und Compliance im Energiemarkt.	
1.	Übergreifende Anforderungen	erster Aufzählungspunkt: • Der MaBiS-Hub ist von technischer Seite so zu dimensionieren, dass er perspektivisch die anwachsende Anzahl von Stamm-und Abrechnungsdaten (siehe Anhang) als auch die von der Bundesnetzagentur festgelegten prozessualen Anforderungen performant abbilden kann	Wir begrüßen die zukunftsorientierte Ausrichtung bzgl. Skalierbarkeit und Performance. Dies erarchten wir als elemantar für eine erfolgreiche Zukunft des MaBiS-Hubs an. Dabei ist bitte zu beachten: Es gilt neben der Anzahl von Stamm- und Abrechnungsdaten, auch die steigende Anzahl an Werten zu berücksichtigen (z.B. aufgrund iMS-Rollout bei Marktlokationen, die nicht bereits zuvor mit 1/4-h bilanziert wurden oder z.B. die steigenden Anforderungen aus Gesetzen (Energy-Sharing, Mispel)). Dabei gilt es unserer Ansicht nach zwischen MV und BA zu unterscheiden. Im allgemeinen unterliegt der MV einer höheren Anzahl an zu verarbeitendenden Stamm-/Abrechnungsdaten sowie Verarbeitung von Einzelwerten als der BA. Des Weiteren sind die Auswirkungen von ACID auf die Skalierbarkeit und zukunftsfähige Performance zu berücksichtigen. Überlegungen zu einer rollierenden Abrechnung im BA und die Abbildung unterschiedlicher Bilanzierungsverfahren sollte bereits perspektivisch berücksichtigt werden.	Ausreichende Berücksichtigung aller Faktoren, die auf die Skalierbarkeit und Performance wirken können. Hinweis: Den genannten Anhang konnten wir nicht finden. Hinweis: Zu diesem Thema stellen wir Ihnen sehr gerne eine von uns erarbeitete Bedarfskurve zur Verfügung. Des Weiteren stellen wir Ihnen in diesem Zuge gerne unsere erstellten Architekturbilder zur Verfügung (zum einen die Darstellung MV bzw. BA mit der "Außenwelt" und zum anderen die Darstellung innerhalb des MV/BA. Die Darstellung mit der "Außenwelt" verdeutlicht dabei u.a., dass auch ein NB oder LF mit ihrer eigenen Architektur einen Beitrag zum Erfolg des MaBiS-Hub beitragen können und unserer Ansicht nach auch müssen).	EnBW Energie Baden-Württemberg AG, Netze BW GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.	Übergreifende Anforderungen	dritter Aufzählungspunkt: • Der Messwertverarbeiter und der Bilanzierungs- und Aggregierungsverantwortliche des MaBiS-Hub halten ihre Daten separat und kommunizieren diese nur über Schnittstellen und die festgelegten Prozesse	Wir begrüßen die systemtechnische und prozessuale Abgrenzung des MV und BA.	Die Abgrenzung ermöglicht einem den Verwendungszwecken angepassten, unabhängigen und damit flexiblen Betrieb des MV und BA. Der Weg über festgelegte Prozesse verhindert ein "Wünsch-Dir-Was" einzelner Marktteilnehmer/-gruppen, ohne einen regulatorischen Hintergrund und einer sinnvoll leistbaren Regelungen der Kostenverrechnung an diese Marktteilnehmer/-gruppen (Umsetzung, Test, Implementierung, Betrieb, Wartung). Siehe hierzu auch ausführlichere Beschreibungen im Register "Governance + Transparenz" zum Kapitel 1.3, zweiter Aufzähluntspunkt. Wir möchten darauf hinweisen, dass auch Schnittstellen zum von uns angesprochenen UBA (s. dazu Register "WiM Teil 2" Nr. 14), wie auch mögliche, zukünftige Anbindungen der BDEW-Codenummerndatenbank oder Zertifikatsabrufe, ausschließlich über festgelegte Schnittstellen (PG EDI@Energy) anzubinden sind.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
1.	Übergreifende Anforderungen	Der MaBiS-Hub ist von technischer Seite so zu dimensionieren, dass er perspektivisch die anwachsende Zahl von Stamm- und Abrechnungsdaten, als auch die von der Bundesnetzagentur festgelegten prozessualen Anforderungen perfomrmant abbilden kann.	Dimension ist Folge der Zentralisierung. Bestehende, dezentrale Plattformen sind auf eine Skalierung ausgerichtet.	Die Hausheld AG ist ein bundesweit tätiger Gateway-Administrator mit einer eigenentwickelten, BSI-konformen Plattform für den sicheren Betrieb intelligenter Messsysteme und die Abwicklung bilanzierungsrelevanter Marktprozesse. Das HH-System ist vollständig mandantenfähig, revisionssicher und integriert die Funktionen zur Aggregation, Validierung und Abrechnung von Messdaten bereits heute in einem geschlossenen, ISMS-zertifizeriten Umfeld.	Hausheld AG
1.	Übergreifende Anforderungen	o Der MaBiS-Hub ist von technischer Seite so zu dimensionieren, dass er perspektivisch die anwachsende Anzahl von Stamm- und Abrechnungsdaten (siehe Anhang) als auch die von der Bundesnetzagentur festgelegten prozessualen Anforderungen performant abbilden kann	Wir konnten den referenzierten Anhang nicht finden		KISTERS AG
1.	Übergreifende Anforderungen	o Dabei soll die Performance entsprechend den Anforderungen skalieren und nicht im o ersten Schritt die perspektivischen Volumina (siehe Anhang) erfüllt werden	Wir konnten den referenzierten Anhang nicht finden		KISTERS AG
1.	Übergreifende Anforderungen	Der Messwertverarbeiter und der Bilanzierungs- und Aggregierungsverantwortliche des MaBiS-Hub halten ihre Daten separat und kommunizieren diese nur über Schnittstellen und die festgelegten Prozesse	Die Verantwortung des Messwertverarbeiters sollte beschrieben werden. Der Betreiber des MaBisHUB und der Bilanzierungs- und Aggregierungsverantwortliche des MaBiS-Hub halten ihre Daten separat und kommunizieren diese nur über Schnittstellen und die festgelegten Prozesse.	Das Marktrollenmodell und die Aufgaben sollten stringent beibehalten werden, um Interpretatiosnspielraum zu vermeiden.	Thüga SmartService GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	Open Source o Der vollständige Quellcode der Anwendung ist unter einer anerkannten Open-Source-Lizenz (z. B. Apache 2.0) zu veröffentlichen o Offene Bereitstellung und Pflege von Dokumentationen und Schnittstellen-Spezifikationen	Streichen	In Anbetracht des anspruchsvollen Zeitrahmens bis 10/2029 sollte auf Open Source verzichtet werden um auf bestehende und bewährte Lösungen zurückzugreifen. Kritisch sehen wir ebenfalls Open Source bei der späteren ISMS Zertifizierung und beim Thema IT-Cyber Security. Zusätzlich ist an der Stelle unklar, auf welchen Funktionsbaustein des MaBiS-Hubs sich die die Anmerkung zum Quellcode bezieht.	Arvato Systems Digital GmbH
1.1.	Technische Gesamt-anforderungen	zu "ACID-Prinzipien als Systemgrundlage", zweiter Aufzählungspunkt: o Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten	Ergänzung der Aussage: o Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten, jedoch nicht für Transaktionen im Rahmen der Durchführung der Marktkommunikation. Hier erfolgen die syntaktischen, semantischen und weiteren Prüfungen auf inhaltliche Korrektheiten im Rahmen der Ausprägungen der Marktkommunikation über die Vorgaben durch EDI@Energy bzw. die festgelegten Prozessdokumente und weitere BDEW-Datenaustausch-Dokumente.	Korrekte Abgrenzung, für welche Sachverhalte ACID Anwendung findet und ggf. in welchem Maße, um Missverständnisse zu vermeiden. Hinweis: Die vorgeschlagene Ergänzung bezieht sich dabei auch auf die Kommunikation zwischen dem MV und dem BA.	BDEW
1.1.	Technische Gesamt-anforderungen	zu "Datenmanagement": o Nutzung eines kanonischen Datenmodells zur Harmonisierung der Datenflüsse	Wir sind nicht in der Lage, diese Aussage in ein Gesamtbild einzuordnen. Von welchen zusammenhängenden Systemen/Datenflüssen wird gesprochen und wie ist in diesem Zusammenhang das von Ihnen in der Konsultation veröffentlichte Datenmodell zu verstehen und wie sind in diesem Zusammenhang die bereits seit Jahren vorhandenen, eindeutigen Begriffsbezeichnungen - insbesondere IDs - der EDI@Energy-Dokumente, der Festlegungen und weiterer BDEW-Dokumente zu verstehen?	Bitte um Konkretisierung, um Missverständnisse zu vermeiden. In keinem Fall darf diese Aussage unserer Ansicht nach dazu führen, dass bereits festgelegte, im Markt verwendete bzw. im BDEW seit Jahren gepflegte "Bezeichner" nun übersteuert werden.	BDEW
1.1.	Technische Gesamt-anforderungen	zu "ACID-Prinzipien als Systemgrundlage", zweiter Aufzählungspunkt: o Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten	Ergänzung der Aussage: o Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten, jedoch nicht für Transaktionen im Rahmen der Durchführung der Marktkommunikation. Hier erfolgen die syntaktischen, semantischen und weiteren Prüfungen auf inhaltliche Korrektheiten im Rahmen der Ausprägungen der Marktkommunikation über die Vorgaben durch EDI@Energy bzw. den festgelegten Prozessdokumenten und weiteren BDEW-Datenaustausch-Dokumenten .	Korrekte Abgrenzung, für welche Sachverhalte ACID Anwendung findet und ggf. in welchem Maße, um Missverständnisse zu vermeiden. Hinweis: Die vorgeschlagene Ergänzung bezieht sich dabei auch auf die Kommunikation zwischen dem MV und dem BA.	Bielefelder Netz GmbH
1.1.	Technische Gesamt-anforderungen	zu "Schnittstellenmanagement", dritter Aufzählungspunkt: o Unterstützung von Schnittstellen für andere Hubs / Plattformen (Interoperabilität)	Die Anforderung der Interoperabilität sollte auch für den MV und BA ausgesprochen werden.	Nach der Aussage der "Übergreifende Anforderungen" muss auch eine Interoperabilität zwischen MV und BA bestehen. Dies ist so auch absolut sinnvoll.	Bielefelder Netz GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	Standardisierte, dokumentierte APIs (z.B. REST mit OpenAPI-Spezifikation)	Der bne sieht in der Vorgabe der Nutzung von standardisierten API, mithin der Nutzung von etablierten Methoden eine wesentliche Voraussetzung für das Gelingen des MaBiS-Hubs. Diese Standards sind entscheiden, da sie von einer großen Zahl von Fachleuten beherrscht werden und ausreichende und gute Entwicklerwerkzeuge verfügbar sind. Durch die Nutzung von etablierten Standards kann sowohl die Entwicklungszeit verkürzt als auch die Qualität deutlich verbessert werden. Die konkrete Darstellung der Prozesse steht allerdings im Widerspruch zur Nutzung der Standard-Methoden. Hierauf hat der bne bereits in der Konsultation des Konzepts zur Nutzung und Veröffentlichung von API-Webdiensten hingewiesen (siehe auch der Konsultationsbeitrag von decarbon1ze et al.). Deshalb muss entweder eine Überarbeitung der Prozesse stattfinden oder eine Klarstellung erfolgen, dass der (technische) Verlauf des Datenaustauschs von der Prozessdarstellung abweichen kann, wenn dies für die Einhaltung der standardisierten IT-Verfahren notwendig ist.		Bundesverband Neue Energiewirtschaft e.V.
1.1.	Technische Gesamt-anforderungen	Verwendung von offenen Programmiersprachen	Diese Forderung sollte erweitert werden um die Nutzung offener Frameworks und Bibliotheken.	Große Business-Anwendungen werden so gut wie nie "from scratch" geschrieben, sondern setzen auf Frameworks auf. Beispiele sind Microsofts .NET Framework, das Spring Framework in Java, oder komplette Web-Frameworks wie Django (Python) oder Rails (Ruby). Ebensowichtig sind grundlegende Bibliotheken für Datenbankzugriff, Logging, zum Bau von APIs, oder für krytografische Funktionen – z.B. Hibernate, Slf4J, http4k oder BouncyCastle Java oder Kotlin.	decarbon1ze GmbH
1.1.	Technische Gesamt-anforderungen	Quellcode unter Open-Source Lizenz	Nicht beantwortet wird die Frage, ob Closed-Source Bibliotheken und Frameworks eingesetzt werden dürfen, und ob von dual-lizenzierte Bibliotheken die kommerzielle Variante genutzt werden darf.	Dies hat zum einen Auswirkungen auf die Kosten in der Entwicklung und im Betrieb; vor allem aber ist die Frage zu klären, ob im Sinne der Nachvollziehbarkeit und Transparenz auch aller verwendeter Code Dritter offenliegen muss um einer umfassenden Analyse zugänglich zu sein.	decarbon1ze GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	Veröffentlichung, offene Bereitstellung	Hier sollte festgehalten werden, - dass alle Artefakte in einem modernen Versionsverwaltungssystem (z.B. git) veröffentlicht werden sollen, inklusive etwaiger Testsysteme und Testdaten sowie aller "Infrastructure as Code" – also der Konfiguration der Cloud-Umgebung, Datenbanken, etc. - dass die Versionsverwaltung nicht nur zur Veröffentlichung des fertigen Produkts dient, sondern dass die komplette Entwicklung bereits öffentlich in besagtem Versionsverwaltungssystem zu erfolgen hat. Technisch gesprochen: Veröffentlich werden müssen alle Repositories des Projekts, nicht nur die produktiv gesetzten Zweige (nicht nur Release-Branches oder Release Tags)	Die offenlegeung der kompletten Repositories macht die Entwicklung insgesamt nachvollziehbar, inklusiver aller Entwurfsentscheidungen. - Somit können Gründe für Entwurfsentscheidungen nachvollzogen werden, was bei der Implementierung von kompatiblen Systemen für Marktpartner viele Fehler verhindern hilft. - Und nur so können interessierte Dritte bereits während der Entwicklung Code beisteuern (sog. "Merge Requests"), z.B. Software-Hersteller, Marktpartner, aber auch die interessierte Öffentlichkeit. - Sicherheitskritisch ist heutzutage insbesondere die Cloud-Infrastruktur. Nur wenn die komplette Konfiguration offengelegt wird, können Dritte die Sicherheit überprüfen und Hinweise zur Behebung von Fehlern geben.	decarbon1ze GmbH
1.1.	Technische Gesamt-anforderungen	KI-Tools, Datenübertragung in nicht-EU Drittländer	Geht es hierbei um jegliche Datenübertragung, oder nur um personenbezogene Daten?	Wenn Übertragung auch des Quellcodes in nicht-EU-Drittländer unterbunden werden soll, muss dies auch für die Source-Code Verwaltung gelten (also z.B. Codeberg anstatt GitHub). Bei KI-Tools käme die Regelung einem Verbot der Nutzung von KI-Tools gleich, weil es m.W. kein ausreichend leistungsfähiges KI-Tool zur Softwareentwicklung in Europa gibt.	decarbon1ze GmbH
1.1.	Technische Gesamt-anforderungen	ACID-Prinzipien	Die Forderung abschwächen zur eventuellen Konsistenz (eventual consistency) in einer für die Aufgaben angemessenen Form (siehe zur Einführung https://de.wikipedia.org/wiki/Konsistenz_(Datenspeicherung)#Verteilte_Systeme). Dazu ist eine umfassende Systemanalyse aller zu implementierenden Prorzesse nötig. Gefordert werden sollte daher, eine solche Analyse durchzuführen und eine entsprechende Empfehlung abzugeben als Teil des Angebotsprozesses. Von Seiten des Auftraggebers muss dann entschieden werden, genau welche Prozesse in welchen Grenzen transaktional auf DatenbankEbene abzuwickeln sind, und welche Konsistenz zwingend erforderlich ist.	Diese Forderung ist nicht praktikabel. Einerseits, weil nicht sauber definiert ist, was mit "transaktionsbasierten Prozessen" gemeint ist. Andererseits, weil für das geforderte Volumengerüst eine vollständig transaktionale Verarbeitung nicht darstellbar ist gemäß des CAP-Theorems. Ein System der geforderten Größenordnung kann praktisch nur als Cloud-System gebaut werden, in dem die Last mittels horizontaler Skalierung auf viele Rechnerknoten verteilt wird. Die Datenhaltung wird nicht komplett in einer relationalen ACID-Datenbank möglich sein; vielmehr wird es zumindest Sharding brauchen (verteilung der Daten nach Primärschlüsseln auf verschiedene Knoten), wahrscheinlich sogar Datenhaltung außerhalb von ACID-Datenbanken. Damit aber handelt es sich um ein verteiltes System, welches entweder Verfügbar (A) oder Konsistent (C) sein kann, nicht aber beides gleichzeitig. Siehe hierzu auch https://www.allthingsdistributed.com/2008/12/eventually_consistent.html	decarbon1ze GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	Schnittstellen-Management	Wir unterstützen die Forderung nach REST-APIs, wie in allen anderen Kommentaren hier ersichtlich.	Die als Beispiel angeführten REST-Schnittstellen passen nicht zur Entscheidung von edi@energy vom Oktober 2025 zur Nutzung proprietärer Webdienste. Mit letzteren wäre der MaBiS-Hub nicht kompatibel mit anderen Systemen, welche gemäß den anerkannten Regeln der Technik Clients für REST-APIs implementieren. Näheres dazu findet sich in unserem Konsultationsbeitrag zum API-Konzept 2025-10-15 sowie in unserem Begleitdokument zur vorliegenden Konsultation.	decarbon1ze GmbH
1.1.	Technische Gesamt-anforderungen	Der vollständige Quellcode der Anwendung ist unter einer anerkannten Open-Source-Lizenz (z. B. Apache 2.0) zu veröffentlichen	Die ÜNB sprechen sich gegen die Veröffentlichung des Quellcodes unter einer Open-Source-Lizenz aus. Derzeit ist nicht zu erwarten, dass sich eine aktive Community um den MaBiS-Hub bilden wird, die den Quellcode in Hinblick auf Funktionsweise, Qualität und Sicherheit untersucht. Stattdessen ist davon auszugehen, dass eine Veröffentlichung potenzielle Schwachstellen offenlegt und die Angriffsfläche ohne relevante Steigerung der Systemsicherheit erhöht. Gleichzeitig wäre die Nutzung von proprietärer Software unmöglich und Softwarehersteller müssten kategorisch ausgeschlossen werden. Zusätzlich geht die Veröffentlichung von Quellcode mit einem nicht zu unterschätzenden administrativen Mehraufwand hinsichtlich Wartung, Sicherheit, Community-Betreuung und Patentierung einher. Die Ziele Vertraulichkeit, Integrität und Transparenz sollten deshalb durch andere Maßnahmen erreicht werden. Zu diesen Maßnahmen zählen neben Auditierungen im Rahmen einer ISO27001-Zertifzierung, Quellcode-Reviews auch Penetrationstests. Ergänzend könnten weitere Zertifizierungen durch geeignete und unabhängige Dritte (z.B. TÜV) erfolgen. Zugleich ist eine selektive Bereitstellung des Quellcodes für berechtigte Interessenten und nach vorheriger Prüfung denkbar. Zudem kann eine transparente Dokumentation zur Funktionsweise und Sicherheitsmaßnahmen (ohne Technische Details) erfolgen.		Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
1.1.	Technische Gesamt-anforderungen	Verwendung offener Datenstandards und Formate (z.B. JSON, XML) unter Berücksichtigung der von der EDI@Energy vorgegebenen Datenformate und Standards	Anpassung der Formulierung: Verwendung offener Datenstandards und Formate (z.B. JSON, XML) unter Berücksichtigung der von der EDI@Energy vorgegebenen Datenformate und Standards unter Berücksichtigung einer hervorgehobenen Rolle der 4ÜNB	Als designierter MaBiS-Hub Betreiber sind in Bezug auf Datenmengen/Skalierungsfähig deutlich höhere Herausforderungen zu bewältigen, daher soll den 4ÜNB hier eine hervorgehobene Rolle zukommen	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	ACID-Prinzipien als Systemgrundlage - Anwendung des ACID-Modells (Atomicity, Consistency, Isolation, Durability) auf alle transaktionsbasierten Prozesse - Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten	Die Anforderung sollte präzisiert werden, um das eigentliche Ziel – die Sicherstellung von Datenintegrität, Nachvollziehbarkeit und fachlicher Konsistenz – klarzustellen, ohne dabei auf eine strikt transaktionale Umsetzung festgelegt zu sein. Vorschlag: „Datenverarbeitungsprozesse müssen die fachliche Konsistenz, Nachvollziehbarkeit und Integrität der Daten sicherstellen. Für bilanzrelevante und revisionspflichtige Verarbeitungsschritte ist transaktionale Integrität erforderlich. Für analytische, aggregierende oder eventgetriebene Prozesse sind Mechanismen wie Idempotenz, Wiederholbarkeit, reproduzierbare Zustandsübergänge sowie – sofern fachlich vertretbar – eventual consistency zulässig, um Skalierbarkeit und Verfügbarkeit sicherzustellen.“	Die bisherige Formulierung legt eine universelle Anwendung des ACID-Modells nahe. Das ist für einen verteilten, skalierbaren Datahub technisch nicht durchgängig realisierbar und würde Skalierung, Fehlertoleranz und Performance unnötig einschränken. Konsistenz- und Integritätsziele sollten kontextabhängig umgesetzt werden: In transaktionalen, bilanzrelevanten Prozessen durch atomare, isolierte Transaktionen. In analytischen und eventbasierten Prozessen durch eventual consistency in Kombination mit idempotenter Verarbeitung und reproduzierbaren Zuständen.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
1.1.	Technische Gesamt-anforderungen	•Dabei soll die Performance entsprechend den Anforderungen skalieren und nicht im ersten Schritt die perspektivischen Volumina (siehe Anhang) erfüllt werden	Anhang fehlt	Anhang ist nicht auffindbar	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
1.1.	Technische Gesamt-anforderungen	• Datenmanagement o Nutzung eines kanonischen Datenmodells zur Harmonisierung der Datenflüsse	Bitte ändern: • Datenmanagement o Nutzung eines kanonischen Datenmodells, welches interoperabel und standardisiert ist, zur Harmonisierung der Datenflüsse.	Nur ein kanonisches, interoperables und standardisiertes Datenmodell stellt sicher, dass alle Marktrollen und Systeme des MaBiS-Hubs auf einer gemeinsamen Datengrundlage arbeiten. Dadurch werden Schnittstellen vereinfacht, Dateninkonsistenzen vermieden und die Anforderungen an Interoperabilität, Nachvollziehbarkeit und regulatorische Konformität (z.B. EU Data Act, AI Act) erfüllt.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	Einsatz von KI-Tools o KI-Tools zur Unterstützung des gesamten Entwicklungsprozesses (von der Anforderungserhebung und -spezifizierung über die technische Spezifizierung, Codegenerierung, Tests bis zur Dokumentation) sind zulässig, wenn Datenschutzkonformität sichergestellt ist (z.B. keine Datenübertragung in Nicht-EU-Drittländer) und generierte Inhalte manuell überprüft und dokumentiert werden o Softwareentwickler behalten die ausschließliche Verantwortung für den KI-produzierten und eingecheckten Quellcode	Bitte ergänzen: o Als KI Modelle zur Prozessautomation und Mustererkennung sind europäische quelloffene Systeme zu verwenden (z. B. Mistral in den unterschiedlichen Derivaten) o KI Trainingsstände zur Prozessautomation und Mustererkennung sind in typischen Quellcodeverwaltungssystemen der Community zur Verfügung zu stellen. o KI generative Daten werden in den Daten gesondert markiert (Nachvollziehbarkeit, z. B. Trainingsversion und AI-Modell)	Zu "Europäische, quelloffene Systeme": • Transparenz und Nachvollziehbarkeit: Europäische Open-Source-Modelle erfüllen die Anforderungen des EU AI Acts an Transparenz, Dokumentation und Auditierbarkeit besser als proprietäre Systeme. • Datensouveränität: Der Einsatz europäischer Systeme stellt sicher, dass Daten (z. B. energiewirtschaftliche, personenbezogene oder vertrauliche Unternehmensdaten) im europäischen Rechtsraum verbleiben und den Vorgaben der DSGVO sowie des EU Data Acts entsprechen. • Interoperabilität und Integrationsfähigkeit: Quelloffene Modelle (z. B. Mistral) lassen sich technisch leichter in bestehende europäische Datenökosysteme (z. B. Energy Data Space) integrieren. • Vermeidung von Abhängigkeiten: Proprietäre Modelle außereuropäischer Anbieter bergen ein Risiko sogenannter Vendor Lock-ins. Offene europäische Modelle fördern digitale Souveränität und Innovationsfähigkeit. Zu "Quellcodeverwaltungssysteme": • Reproduzierbarkeit und Vertrauen: Durch Veröffentlichung der Trainingsstände (z. B. Modellversionen, Hyperparameter, Trainingsdatenquellen) in Systemen wie GitLab, GitHub wird die Nachvollziehbarkeit und Validierbarkeit der KI-Ergebnisse sichergestellt. • Community-basierte Qualitätskontrolle: Offene Bereitstellung ermöglicht Peer Reviews, Fehlererkennung und kollektive Weiterentwicklung der Modelle durch die Fachcommunity. • Regulatorische Konformität: Der EU AI Act fordert nachvollziehbare Trainingsprozesse für vertrauenswürdige KI-Systeme; die Dokumentation in Versionskontrollsystemen erfüllt diesen Nachweis. • Nachhaltige Weiterentwicklung: Versionierte Ablage der Trainingsstände schafft eine Basis für kontinuierliche Verbesserung und Wiederverwendung in verschiedenen Anwendungen (z. B. neue Prozessmodule im MaBiS-Hub). Zu "gesonderte Markierung": • Transparenzpflicht: Gemäß EU AI Act und Data Governance Act müssen durch KI erzeugte oder veränderte Daten eindeutig gekennzeichnet werden, um ihre Herkunft und Zuverlässigkeit bewerten zu können.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				• Nachvollziehbarkeit und Auditfähigkeit: Durch Markierung (z. B. Metadatenfelder wie generatedByModel, trainingVersion) wird ersichtlich, welche Daten maschinell generiert wurden — essenziell für Prüf-, Validierungs- und Haftungsfragen. • Vermeidung von Datenverfälschung: In regulierten Bereichen wie der Energiewirtschaft ist es kritisch, reale Mess- oder Geschäftsdaten von synthetischen KI-Daten zu unterscheiden. • Datenqualität und Rückverfolgbarkeit: Markierungen ermöglichen die Rückverfolgung bis zur Modellversion, was für Korrektur, Re-Training oder rechtliche Nachweise unerlässlich ist.	
1.1.	Technische Gesamt-anforderungen	Schnittstellenmanagement o Standardisierte,dokumentierte APIs (z.B. REST mit OpenAPI-Spezifikation)	Bitte ändern: Schnittstellenmanagement o Standardisierte,dokumentierte APIs (z .B. REST mit OpenAPI-Spezifikation mindestens in der Version 3.1)	OpenAPI 2.0 ist die ältere Version. OpenAPI 3.x (3.0, 3.1) ist der aktuelle Standard, der eine Vielzahl struktureller und semantischer Erweiterungen bringt. Die Versionen können unterschieden werden hinsichtlich • Interoperabilität: Nur OpenAPI 3.1 ist 100 % JSON Schema-kompatibel, was die Voraussetzung für neue EU-Dateninitiativen ist (z. B. Data Spaces, ENTSO-E ESMP-Schemas). • Regulatorische Nachvollziehbarkeit: In europäischen Projekten wird zunehmend gefordert, dass API-Spezifikationen semantisch validierbar und versioniert sind (ähnlich wie CIM-Profile). Das geht nur konsistent mit OpenAPI 3.1 + JSON Schema. • Migration und Governance: Wenn man eine API-Governance-Struktur oder ein Data-Space-Portal aufbaut, benötigt man eine klare Versionstrennung, z. B. um: o inkompatible Schemas zu erkennen, o automatische Generierung von Clients/Servern zu ermöglichen, o Open-Source-Compliance sicherzustellen.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	• Softwareentwicklung und Quellcode o Verwendung von offenen Programmiersprachen mit breiter Community-Unterstützung (z. B. Java, Python, Go)	Bitte ergänzen: • Softwareentwicklung und Quellcode o Verwendung von offenen Programmiersprachen mit breiter Community-Unterstützung (z. B. Java, Python, Go), jedoch, wenn möglich, Beschränkung auf zwei Programmiersprachen für die tatsächliche Umsetzung (z. B. Javascript Frontend, bzw. PHP im Backend). Die Schnittstellen auf Seite der Marktpartner sind davon nicht betroffen. o Der Quellcode muss durch Menschen erstellt sein (nicht ausschließlich durch KI generiert). o Es ist ein "Software Bill of Materials" zu pflegen für jeden benutzten Fremdcode.	Es muss verhindert werden, dass ein bunter Blumenstrauß an unterschiedlichen Umsetzungen entsteht. Die Kompatibilität und Verfügbarkeit von Personal muss für die nächsten 30 Jahre diesen Anforderungen Stand halten. Insbesondere in der Startphase ist es wichtig, dass für den Menschen lesbarer und wartbarer Quellcode erzeugt wird - neben den Logik-Risiken durch KI. Der Einsatz von fremden Quellcode muss dem Grundsatz nach so wenig wie möglich erfolgen, insbesondere proprietäre Bibliotheken bestehen aus sehr vielen Bibliotheken mit vielen, schwer wartbaren Abhängigkeiten. Hierzu gehört es zur fortschrittlichen Technik, dass mit entsprechenden Tools ein "Software Bill of Materials" gepflegt wird.	E.ON Netze
1.1.	Technische Gesamt-anforderungen	• Open Source o Der vollständige Quellcode der Anwendung ist unter einer anerkannten Open-Source-Lizenz (z. B. Apache 2.0) zu veröffentlichen	Bitte ändern: o Der vollständige Quellcode steht allen Marktpartnern paritätisch zu. Jeder Marktpartner hat das Recht, jederzeit Einsicht in den Quellcode zu verlangen. Gleichzeitig ist der Quellcode als schützenswertes Gut zu behandeln.	Im Kontext einer KRITIS-Infrastruktur sollte der Quellcode nicht öffentlich zugänglich gemacht werden, da er potenziell einen primären Angriffspunkt darstellen kann – selbst wenn sowohl die Infrastruktur als auch der Code selbst als gehärtet gelten.	E.ON Netze
1.1.	Technische Gesamt-anforderungen	• Schnittstellenmanagement o Standardisierte, dokumentierte APIs (z.B. REST mit OpenAPI-Spezifikation) o Verwendung offener Datenstandards und Formate (z.B. JSON, XML) unter Berücksichtigung der von der EDI@Energy vorgegebenen Datenformate und Standards	• Schnittstellenmanagement o Standardisierte, dokumentierte APIs (z.B. REST mit OpenAPI-Spezifikation) o Verwendung offener Datenstandards und Formate (z. B. JSON, XML) zur Sicherstellung von Interoperabilität in Abstimmung mit den von EDI@Energy vorgegebenen Datenformaten und Standards für die Marktkommunikation	Offene Datenstandards ermöglichen Interoperabilität. Damit die Schnittstellen in der Marktkommunikation maximal wiederverwendet und stabil gehalten werden, sollten diese von der EDI@Energy vorgegeben werden.	E.ON Netze
1.1.	Technische Gesamt-anforderungen	neuer Aufzählungspunkt	Bitte ergänzen: Durch API-basierte Kommunikation eröffnen sich zusätzliche Integrationsmöglichkeiten – etwa asynchrone Schnittstellen oder das gezielte Abholen von Daten. Für die konkrete technische und konzeptionelle Ausgestaltung der APIs und Datenformate durch die EDI@Energy sollen alle Möglichkeiten der API-Verfahren zur optimalen Ausgestaltung der APIs und Datenaustausche erlaubt sein. Wir sehen eine Chance darin, den Übermittlungsbegriff an dieser Stelle weiter zu	Ein reines Push-Verfahren in der herkömmlichen technischen Interpretation kann zu Herausforderungen führen, etwa wenn Zielsysteme der Marktpartner zeitweise nicht erreichbar sind, Daten mehrfach gesendet werden müssen oder eine hohe Zahl gleichzeitiger Übertragungen ausgehend vom MaBiS-Hub die Systeme belastet. Zudem ist die Steuerung und Nachverfolgung solcher Prozesse oft aufwändig. Dadurch steigt die Abhängigkeit von der Verfügbarkeit aller beteiligten Systeme und die Komplexität der Steuerung.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
			interpretieren, um an ausgewählten Stellen durch alternative technische Umsetzungen von Push-Prozessen Mehrwerte zu heben und dadurch Mehrwerte für die Use Cases zu schaffen.	Derzeit werden alle Kommunikationsprozesse als reine Push-Verfahren ausgelegt. Wir weisen darauf hin, dass dies nicht in jedem Fall (sondern durchaus häufig) die technisch/ prozessuale optimale Lösung darstellt und potenziell nachteilige technische Implikationen haben kann. Der Vorteil eines Hubs liegt in der zentralen Bereitstellung von Daten, die jederzeit abrufbereit vorliegen sollten. Nur so kann sich der Datenberechtigte optimieren und auf unterschiedliche Stuationen reagieren. Durch gezieltes Abholen von Daten werden Datenschiefstände und aufwändige Updates von Daten und Versionierungen bei den Marktpartnern minimiert. So sind z. B. fehlerhafte Abrechnungen auf Grund nicht aktuell gehaltener Daten bei den Datenberechtiigten vermeidbar oder können durch die Marktpartner selbstständig schnell aufgeklärt werden. Mit dem Einsatz von API-basierter Kommunikation eröffnen sich neue Möglichkeiten, die für die Konzeption des MaBiS-Hubs in Betracht gezogen werden müssen, um den Mehrwert eines Hubs zu heben: Aus technischer Sicht ist in ausgewählten Prozessen ein alternativer Übermittlungsansatz effektiver, weil Empfänger selbst steuern können, welche Daten sie wann abrufen. Für den Hub reduziert sich damit die Abhängigkeit von der technischen Verfügbarkeit der Marktpartnersysteme und der technische Aufwand für eine garantierte Nachrichtenzustellung. Zum Beispiel sind hybride Modelle denkbar, bei denen eine kurze Benachrichtigung die Marktpartner auf neue oder geänderte Daten hinweist, die vom Marktpartner dann gezielt, verpflichtend oder zum besten Zeitpunkt abgeholt werden müssen. Nicht immer ist es erforderlich, die Bereitstellung von Daten anzeigen zu müssen, da z. B. auch der Prozessablauf mit seinen festen Terminen das Vorhandensein von Daten vorgibt, z. B. die tägliche Bereitstellung von Lastgängen. Hier könnte der Datenberechtigte erst dann die Daten abrufen, wenn er sie benötigt, bzw. er eine bessere Qualität haben möchte, da er weiß, dass sich im Nachlauf der ersten Bereitstellung die Qualtät durch Ersatz der „vorläufigen Werte“ die Datenqualität erhöht.	

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				In beiliegendem Dokument "Entwurf_Pull-Verfahren_Use-Case_Aufbereitung_und_Übermittlung_von_Werten" haben wir gemeinsam mit Amprion am Beispiel des Use Cases "Wertebereitstellung durch den MV" beispielhaft versucht aufzuzeigen, wie die Nutzung von RESTful API eingesetzt werden kann. Aufgrund der Kürze der Zeit war es uns nicht möglich, die komplette Optimierung innerhalb der Use Cases der GPKE/WiM zu modellieren. So z. B. könnte der durch den BDEW und uns zusätzlich geforderten Prozess der GPKE "Übermittlung von Informationen" (siehe Konsultationsbeitrag GPKE, Teil 4) den im Beispiel unter 2.4.5 SD "Abholung Wert je Marktlokation" subsumieren. Wir möchten darauf hinweisen, dass es für die Darstellung der unterschiedlichen Möglichkeiten von API-Verfahren im Verband noch keine Regelung über dessen Notation gibt, daher wurde in dem Beispiel, wie bisher bekannt, mit einem Hin- und Rückpfeil gearbeitet. Es wären aber auch andere, übersichtlichere Darstellungsmöglichkeiten möglich. Für weitere Erläuterungen stehen wir gerne bereit, um etwa die Optimierungsmöglichkeiten durch die Verwendung weiteren API-Ausprägungsmöglichkeiten zu diskutieren.	
1.1.	Technische Gesamt-anforderungen	Aussagen zu den Punkten " Softwareentwicklung und Quellcode" sowie "Open Source"	Wir begrüßen die Verwendung offener Programmiersprachen und der Veröffentlichtung des Quellcodes und weiterer Dokumente. Wir schlagen hierbei vor, dass auch die Konfigurationstabellen/-dateien mit veröffentlicht werden sollten.	Dies ermöglicht dem Markt die Umsetzungen nachvollziehen zu können und gibt dem Markt Sicherheit in die Anwendungen. Insbesondere die Veröffentlichung der Konfigurationstabellen/-dateien ermöglicht Systemtests auch ohne die Einbindung des MaBiS-Hub-Betreibers.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
1.1.	Technische Gesamt-anforderungen	zu "ACID-Prinzipien als Systemgrundlage", zweiter Aufzählungspunkt: o Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten	Ergänzung der Aussage: o Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten, jedoch nicht für Transaktionen im Rahmen der Durchführung der Marktkommunikation. Hier erfolgen die syntaktischen, semantischen und weiteren Prüfungen auf inhaltliche Korrektheiten im Rahmen der Ausprägungen der Marktkommunikation über die Vorgaben durch EDI@Energy bzw. den festgeleten Prozessdokumenten und weiteren BDEW-Datenaustausch-Dokumenten .	Korrekte Abgrenzung, für welche Sachverhalte ACID Anwendung findet und ggf. in welchem Maße, um Missverständnisse zu vermeiden. Hinweis: Die vorgeschlagene Ergänzung bezieht sich dabei auch auf die Kommunikation zwischen dem MV und dem BA.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
1.1.	Technische Gesamt-anforderungen	zu "Schnittstellenmanagement", dritter Aufzählungspunkt: o Unterstützung von Schnittstellen für andere Hubs / Plattformen (Interoperabilität)	Die Anforderung der Interoperabilität sollte auch für den MV und BA ausgesprochen werden.	Nach der Aussage der "Übergreifende Anforderungen" muss auch eine Interoperabilität zwischen MV und BA bestehen. Dies ist so auch absolut sinnvoll.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	zu "Datenmanagement": o Nutzung eines kanonischen Datenmodells zur Harmonisierung der Datenflüsse	Wir sind nicht in der Lage, diese Aussage in ein Gesamtbild einzusortieren. Von welchen zusammenhängenden Systemen/Datenflüssen wird gesprochen und wie ist in diesem Zusammenhang das von ihnen in der Konsultation veröffentlichte Datenmodell zu verstehen und wie sind in diesem Zusammenhang die bereits seit Jahren vorhandenen, eindeutigen Begriffsbezeichnungen - insbesondere IDs - der EDI@Energy-Dokumente, der Festlegungen und weiteren BDEW-Dokumente zu verstehen. Wir können die Aussage dahingehend verstehen, sofern damit gemeint ist, dass der MV und BA in sich jeweils, die im Markt bereits bestehenden, allgemeingültigen Datenmodell-relevanten Vorgaben abbilden und darüber hinausgehend in sich selbst relevante, interne Elemente eineindeutig deklarieren. Wir sind aktuell nicht in der Lage ein CDM zwischen dem MV und BA als relevant anzusehen, da wir uns in diesem Austausch bereits in "festgelegtem, beschriebenem Teritorium" befinden. Bezüglich eines gemeinsamen Verständnisses grundlegender sonstiger zu vewaltender Aspekte innerhalb der beiden Systeme, kann dies von uns nachvollzogen werden.	Bitte um Konkretisierung, um Missverständnisse zu vermeiden. In keinem Fall darf diese Aussage unserer Ansicht nach dazu führen, dass bereits festgelegte, im Markt verwendete bzw. im BDEW seit Jahren gepflegte "Bezeichner" nun übersteuert werden.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
1.1.	Technische Gesamt-anforderungen	Standardisierte, dokumentierte APIs (z.B. REST mit Open API-Spezifikation)	Spezifikatiionen fehlen	Fehlende Schnittstellenspezifikation (API-Formate, Versionierung, Rückmeldeverfahren).	Hausheld AG
1.1.	Technische Gesamt-anforderungen	Unterstützung von Schnittstellen für andere Hubs/Plattformen (Interoperabilität)	Eingriff in bestehende Kommunikations- und Sicherheitsarchitektur	Die Hausheld-Plattform basiert auf einer proprietären, nach BSI-TR 03109-6/-7 zertifizierten Systemarchitektur mit integrierter Datenaggregation. Eine verpflichtende Nutzung eines externen MaBis - Hubs würde tiefgreifende Veränderungen in Kommunkations -und Sicherheitsarchitektur erfordern.	Hausheld AG
1.1.	Technische Gesamt-anforderungen	Verwendung von offenen Programmiersprachen mit breiter Community-Unterstützung	Die Forderung nach der Verwendung offener Programmiersprachen mit breiter Community-Unterstützung sollte konsequent erweitert werden: Nicht nur die Programmiersprache selbst, sondern auch das gesamte API-Tooling, insbesondere für die Erstellung, Validierung und Nutzung von OpenAPI-Spezifikationen, muss dem aktuellen Stand der Technik entsprechen. Dies umfasst etablierte Ökosysteme, automatische Code- und Client-Generierung, konsistente Modellierungsmuster sowie die Unterstützung moderner API-Design-Guidelines.	Die aktuell gewählte Vorgehensweise, bestehende SOAP-artige Webservice-Strukturen in mehrere OpenAPI-Spezifikationen zu überführen, führt faktisch zu einer Replikation des alten Paradigmas in einem neuen Format. Dies erzeugt erheblichen Mehraufwand bei allen Marktteilnehmern: •Die Implementierungen müssen komplexe, prozessgetriebene API-Designs nachbilden, die nicht dem ressourcenorientierten Ansatz moderner REST-Architekturen entsprechen. •Automatisierte Code-Generierung, die ein zentrales Effizienz- und Qualitätsmerkmal von OpenAPI ist, wird dadurch weitgehend unterlaufen. •Marktteilnehmer benötigen individuelle Integrationslogik, statt auf generierten, standardisierten Client- und Server-Code zurückgreifen zu können.	Hochfrequenz Unternehmensberatung GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				Ein RESTful, ressourcenorientiertes OpenAPI-Design ermöglicht hingegen eine wesentlich stärkere Automatisierung: •Große Teile der Client- und Server-Implementierungen lassen sich aus stabilen, konsistenten Spezifikationen direkt generieren. •Redundanzen werden reduziert, Fehlerquellen minimiert und Entwicklungszyklen deutlich verkürzt. •Die breitere API-Community stellt umfangreiche Tools bereit, die bei einem ressourcenorientierten Modell vollständig wirksam werden. Dies führt zu spürbar geringeren Implementierungs- und Betriebskosten, schnellerer Marktreife sowie zu einem robusteren und langfristig wartbaren technischen Fundament für den MaBiS-Hub.	
1.1.	Technische Gesamt-anforderungen	Unterstützung von Schnittstellen für andere Hubs / Plattformen (Interoperabilität)	Um eine hohe Interoperabilität mit anderen Hubs und Plattformen sicherzustellen, sollte der MaBiS-Hub konsequent auf den heute branchenübergreifend etablierten REST-Architekturstil setzen. REST hat sich als de-facto-Standard für offene, interoperable Schnittstellen durchgesetzt und bietet damit die bestmögliche Grundlage für zukunftssichere Integrationen.	Die Nutzung weit verbreiteter Architekturansätze wie REST erleichtert die schnelle und kosteneffiziente Anbindung externer Systeme erheblich. REST-APIs profitieren von: •breiter Unterstützung durch nahezu alle modernen Entwicklungsumgebungen und Integrationsplattformen, •umfangreichem Tooling (OpenAPI, Code-Generatoren, API-Gateways, Monitoring-Tools), •hoher Akzeptanz in anderen energiewirtschaftlichen Hubs (z. B. Redispatch-Plattformen, Netzbetreiberportale, Marktkommunikationssysteme), Durch den Verzicht auf proprietäre oder nachgebildete SOAP-Muster werden Integrationshemmnisse reduziert, die Wiederverwendbarkeit bestehender Komponenten erhöht und die Zusammenarbeit zwischen Marktteilnehmern sowie zwischen verschiedenen digitalen Hubs deutlich erleichtert. Dies führt zu schnelleren Integrationszeiten, geringeren Entwicklungskosten und einer insgesamt höheren Interoperabilität des MaBiS-Hub im wachsenden Ökosystem energiewirtschaftlicher Plattformen.	Hochfrequenz Unternehmensberatung GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	o Der vollständige Quellcode der Anwendung ist unter einer anerkannten Open-Source-Lizenz (z. B. Apache 2.0) zu veröffentlichen	Open Source kann auch contraproduktiv für die System-Sicherheit sein: die Analysemöglichkeit auf open source Basis ermöglicht auch Angreifern Schwachstellen direkt systematisch zu suchen/zu finden und direkt auszunutzen. Wenn "Open Source" angewendet werden soll, dann muss auf jeden Fall eine policy definiert werden, die sicherstellt, dass nur authorisierte Contributor Quell-Code ändern können/dürfen. Weiterhin hat die open source-Anforderung auch hohe Auswirkungen auf den Lizenzpreis der Software, da die gesamte Entwicklung der für den MaBiS-Hub speziell zu realisierende Module als auch alle Basis / Infrastruktur-Module von dem einen Kunden MaBiS-Hub finanziert werden müssen. Gleiches gilt für den Support und die Weiterentwicklung der Module. Das bedeutet eine Umstellung des Geschäftsmodell des Softwarehersteller. Hierdurch sehen sich evtl. Hersteller aus anderen Branchen / oder Projekthersteller im Vorteil, was bei der langfristigen Wartung, Pflege und Weiterentwicklung Herausforderungen mit sich bringen kann.	o Open Source alleine ist kein Garant für sichere Software. Open Source lebt von großen Communities mit vielen Contributoren und von mehreren Maintainern für das Projekt. o Angreifer könnten such versuchen Schwachstellen einzubringen (Beispiel liblzma library und SSH, CVE-2024-3094) o Neben Open Source können auch externe Reviews, Lieferantenaudits und Quellcodehinterlegung als Vertrauensanker beitragen. o In 5.4 wird bereits der externe code review sicherheitskritischer Module gefordert. o Hersteller- und Kunden-Tests könnten durch Testdefinitionen der Netzbetreiber, Lieferanten und Bilanzkreisverantwortlichen über die Governance ergänzt werden.	KISTERS AG
1.1.	Technische Gesamt-anforderungen	o Anwendung des ACID-Modells (Atomicity, Consistency, Isolation, Durability) auf alle transaktionsbasierten Prozesse o Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten	Wir empfehlen den Entfall der Forderung des ACID-Modells.	Bei Festlegung auf ACID ist es nicht möglich, ein verteiltes System aufzubauen mit Konsistenz, hoher Verfügbarkeit und Ausfalltoleranz ("Das CAP-Theorem oder Brewers Theorem besagt, dass es in einem verteilten System unmöglich ist, gleichzeitig die drei Eigenschaften Consistency (Konsistenz), Availability (Verfügbarkeit) und Partition Tolerance (Ausfalltoleranz) zu garantieren.", Quelle: https://de.wikipedia.org/wiki/CAP-Theorem). Dieses ist allerdings eine übliche Architektur für den Aufbau horizontal skalierbarer Systeme (siehe Kapitel 4.3) zur Verarbeitung großer Datenmengen.	KISTERS AG
1.1.	Technische Gesamt-anforderungen	Datenmanagement o Nutzung eines kanonischen Datenmodells zur Harmonisierung der Datenflüsse	Konkretisierung auf die Gestaltung der Schnittstellen sollte erfolgen. Die eigentliche Datenablage im System sollte davon abweichen können. Darüber hinaus sollten in den Schnittstellen nur die im jeweiligen Prozess benötigten Informationen ausgetauscht werden und irrelevanten Informationen entfallen (Datensparsamkeit, Performance, etc.).		KISTERS AG

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen		Umstellung der IT-Systeme bremst Fortschritt in anderen Bereichen	Die Energiewende fordert im Bereich Strom die Netzbetreiber, Messstellenbetreiber und Liefe-ranten in außerordentlicher Weise. Die Umstellungen, die die Einführung eines MaBiS-Hubs mit sich bringen würde, kämen zusätzlich zu anderen notwendigen Veränderungen hinzu und wird deren Umsetzung verlangsamen. Die Ankündigung, die regelmäßigen Formatänderungen im Umsetzungsjahr auszusetzen kann nur bedingt für Erleichterung sorgen. Vielmehr stellt der in 2029 für neun Monate geplante Parallelbetrieb des aktuellen und des neuen Übertragungsweges die Branche vor große Herausforderungen. Der Verteilnetzbetreiber muss sicherstellen, dass in Format und Auswahl unterschiedlich zu versendende Daten am Ende zu gleichen Bilanzierungsergebnissen führen.	Klafka & Hinz Energie-Informations-Systeme GmbH
1.1.	Technische Gesamt-anforderungen		volkswirtschaftliche Kostensteigerung	Die bestehenden dezentralen Systeme der VNB müssen geändert werden, Schnittstellen zum geplanten MaBis-Hub müssen entwickelt werden. Der Aufbau der zentralen Aggregationsstelle und deren Betrieb wird zusätzlich erhebliche finanzielle Aufwände verursachen. Insgesamt steigen die volkswirtschaftlichen Kosten an.	Klafka & Hinz Energie-Informations-Systeme GmbH
1.1.	Technische Gesamt-anforderungen		kein Erfolg bei Datensparsamkeit	Der VNB benötigt schon zur Rechnungskontrolle der DBA die Einzelzeitreihen der Abnahme- und Einspeisestellen. Zudem ist er ja der Betreiber des Netzes. Insbesondere bei der kommenden deutlichen Zunahme des Absatzes von elektrischer Energie sowie der Zunahme von dezentralen Einspeisungen ist die Kenntnis über die genauen Verläufe dieser Netznutzungen wichtig. So werden jetzt digitale Zwillinge für Niederspannungsnetze aufgebaut und in MS-Leitsystemen die RLM-Zeitreihen sichtbar gemacht. Dies dient dazu Netzausbau zu vermeiden und so die Kosten für das elektrische Netz zu senken. Auch für die Umsetzung der gesetzlichen Pflichten aus §14a EnWG benötigt der VNB Einzelzeitreihendaten von Abnahme- und Einspeisestellen, damit er Überlastungen auch entlang von Kabelverläufen feststellen bzw. die Ursache von Spannungsgrenzverletzungen identifizieren kann. Neuartige KI-gestützte Verfahren er-möglichen dabei auch Alterungsanalysen von Betriebsmitteln durchzuführen, wenn langfristige Zeitreihenverläufe von Absatz und Einspeisungen vorliegen.	Klafka & Hinz Energie-Informations-Systeme GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				Auch zur Durchführung der Netznutzungsabrechnung benötigt der Netzbetreiber teilweise Einzelzeitreihen. Insbesondere mit den neuen dynamischen Tarifen für die Netznutzung sind Zeitreihen der MaLos bzw. NeLos notwendig. Zukünftige Weiterentwicklungen der heutigen Tageszeitabhängigen Netzentgelte hin zu dynamisch von der Netzauslastung abhängigen Tarife sollten direkt mitgedacht werden. Die Abwicklung der Abnahme- und Förderpflichten nach dem Erneuerbare-Energien-Gesetz und dem Kraft-Wärme-Kopplungsgesetz basiert ebenfalls auf Einzelzeitreihen. Dies gilt ebenso zur ordnungsgemäßen Bestimmung der Konzessionsabgabe nach der Konzessionsabgabenverordnung.	
1.1.	Technische Gesamt-anforderungen		Zentrales vs. dezentrales System	In der Energiewirtschaft wird das n-1-Kriterium sehr hoch gehalten. Übertragen lässt sich dies, üblicherweise für Netzkomponenten angewendete Prinzip auch für die Abrechnung. Aktuell gibt es in Deutschland hunderte verteilte Abrechnungssysteme. Wenn eines, aus welchem rund auch immer ausfällt, können einige Endverbraucher, Lieferanten o. ä. nicht abgerechnet werden. Was passiert aber, wenn alle Systeme ihre Daten zentral von einem "single point of truth" erhalten? Was passiert, wenn dieser MaBiS-Hub ausfällt? Dann wird der "single pont of truth" zum "single point of failure" und in ganz Deutschland kann niemand mehr irgendwen abrechnen – die ganze Energiebranche bekommt kein Geld mehr. Das Ausfallrisiko lässt sich durch Parallelisierung / Schaffung von Redundanzen verringern. Das ist aber nur die Hardwareseite. Die Software, die auf allen Systemen läuft ist immer die gleiche. Wenn es dort einen Fehler gibt, z. B. nach einem Update, fallen auch alle gespiegelten Systeme aus. Diese Vorstellung spricht gegen die derzeitige Konzeption des MaBiS-Hubs, welche ein zentrales System vorsieht.	Klafka & Hinz Energie-Informations-Systeme GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	Standardisierte, dokumentierte APIs (z.B. REST mit OpenAPI-Spezifikation)	Die Energiebranche steht schon jetzt vor großen Herausforderungen, die in Zukunft nur noch wachsen werden. Bereits heute zeigt sich, dass die bisherigen EDIFACT-basierten Datenformate die Komplexität des Marktes nur noch schwer abbilden können. Dazu kommt, dass im aktuellen Modell versucht wird, diese hochkomplexen Datenstrukturen mit einer kaum noch überschaubaren Anzahl an Geschäftsprozessen zwischen den unzähligen Systemen aller Akteure synchron zu halten. Dies ergibt ein sehr hohes Fehlerpotenzial, welches jeder Marktteilnehmer im laufenden Geschäft zu spüren bekommt. Mit Kraken entwickeln wir eine globale Energieplattform, auf der bereits heute über 70 Mio. Lieferstellen laufen, davon über eine 1 Million in Deutschland. Auf Basis dessen und insbesondere auch aus unseren Erfahrungen in anderen Ländern begrüßen wir das Vorhaben der Bundesnetzagentur zur Einführung eines zentralen MaBiS-Hub daher ausdrücklich. Wir sind überzeugt, dass zentrale, leistungsfähige Datenplattformen der entscheidende Schlüssel für die zukünftige Energiewirtschaft sind. Jedoch birgt ein IT-Projekt dieser Größenordnung hinsichtlich Kosten, Dauer und Komplexität natürlich auch große Risiken. Daher ist es aus unserer Sicht extrem wichtig, durchweg auf offene & bewährte Standards und Strukturen zu setzen. Dies führt nicht nur dazu, dass durch die umsetzenden Softwarefirmen bereits existierende Lösungen und Softwarebibliotheken wiederverwendet werden können und somit Zeit und Kosten gespart werden, sondern es führt durch die global etablierten Standards auch zu einer höheren Stabilität und dadurch zu einer besseren Datenqualität.	(Im Text links mit eingearbeitet)	Kraken Labs Ltd.

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
			Dies bedeutet auch, dass es nicht reicht, die bestehenden Prozesse in ihrer aktuellen Form einfach von “EDIFACT über AS4” zu “JSON über HTTP” umzuwandeln. Damit würden wir all die Probleme der “alten Welt” in die “neue Welt” mitnehmen. Dies kann man beispielhaft an den spezifizierten “REST”-Endpunkten sehen, die zwar “JSON über HTTP” transportieren, aber eben nicht REST-Prinzipien entsprechen und stattdessen versuchen, die alten Prozesse aus der EDIFACT-Welt im JSON-Format umzusetzen. (https://edi-energy.github.io/Konzept_API_Strom/) Dies möchten wir an zwei Beispielen illustrieren: So werden in der Spezifikation POST-Requests zur Abfrage von Werten benutzt. Wenn man sich jedoch den Wikipedia Artikel zu REST anschaut (https://de.wikipedia.org/wiki/Representational_State_Transfer) steht dort klar, dass die Aufgabe von POST wie folgt lautet: “Fügt eine neue Ressource unterhalb der angegebenen Ressource ein”. Stattdessen sieht der REST-Standard für eine solche Aufgabe den GET-Request vor. Zu diesem lautet die klar passende Erklärung: “Fordert die angegebene Ressource vom Server an”. Ein weiterer Punkt wäre die eigentlich geforderte Zustandslosigkeit von REST. Hierzu sagt Wikipedia: “Weder der Server noch die Anwendung soll Zustandsinformationen zwischen zwei Nachrichten speichern”. Dies wird in den spezifizierten Endpunkten durch die Verwendung von “transactionIds” nicht eingehalten. All dies ließe sich lösen, indem die APIs wie von REST gefordert ressourcenorientiert umgesetzt werden würden. Dies würde auch dem entsprechen, wie REST-APIs global existieren und genutzt werden. Im Rahmen dessen möchten wir auch nochmal auf unseren Vorschlag vom letzten Jahr zur Malo-Ident-API hinweisen. In dieser API existieren diese Probleme ja ebenfalls und unser Vorschlag eliminiert diese durch ein paar Änderungen an der Ausgestaltung: https://tech.octopus.energy/mako-3.0-proposal/. Ebenfalls empfehlen wir die Richtlinien der britischen Regierung zu REST-APIs, die hier öffentlich zugänglich sind: https://www.gov.uk/guidance/gds-api-technical-and-data-standards		

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
			Zusammenfassend möchten wir sagen: Kraken begrüßt das Vorhaben der Bundesnetzagentur zum zentralen MaBiS-Hub als Schlüssel für die zukünftige Energiewirtschaft. Um jedoch die Risiken dieses IT-Großprojekts zu minimieren, fordern wir die konsequente Nutzung offener, global bewährter REST-Standards. Die bloße Übertragung komplexer EDIFACT-Prozesse in ein "JSON über HTTP"-Format ohne Beachtung von REST-Prinzipien (ressourcenorientiert, zustandslos, korrekte HTTP-Verben, etc.) ist unzureichend und würde die alten Probleme beibehalten. Wir schlagen vor, die Schnittstellenspezifikationen an diese essenziellen REST-Prinzipien anzupassen. Dies halten wir für notwendig, um die angestrebte Stabilität, Datenqualität und Zukunftsfähigkeit des Hubs zu erreichen.		
1.1.	Technische Gesamt-anforderungen	Standardisierte, dokumentierte APIs (z.B. REST mit OpenAPI-Spezifikation)	Eine REST-Architektur auf Ressourcenbasis mit guter Dokumentation (OpenAPI), sinnvoller Ereignisorientierung sowie asynchronen, robusten Schnittstellen ist zu begrüßten. Der vorgestellte Ansatz, SOAP-Logik im OpenAPI-Gewand fortzuführen (ein Endpunkt, fast nur POST, kaum echte Ressourcen), konserviert die Komplexität. Das zeigt sich auch in historischen Artefakten der deutschen Marktkommunikation (z. B. EDI-Ansätze). Deshalb gilt: entweder SOAP oder echtes REST – ohne Hybridisierung, die die Nachteile beider Welten vereint. Konkret lässt sich auf die bereits existierenden Web-Services des Marktstammdatenregisters verweisen, die historisch auf SOAP/WSDL basieren. Diese Dienste waren ein wichtiger erster Schritt in Richtung Web-Schnittstellen, taugen jedoch nicht als Blaupause für eine moderne, skalierbare Marktkommunikation. Statt SOAP in OpenAPI zu „imitieren“, sollten ressourcenorientierte REST-Schnittstellen mit sauberer Versionierung, klaren Fehlersemantiken, fein granulierten Endpunkten und Events/Subscriptions (inklusive Zustellquittungen) etabliert werden – im Sinne etablierter Public-Sector-API-Guidelines. Ergänzend empfehlen wir, die GPKE-Logik nicht reflexhaft „API-gleich“ zu ändern, sondern wo nötig gezielt zu entkoppeln: Geschäftsprozesse bleiben fachliche Orchestrierungen, technische Schnittstellen liefern die robusten, beobachtbaren Bausteine dafür.	Siehe Hinweis/Anmerkung	Mako365 GmbH
1.1.	Technische Gesamt-anforderungen	ACID-Prinzipien als Systemgrundlage		Die ACID Prinzipien für verteilte Systeme zu Fordern ist in der Informatik umstritten (siehe https://de.wikipedia.org/wiki/ACID). Siehe zusätzlich CAP-Theorem welche die technische Machbarkeit der Erfüllung aller ACID Eigenschaften im Konflikt mit hoher Verfügbarkeit sieht. Vorschlag: diese techische Anforderung auf relistische BASE-Prinzipien umstellen. Zusätzlich sollte eine fundierte Abwägung hinsichtlich Konsistenz und Verfügbarkeit erfolgen und welche dieser beiden Richtungen präferiert werden soll.	SAP SE

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	Unterstützung von Schnittstellen für andere Hubs / Plattformen (Interoperabilität)	Punkt unter Schnittstellenmanagement	Es muss präzisiert werden was für weitere Schnittstellen unterstützt werden sollen, andernfalls kann jede beliebige externe Schnittstelle gemeint sein, was eine unnütze und sinnfreie Aussage darstellt.	SAP SE
1.1.	Technische Gesamt-anforderungen	Open Source * Der vollständige Quellcode der Anwendung ist unter einer anerkannten Open-Source-Lizenz (z. B. Apache 2.0) zu veröffentlichen * Offene Bereitstellung und Pflege von Dokumentationen und Schnittstellenspezifikationen	Die Aussage ist zu streichen und durch die folgende zu ersetzen: Der Quellcode muss für die Auftraggeber immer und für von ihnen beauftragte Erfüllungsgehilfen einsehbar sein. Vertragliche vereinbarte Vertrauligkeitsvereinbarungen sind dabei einzuhalten. Die aktuelle Dokumentation und Schnittstellenspezifikationen müssen öffentlich zur Verfügung gestellt werden. Sowohl für alle im Rahmen des bestellten Gewerke sind die Rechte von Auftraggeber und Auftragnehmer zu wahren.	Die Forderung nach einer Open-Source-Lizenz bei der der Auftragnehmer Rechte an vorhandener in das Projekt eingebrachter Software aufgeben müsste, schließt am Markt verfügbare und etablierte Lösungen aus und vergrößert das Risiko einer längeren Projektlaufzeit.	Schleupen SE
1.1.	Technische Gesamt-anforderungen	Anwendung des ACID-Modells (Atomicity, Consistency, Isolation, Durability) auf alle transaktionsbasierten Prozesse'	Anpassung notwendig.	Die Forderung schränkt den möglichen Lösungsraum zu stark ein. Insbesondere stark skalierende, verteilte Softwaresysteme verwenden in der Regel alternative Verfahren zur Sicherung der Datenkonsistenz, um die zu erwartenden Performance-Anforderungen zu erfüllen (z. B. erfordern in verteilten Systemen ACID-Transaktionen in der Regel Transaktionskoordinatoren, die ihrerseits neue Komplexität und damit Fehleranfälligkeit in das System einführen). Die Kopplung zwischen den Teilsystemen nimmt zu was deren Wartung erschwert. Das Dokument sollte aus unserer Sicht die zu erreichenden Ziele beschreiben (Anforderungen), ohne die Möglichkeiten der technischen Realisierung einzuschränken (eher das "Was" beschreiben als das "Wie").	Schleupen SE
1.1.	Technische Gesamt-anforderungen	Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten	Anpassung notwendig.	Die Forderung schränkt den möglichen Lösungsraum zu stark ein. Insbesondere stark skalierende, verteilte Softwaresysteme verwenden in der Regel alternative Verfahren zur Sicherung der Datenkonsistenz, um die zu erwartenden Performance-Anforderungen zu erfüllen (z. B. erfordern in verteilten Systemen ACID-Transaktionen in der Regel Transaktionskoordinatoren, die ihrerseits neue Komplexität und damit Fehleranfälligkeit in das System einführen). Die Kopplung zwischen den Teilsystemen nimmt zu was deren Wartung erschwert. Das Dokument sollte aus unserer Sicht die zu erreichenden Ziele beschreiben (Anforderungen), ohne die Möglichkeiten der technischen Realisierung einzuschränken (eher das "Was" beschreiben als das "Wie").	Schleupen SE

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
1.1.	Technische Gesamt-anforderungen	Nutzung eines kanonischen Datemodells zur Harmonisierung der Datenflüsse	Anpassung notwendig.	Kanonische Datenmodelle haben sich insbesondere bei größeren Systemen als eher hinderlich erwiesen (Stichworte: SOA + Enterprise Service Bus-Systeme mit kanonischen Datenmodellen). Insbesondere entsteht schnell der Nachteil, dass Datenstrukturen (z.B. eine Person) für alle denkbaren Anwendungsfälle die gleiche Struktur haben, obwohl je nach Anwendungsfall nur eine Teilmenge benötigt wird. Ferner besteht bei rein kanonischen Modellen die Gefahr, dass Änderungen nahezu alle Softwareteile betreffen, selbst wenn sie nur für einzelne Anwendungsfälle relevant sind. Architekturansätze wie DDD verfolgen das Ziel, Daten kontextbezogen zu modellieren (eine Person kann in einem Kontext der Rechnungsempfänger, in einem anderen der Eigentümer sein). Im Sinne eines einfachen Datenaustausches ist es sicherlich sinnvoll, Objekte so weit zu harmonisieren, dass gleiche Felder von Objekten den gleichen Aufbau haben. Das Dokument sollte aus unserer Sicht die zu erreichenden Ziele beschreiben (Anforderungen), ohne die Möglichkeiten der technischen Realisierung einzuschränken (eher das "Was" beschreiben als das "Wie").	Schleupen SE
1.1.	Technische Gesamt-anforderungen	Open Source o Der vollständige Quellcode der Anwendung ist unter einer anerkannten Open-Source Lizenz (z. B. Apache 2.0) zu veröffentlichen o Offene Bereitstellung und Pflege von Dokumentationenund Schnittstellen Spezifikatione	Die eingesetzte 3rd-Party-Software, Module, Bibliotheken usw. sollten ebenfalls Open Source sein, weil nur damit der gesamte MaBiS-Hub vollständig überprüft werden kann. Siehe dazu auch 5.3 Software Bill of Materials. Für eine vollständige Sicherheitsprüfung müssen auch die eingesetzten 3rd-Party-Komponenten überprüfbar sein (vgl. aktuelle Supply-Chain-Angriffe).		SWM Infrastruktur GmbH & Co. KG
2.1.	Reaktions- und Antwortzeiten	zu "Service Level Objectives (SLO)", erster Aufzählungspunkt: o End-to-End Latenzbudget (Perzentile): P50=100ms, P95=500ms, P99=1000ms	Wir sind nicht in der Lage, diese Aussage in ein Gesamtbild einzusortieren (auch unter Berücksichtigung der SLO-Begriffsbeschreibung im Kapitel "Definitionen" ist uns dies nicht möglich). Auf welche End-to-End-Beziehung bezieht sich die Aussage?	Bitte um Konkretisierung, um Missverständnisse zu vermeiden.	BDEW
2.1.	Reaktions- und Antwortzeiten	Allgemein	Metriken für Skalierung und Performance-Degradation fordern – Metriken sollten bezogen sein auf eine definierte Systemlast (wie lange darf eine definierte Anfrage dauern, wenn z.B. bereits 1000 solcher Anfragen aktiv sind?). Welche Metriken beziehen sich auf ein aktuelles Arbeits-Set, Z.B. von Werten der letzten drei Tage – im Unterschied z.B. zur Anfrage von historischen Werte von letztem Jahr, die nicht im Cache vorliegen.	Die beschriebenen Metriken scheinen für ein monolithisches System gedacht zu sein, nicht für ein horizontal skaliertes Cloud System. Hier sollten sinnvolle Metriken gefunden werden, die tatsächlich in der Praxis relevante Performance-Anforderungen abbilden. Synthetische Metriken können sehr hohe Kosten verursachen, ohne praktischen Nutzen zu stiften.	decarbon1ze GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
2.1.	Reaktions- und Antwortzeiten	SLOs	Auf welche Art der Anfragen beziehen sich die Latenzen? Warum 100ms? 500ms? Hier sollten besser für ausgewählte Prozesse und Ressourcen-Abrufe realistische Werte unter Last angegeben werden.	Für echte REST-APIs, wie wir sie in anderen Kommentierungsblättern vorgeschlagen haben, kann eine Anfrage vom Client aus gesehen umfangreiche synchrone Datenbank-Abfragen und Berechnungen auslösen, und somit realistisch einige Sekunden in Anspruch nehmen. Dennoch ist systemisch eine synchrone Antwort innerhalb eines definierten Timeout (z.B. 15s) oftmals besser als eine sehr schnelle Antwort (100ms) mit dann folgender asynchroner Verarbeitung und einer asynchronen Rückmeldung des Ergebnisses später. Beispiel hier ist die Prüfung einer eingehenden Berechnungsformel, wie in unserem Kommentar Nr. 5 zur WiM Teil II ausgeführt.	decarbon1ze GmbH
2.1.	Reaktions- und Antwortzeiten	Systemauslastungsgrenzen CPU-Auslastung: P99 ≤ 80% RAM-Auslastung: P99 ≤ 80%	Hier sollten keine Grenzen vorgegeben werden	Entscheidend ist ob der Hub Anfragen korrekt und schnell genug bearbeiten kann. Ob dies mit einer Auslastung >80% geschieht spielt dabei keine Rolle.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
2.1.	Reaktions- und Antwortzeiten	End-to-End Latenzbudget (Perzentile): P50=100ms, P95=500ms, P99=1000ms	Ändern in: Umformulieren des End-to-end Latenzbudgets in "Antwortzeiten". Die Perzentil Angaben sollen gestrichen werden. Und durch folgende Formulierung ersetzt werden: Die Antwortzeiten sollen im weiteren Verlauf festgelegt werden, in Abhängigkeit der umzusetzenden APIs und Prozesse.	- Ein End-to-End Latenzbudget kann durch den MaBiS-Hub nicht gewährleistet werden, da kein Einfluss auf die Internet Kommunikationsstrecken und Infrastruktur der Marktpartner vorhanden ist - Eine Unterscheidung in „Client-Visible Latency“ und einer „Time to persist / time to business completion“ erscheint sinnvoll. - vor dem Hintergrund des genannten: Umbenennung in Antwortzeit. Eine definition der Antwortzeiten zum aktuellen Zeitpunkt ist sehr schwer möglich, dies könnte zu unverhältnismäßigem Mehraufwand führen.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
2.1.	Reaktions- und Antwortzeiten	• Allgemein: o Überwachung und Dokumentation der vorgegebenen Zielwerte als Messgröße	Bitte ergänzen: • Allgemein: o Überwachung und Dokumentation der vorgegebenen Zielwerte als Messgröße. Es sind KPIs der High- und Low-Watermarks zu definieren.	Das Monitoring und Reporting beschreibt, wann, welcher Report an wen gehen soll (siehe im weiteren Textverlauf 9. Monitoring und Reporting). Der Sinn des Satzes in jetziger Form ist unverständlich.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
2.1.	Reaktions- und Antwortzeiten	zu "Service Level Objectives (SLO)", erster Aufzählungspunkt: o End-to-End Latenzbudget (Perzentile): P50=100ms, P95=500ms, P99=1000ms	Wir sind nicht in der Lage, diese Aussage in ein Gesamtbild einzusortieren (auch unter Berücksichtigung der SLO-Begriffsbeschreibung im Kapitel "Definitionen" ist uns dies nicht möglich). Auf welche End-to-End-Beziehung bezieht sich die Aussage? Wir können die Aussage dahingend verstehen, sofern damit gemeint ist, dass der MV und BA in sich jeweils über dessen verschiedenen "internen" Verbindungen eine Latenz einhalten müssen (innerhalb interner Services, den Back-Up-Systemen (s. Kapitel 3.3) oder den Services im Cloud-Verbund (s. Kapitel 4.1). In wie weit man eine Latenz über das weitere Netz/andere Marktteilnehmer vorschreiben möchte, ist uns nicht klar. Selbstverständlich kann man über Datenübertragungswege sinnvolle, latente Wege vorgeben. Dies findet unserer Ansicht nach jedoch bereits heute über die Vorgaben durch EDI@Energy statt. Sofern hierzu eine Überarbeitung im Rahmen der Einführung des MaBiS-Hubs gewünscht ist, ist es unserer Ansicht nach jedoch sinnvoll, dies konkret an den BDEW zu formulieren.	Bitte um Konkretisierung, um Missverständnisse zu vermeiden.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
2.1.	Reaktions- und Antwortzeiten	Systemauslastungsgrenzen CPU-Auslastung: P99 ≤ 80% RAM-Auslastung: P99 ≤ 80%	In einem Kubernetes System wäre das die mittlere Auslastung aller MultiCore-CPUs der beteiligten Knoten? Je nach Betriebsplattform hat die Auslastung einer einzelnen realen oder virtuellen CPU und RAM keine Aussagekraft.		KISTERS AG
2.1.	Reaktions- und Antwortzeiten	End-to-End Latenzbudget	Punkt unter Service Level Objectives	Bitte Begriff End-to-End Latenzbudget definieren.	SAP SE
2.1.	Reaktions- und Antwortzeiten	Systemauslastungsgrenzen o CPU-Auslastung: P99 ≤ 80% o RAM-Auslastung: P99 ≤ 80%	Punkt unter Service Level Objectives	Für welche Komponente soll diese Systemauslastung gelten (Datenbank, Applikationsserver, oder an einer Interfaceinteraktion beteiligte Microservices) oder gilt das für alle genutzten Komponenten oder ist die SLO eine Mittelwert für alle genutzten Komponenten? Bitte konkretisieren.	SAP SE
2.2.	Anfragen-verarbeitung	Anfragenverarbeitung ≥ 1.000 gleichzeitige API-Aufrufe pro Sekunde (RPS)	Anfragenverarbeitung ≥ 1.000 gleichzeitige API-Aufrufe pro Sekunde (RPS) ohne fachliche Prüfung	Wir gehen davon aus, dass sich die Anfrageverarbeitung von 1000 gleichzeitigen API-Aufrufen pro Sekunde keine fachliche Prüfung der übertragenen Nachrichten beinhaltet sondern sich rein auf den Webservice bezieht.	Arvato Systems Digital GmbH
2.2.	Anfragen-verarbeitung	Für API-Anfragen/-Antworten ist die Payload (Body) auf o 2MB maximal beschränkt o Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden	Für API-Anfragen/-Antworten ist die Payload (Body) auf o 256kb maximal beschränkt o Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden	Die maximale Dateigröße der z.B. JSON sollte von 2MB auf 256kb begrenzt werden die dies eine Standardgröße bei den Hyperscaler ist und sich somit einfacher händeln lassen was sich positiv auf die Reaktions- und Antwortzeiten auswirkt.	Arvato Systems Digital GmbH
2.2.	Anfragen-verarbeitung	Dritter Aufzählungspunkt, zweiter Unterpunkt: o Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden	Wir schlagen vor, dass dies, wie bisher über EDI@Energy vorgegeben/geregelt wird.	Nur so ist der geforderte Wunsch nach der Verwendung von Komprimierungen sinnvoll und einheitlich im Markt anwendbar.	BDEW
2.2.	Anfragen-verarbeitung	--	Wir können den Unterschied zwischen dem Begriff "Reaktionszeit" (Kapitel 2.1.) und "Anfrageverarbeitung" nicht erkennen.	Bitte um Konkretisierung, um Missverständnisse zu vermeiden.	BDEW

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
2.2.	Anfragen-verarbeitung	Dritter Aufzählungspunkt, zweiter Unterpunkt: o Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden	Wir schlagen vor, dass dies, wie bisher über EDI@Energy vorgegeben/geregelt wird.	Nur so ist der geforderte Wunsch nach der Verwendung von Komprimierungen sinnvoll und einheitlich im Markt anwendbar.	Bielefelder Netz GmbH
2.2.	Anfragen-verarbeitung	Datenempfang	Auf welche APIs bezieht sich die Forderung von 1000 Requests/s? Auf echte REST-APIs, oder auf den Empfang von Nachrichten über Webdienste? Warum genau 1000?	Anforderungen an die Performance des Empfangs hängen stark davon ab, wie viel synchrone Prüfung erfolgen soll. Je besser die Prüfung beim (synchronen) Aufruf, desto weniger fehlerhafte Daten kommen ins System, desto schneller können Client-Systeme ohne aufwändiges Clearing später ihre Anfragen korrigieren. Pauschal 1000 Requests/s festzulegen, ist ohne Kontext nicht sinnvoll	decarbon1ze GmbH
2.2.	Anfragen-verarbeitung	Payload-Größe	Keine Begrenzung auf einen festen Wert. Aber: Forderung nach einer Maximalgröße, welche auf Seiten der Infrastruktur durchgesetzt werden kann (z.B. in Load-Balancern).	Warum die Begrenzung der Payload Größe hier? Zum aktuellen Zeitpunkt sind solche Werte willkürlich und können negative Auswirkungen auf die Entwicklung haben. Besser: Während der Entwicklung darf ein sinnvoller Wert festgelegt werden – nachdem die Systemarchitektur steht, die Schnittstellen-Technologie bekannt ist (REST oder Webservice), und die Grundzüge der Verarbeitung von Requests und der Persistenz entworfen sind.	decarbon1ze GmbH
2.2.	Anfragen-verarbeitung	Komprimierung	Standard-Komprimierung auf Ebene der Transport-Infrastruktur ist zu nutzen (HTTP/2 mit HPACK)	Komprimierung erfolg heute auf Ebene der Infrastruktur standardmäßig, wenn REST-APIs und TLS gemäß Stand der Technik zum Einsatz kommt. Weitere ad-hoc Komprimierung auf Anwendungsebene ist kontraproduktiv.	decarbon1ze GmbH
2.2.	Anfragen-verarbeitung	Für API-Anfragen/-Antworten ist die Payload (Body) auf 2MB maximal beschränkt	Sollte innerhalb EDI@Energy behandelt werden	Die Vorgaben haben deutliche Auswirkungen auf die Schnittstellengestaltung und sollten nicht innerhalb der IT-Leitlinien behandelt werden	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
2.2.	Anfragen-verarbeitung	Anfragenverarbeitung ≥ 1.000 gleichzeitige API-Aufrufe pro Sekunde (RPS)	Ergänzen: Zum Schutz vor Missbrauch und Lastspitzen muss ein sinnvolles Rate Limit inkl. Burst je Marktpartner festgelegt werden können. Die Werte können unterschiedlich je Größe des Marktteilnehmers ausfallen. Ein Beispiel hierfür könnte sein: Große Marktpartner (>100.000 MaLo) -> 200-500 RPS (Burst bis 1000 RPS für max 30 sek	Diese Forderung dient dem Schutz des MaBiS-Hubs. Ressourcen können hierdurch auch effizienter genutzt werden. Die genaue Höhe der Rate Limits und Burst Werte muss noch herausgearbeitet werden	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
2.2.	Anfragen-verarbeitung	• Anfragenverarbeitung ≥ 1.000 gleichzeitige API-Aufrufe pro Sekunde (RPS)	Bitte ergänzen: Die Anfragequeue darf auf maximal 10% seines Gesamtvolumens ansteigen. Die Verweildauer in der Queue pro Anfrage darf nicht mehr als 2 Sekunden betragen (Latenz). Es ist ein Autoscaler in Kombination mit einem Loadbalancer zu verwenden	Der Wert ist sehr starr und kann dazu führen, dass ein nicht benötigter, riesiger Maschinenpark aufgebaut wird. Es könnte umgekehrt aber auch sein, dass die vorhandenen Maschinen nicht ausreichen. Sämtliche Requests, die an einen Hub gehen, werden üblicherweise in eine sog. Request Queue eingespeist, die je nach Anzahl vorhandener Threads mehr oder weniger parallel/sequentiell abgearbeitet wird. Entscheidend ist also, dass die Anfragen nicht zu lange in der Queue verweilen. Dazu gibt es heute - gerade im containerisierten Umfeld (z. B Kubernetes) Möglichkeiten, Instanzen (also zusätzliche Rechner) hinzuzunehmen bzw. abzuschalten, wenn diese nicht benötigt werden. Dieses sog. Autoscaling spart Geld, Energie und Ressourcen und ist weniger starr als die Anzahl von API-Aufrufen.	E.ON Netze
2.2.	Anfragen-verarbeitung		Bitte neuen Aufzählungspunkt ergänzen: • Für langlaufende Prozesse werden Eventqueues (SSE, Web Sockets bzw. MQTT oder vergleichbare) verwendet. Die Laufzeit dafür kann unbegrenzt sein. Poll-Mechanismen sind verboten.	Es gibt langlaufende Prozesse. In der Regel wird dann der Request sofort mit einem Response und z. B. einer QueueID an den Marktpartner bestätigt. Der Marktpartner weiß mit diesem Response, dass der MaBiS-Hub zur Verarbeitung länger benötigt. Mit Eventqueues meldet sich der MaBis-Hub aktiv beim Marktpartner, wenn die Verarbeitung abgeschlossen ist. Der Marktpartner soll nicht über Pollmechanismen laufend anfragen dürfen, welchen Status die Verarbeitung hat.	E.ON Netze
2.2.	Anfragen-verarbeitung	--	Wir können den Unterschied zwischen dem Begriff "Reaktionszeit" (Kapitel 2.1.) und "Anfrageverarbeitung" nicht erkennen.	Bitte um Konkretisierung, um Missverständnisse zu vermeiden.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
2.2.	Anfragen-verarbeitung	Dritter Aufzählungspunkt, zweiter Unterpunkt: o Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden	Wir schlagen vor, dass dies wie bisher über EDI@Energy vorgegeben/geregelt wird. Des Weiteren schlagen wir in diesem Zuge vor, dass die Dateigröße nicht wie im Dokument fix mit 2 MB vorgegeben wird, sondern in Abhängigkeit zur Komprimierungstechnologie über edi@energy definiert wird.	Nur so ist der geforderte Wunsch nach der Verwendung von Komprimierungen sinnvoll und einheitlich im Markt anwendbar und die Vorgabe von Dateigrößen folgt dem für den MaBiS-Hub relevanten Stand der Technik.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
2.2.	Anfragen-verarbeitung	Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden	Theoretisch ist eine Komprimierung bei jeder Anfrage in der Payload möglich. Trade off zwischen Gewinn durch weniger zu übertragender Daten und CPU Zeit für Komprimierung und Dekomprimierung. Sollte durch Gremien wie edi@energy einheitlich geregelt werden		KISTERS AG
2.2.	Anfragen-verarbeitung	Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden		Bitte konkretisieren, insbesondere wo Komprimierungsalgorithmen für Payload nicht einsetzbar sind.	SAP SE
2.2.	Anfragen-verarbeitung	Für API-Anfragen/-Antworten ist die Payload (Body) auf * 2 MB maximal beschränkt * Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden	Wir schlagen vor, dass diese Regelungen weiterhin durch die EDI@Energy Dokumente vorgegeben werden. Daher ist die Aussage aus den IT-Leitlinien zu streichen.	Diese Regelungen sollten nicht in einer Prozessbeschreibung festgelegt werden. Stattdessen sollten die Relegungen immer wieder überprüft und Änderungen über die halbjährlichen Konsultationen eingebracht werden können.	Schleupen SE

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
2.2.	Anfragen-verarbeitung	Für API-Anfragen/-Antworten ist die Payload (Body) auf o 2MB maximal beschränkt o Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden	Wie folgt anpassen: Für API-Anfragen/-Antworten ist die Payload (Body), auf o 2MB beschränkt. o Wo eine Komprimierung möglich ist, ist diese zwingend anzuwenden. Es ist ein allgemein anerkannter und etablierter Komprimierungsalgorithmus für alle, wie z.B. GZIP oder 7zip gleichermaßen zu verwenden.	Für die Anwendung von Komprimierungen ist eine einheitliche und klare Regelung im Markt erforderlich. Aus Kosten- und Effizienzgründen sollte sich auf einen möglichst von vielen Anwendungen unterstützen und gut verfügbaren Algorithmus verständiigt werden. Die Regelungen dazu sollten wie bisher auch für die anderen MaKo-Verfahren durch edi@energy und deren untergeordneten PG erarbeitet und in einer spezifischen Hub-RzÜ festgelegt werden.	Vattenfall Euope Sales GmbH
3.	Verfügbarkeit	fehlt	Ergänzung als Vorgabe zum Standort: Standort des Rechenzentrums ist Deutschland		SWM Infrastruktur GmbH & Co. KG
3.1.	Technische Verfügbarkeit		Anforderungen anpassen an Cloud-Architektur	Verfügbarkeit ist vorgegeben wie bei einem traditionellen Server-System. Für Cloud-Anwendungen mit horizontaler Skalierung sollte unterschieden werden zwischen einem kompletten Ausfall (auf Ebene der Infrastruktur) sowie Degradation der Performance wegen Problemen in der horizontalen Skalierung. Auch hier stellt sich die Frage, warum genau die angegebenen Werte gewählt wurden. Wenn es keinen nachvollziehbaren harten Grund gibt, scheint es besser, die Entwurfsphase abzuwarten. Kleine Unterschiede in den Anforderungen können sehr teure Lösungen bedingen (oder eben nicht), ohne dass Kunden des Systems nachher davon profitieren	decarbon1ze GmbH
3.1.	Technische Verfügbarkeit	• SLO Technische Verfügbarkeit: o Kernsystem: ≥99,95% (max. ~22 min Downtime pro Monat)	• SLO Technische Verfügbarkeit: o Kernsystem: Ausfall pro Jahr max. 25 h	Bessere, interpretationsfreie Lesbarkeit als prozentuale Angaben. Die ausgefallenen Minuten können auf das gesamte Kalenderjahr kumuliert werden.	E.ON Netze
3.1.	Technische Verfügbarkeit	Technische Verfügbarkeit: o Kernsystem: ≥99,95% (max. ~22min Downtime pro Monat)	Konkretisierung notwendig.	1) Die Forderung ist grundsätzlich nachvollziehbar, führt aber in ihrer Absolutheit ggf. zu erheblichen zusätzlichen Betriebsaufwänden. Wie zum Beispiel der letzte mehrstündige Ausfall der Region us-east-1 bei AWS gezeigt hat, braucht es für diese Verfügbarkeits-Anforderung in Verbindung mit der Restore-Anforderung von 22 Minuten (siehe 3.3) in dieser Konstallation (AWS) wahrscheinlich eine Replikation zwischen zwei Regions (also >= 2 Datacenter mit >=2 AZs). 2) Je nach Ausgestaltung der Schnittstellen zwischen MaBiS-Hub und den restlichen Marktteilnehmern (MSB, NB, ..) ist zu berücksichtigen, dass die kürzesten Fristen in der Marktkommunikation derzeit 15 Minuten für neg. CONTRLs und 45 Minuten für APERAKs sind. Aktuell gibt es jedoch keine Downtime-Regelung für WebAPIs, diese sollten für alle WebAPIs in der Marktkommunikation erstellt werden.	Schleupen SE
3.2.	Betriebs-verfügbarkeit	Dritter und vierter Aufzählungspunkt: • Wartungsarbeiten und damit verbundene Einschränkungen sind 7 Tage vor Durchführung anzukündigen, sofern diese an Wochenenden durchgeführt werden • Wartungsarbeiten und damit verbundene Einschränkungen sind 14 Tage vor Durchführung anzukündigen, sofern diese an einem Werktag durchgeführt werden müssen	Ausfallzeiten sind aufgrund der erforderlichen Resilienz auf ein absolutes Minimum zu reduzieren (High Availability under High Load). Ideal ist eine Verfügbarkeit von 100%. Planbare Wartungen müssen daher zwingend an "nicht WT" durchgeführt werden.		Bielefelder Netz GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
3.2.	Betriebs-verfügbarkeit	• SLO Betriebsverfügbarkeit: o Kernsystem: ≥99,68%: (technische Verfügbarkeit + 24h (geplante) Downtime pro Jahr)	• SLO Betriebsverfügbarkeit: o Kernsystem: ≥99,68%: (technische Verfügbarkeit + 48 h (geplante) Downtime pro Jahr)	365 * 24 = 8760; 8760 * 99,68 / 100 ~ 8732; 28 = 8760 - 8732; => 2 1/4 Tage Totalausfall pro Jahr!!! Eine Umrechnung auf Monat macht wenig Sinn, da Downtimes in der Regel für größere Systemupdates geplant sind. 22 Minuten sind aus heutiger technischer Sicht mit QS und Rollbackverfahren nicht machbar. Daher sollte eher ein Jahreswert publiziert werden.	E.ON Netze
3.2.	Betriebs-verfügbarkeit	Dritter und vierter Aufzählungspunkt: • Wartungsarbeiten und damit verbundene Einschränkungen sind 7 Tage vor Durchführung anzukündigen, sofern diese an Wochenenden durchgeführt werden • Wartungsarbeiten und damit verbundene Einschränkungen sind 14 Tage vor Durchführung anzukündigen, sofern diese an einem Werktag durchgeführt werden müssen	Zusammenfassung der beiden Punkte und Anpassung der Zeitvorgaben: • Wartungsarbeiten und damit verbundene Einschränkungen sind mindestens einen Monat vor Durchführung anzukündigen	Insbesondere die in Kapitel "Anfragenvearbeitung" beschriebene Hauptlast des Datenempfangs von Werten, aber auch die Datenübermittlung von Werten basiert auf "T" und nicht auf "WT". Aus diesem Grund sollte unabhängig davon, ob die Wartungsarbeit an einem Werktag stattfindet oder nicht, gleichermaßen vorab informiert werden. Insbesondere, wenn die mit den Wartungsarbeiten verbundenen Einschränkungen Aufwände bei den Marktpartner verursachen - ggf. an einem Nicht-Werkttag - ist eine rechtzeitige Einplaung der Kapazitäten notwendig. Wir sehen daher keine Reduzierung der Ankündigungszeit, nur weil die Wartungsarbeit und damit ggf. einhergehender Einschränkungen an einem Nicht-Werktag erfolgt. Des Weiteren sind im Standard Wartungsarbeiten langsfristig planbar, haben jedoch in den meisten Fällen immer Auswirkungen auf den Markt, der sich darauf IT-technisch und/oder personell einstellen muss. Wartungsarbeiten müssen unserer Ansicht nach daher mindestens einen Monat vor Durchführung angekündigt werden.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
3.2.	Betriebs-verfügbarkeit	Wartungsarbeiten und damit verbundene Einschränkungen sind 7 Tage vor Durchführung anzukündigen, sofern diese an Wochenenden durchgeführt werden	Neben Bugfixing und inhaltlichen / regulatorischen Anpassungen ist auch von sehr kurzfristigen CVE-Behebungen auszugehen. Diese sind nach BSI so schnell wie möglich umzusetzen, was keine solche Vorankündigungszeit zulässt.		KISTERS AG
3.2.	Betriebs-verfügbarkeit	geplante Downtime ist als Gesamtbudget für ein Jahr zu verstehen und kann verteilt werden [,,,] * Wartungsarbeiten und damit verbundene Einschränkungen sind 7 Tage vor Durchführung anzukündigen, sofern diese an Wochenenden durchgeführt werden * Wartungsarbeiten und damit verbundene Einschränkungen sind 14 Tage vor Durchführung anzukündigen, sofern diese an einem Werktag durchgeführt werden müssen	geplante Downtime ist als Gesamtbudget für ein Jahr zu verstehen und kann verteilt werden [...] * Wartungsarbeiten und damit verbundene Einschränkungen sind 7 Tage vor Durchführung anzukündigen, sofern diese an Wochenenden durchgeführt werden * Wartungsarbeiten und damit verbundene Einschränkungen sind 14 Tage vor Durchführung anzukündigen, sofern diese an einem Werktag durchgeführt werden müssen * Adhoc-Downtimes zur Abwendung von Schäden sind möglich	Zur Abwendung von Schäden und längeren Ausfällen müssen in drigenden Fälllen Downtimes mit kürzeren Vorlaufzeiten möglich sein.	Schleupen SE

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
3.2.	Betriebs-verfügbarkeit	* Wartungsarbeiten und damit verbundene Einschränkungen sind 7 Tage vor Durchführung anzukündigen, sofern diese an Wochenenden durchgeführt werden * Wartungsarbeiten und damit verbundene Einschränkungen sind 14 Tage vor Durchführung anzukündigen, sofern diese an einem Werktag durchgeführt werden müssen	Wie folgt anpassen: * Wartungsarbeiten und damit verbundene Einschränkungen sind mindestens 20 Werktage vor Durchführung anzukündigen	Die Ankündigungsfristen sind zu kurz. Auch ist unklar, warum diese in Abhängigkeit des Ereignistages, Werktag oder Wochenende, unterschiedlich sein sollen. Die MP müssen sich auf das Ereignis vorbereiten können und z.B. DL umplanen und ggf. Personal für die wiederinbetriebnahme bereit halten. Zudem könnten die MP mit ausreichend Vorlauf das Wartungsfenster nutzen um selbst synchron Wartungsarbeiten vornehmen zu können.	Vattenfall Euope Sales GmbH
3.3.	Backups & Disaster Recovery	Test und Verifizierung o Funktions- und Backuptests des/der Systems(e) sind halbjährlich durchzuführen und zu protokollieren	Statt Backuptests müsste es Restore- und Wiederherstellungstest heißen.		BDEW
3.3.	Backups & Disaster Recovery	Wiederherstellungszeit o Zulässige Zeitspanne bis zur Wiederherstellung bei Ausfall von Systemkomponenten, -diensten, -prozessen, & -funktionen als Recovery Time Objective (RTO): o Kernsysteme: ≤ 22min o Unterstützende Systeme: ≤ 2h	Recovery Times sollten realitisch überprüft und angepasst werden. Zu kurze Recovery times was nur redundante Systeme bedeuten kann, was in der Funktionalität zu überprüfen wäre. - > in 22min schafft man in der Regel keinen Restore eines Systems.	Bzgl. RTO / RPO Zeit sollte bewusst sein, das im Rahmen eines Cloudverfahren ein Wechsel des Cloudprovider innerhalb der genannten Zeit möglich sein sollte. Die Störungen/Ausfälle der Clouds (AWS, Azure etc.) in den letzten Monaten haben > 22 Min. gedauert. Es ist unwahrscheinlich, dass die Cloudprovider entsprechende SLAs anbieten. Auch redundante Systeme auf derselben Cloudinfrastruktur helfen hier nicht.	BDEW
3.3.	Backups & Disaster Recovery	Backup-Protokolle von vollständigen Backups sind zu erstellen	Unveränderliche (immutable) Backups sind zu bevorzugen.	Zur Sicherstellung, dass Backups im Nachgang nicht verändert oder gelöscht werden können.	BDEW
3.3.	Backups & Disaster Recovery	zu "Backups", Unterpunkt "Grundlegend", erster Aufzählungspunkt: Anwendung 3-2-1 Prinzip für alle vollständigen Backups: 3 gesamt, 2 auf unterschiedlichen Medien am gleichen Ort und 1 Backup an einem anderen Ort (Georedundanz)	Ergänzung um einen zusätzlichen Satz: Anwendung 3-2-1 Prinzip für alle vollständigen Backups: 3 gesamt, 2 auf unterschiedlichen Medien am gleichen Ort und 1 Backup an einem anderen Ort (Georedundanz). Der physische Standort des Hostings (vertragliche Zusicherung) ist Deutschland.	Wir schlagen ein Hosting in Deutschland aus Gründen der Sicherheit vor.	Bielefelder Netz GmbH
3.3.	Backups & Disaster Recovery		Anforderungen anpassen an Cloud-Architektur	Die Anforderungen klingen wiedrum stark auf ein konventionelles Server-System bezogen, nicht auf ein Cloud-System. In letzterem werden Daten typischerweise bereits im Wirkbetrieb mehrfach repliziert, um die nötige Leistungsfähigkeit zu erzielen. Daher scheint es sinnvoller, Ziele für das Backup anzugeben anstatt konkreter technischer Vorgaben. Z.B., dass Daten immer an zwei geografisch getrennten Orten liegen müssen.	decarbon1ze GmbH
3.3.	Backups & Disaster Recovery	•Durchführung : oViertelstündliche Snapshots, Aufbewahrungszeit 1 Tag oTägliche inkrementelle Backups, Aufbewahrungszeit 7 Tage oWöchentlich vollständige Backups, Aufbewahrungszeit 30 Tage oMonatlich vollständige Backups werden 12 Monate lang aufbewahrt	Jährlich vollständige Backups impliziert, dass diese auch eingespielt werden müssen. Dies stellt einen unverhältnismäßigen Mehraufwand an das System dar und sollte gestrichen werden.	Das System muss dann über einen Zeitraum von einem Jahr vollständig rückwärts kompatibel sein. Sprich auch alle Softwareversionen etc. müssen vorgehalten werden. Gegen eine reine Archivierung und Aufbewahrung der Daten spricht jedoch nichts.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
3.3.	Backups & Disaster Recovery	Backups sind, unter Berücksichtigung der aktuell geltenden Best-Practice-Vorgaben des Bundesverbands IT-Sicherheit, zu verschlüsseln und vor unbefugten Zugriffen zu schützen	Referenzierung des Verbandes IT-Sicherheit streichen.	Es existiert aktuell keine Verpflichtung auf den Stand der Technik des Bundesverband IT-Sicherheit. Das BSI reklamiert ebenfalls die Definition des Stands der Technik für sich. Wenn dann sollte es nur als Empfehlung aber nicht als verpflichtend berücksichtigt werden. Backups sind zu verschlüsseln und vor unbefugtem Zugriff zu schützen.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
3.3.	Backups & Disaster Recovery	Test und Verifizierung o Funktions- und Backuptests des/der Systems(e) sind halbjährlich durchzuführen und zu protokollieren	Statt Backuptests müsste es Restore- und Wiederherstellungstest heißen.	Nachschärfung	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
3.3.	Backups & Disaster Recovery	Wiederherstellungszeit o Zulässige Zeitspanne bis zur Wiederherstellung bei Ausfall von Systemkomponenten, -diensten, -prozessen, & -funktionen als Recovery Time Objective (RTO): o Kernsysteme: ≤ 22min o Unterstützende Systeme: ≤ 2h	Recovery Times sollten realistisch überprüft und angepasst werden. Zu kurze Recovery times was nur redundante Systeme bedeuten kann, was in der Funktionalität zu überprüfen wäre. - > in 22min schafft man in der Regel keinen Restore eines Systems.		Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
3.3.	Backups & Disaster Recovery	zu "Backups", Unterpunkt "Grundlegend", erster Aufzählungspunkt: Anwendung 3-2-1 Prinzip für alle vollständigen Backups: 3 gesamt, 2 auf unterschiedlichen Medien am gleichen Ort und 1 Backup an einem anderen Ort (Georedundanz)	Ergänzung um einen zusätzlichen Satz: Anwendung 3-2-1 Prinzip für alle vollständigen Backups: 3 gesamt, 2 auf unterschiedlichen Medien am gleichen Ort und 1 Backup an einem anderen Ort (Georedundanz). Der physische Standort des Hostings (vertragliche Zusicherung) ist Deutschland.	Wir schlagen ein Hosting in Deutschland aus Gründen der Sicherheit vor.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
3.3.	Backups & Disaster Recovery	o Backups sind, unter Berücksichtigung der aktuell geltenden Best-Practice-Vorgaben des Bundesverbands IT-Sicherheit, zu verschlüsseln und vor unbefugten Zugriffen zu schützen	Referenzierung des Verbandes IT-Sicherheit.	Wieso wird hier nicht auf eine Vorgabe des BSI refrenziert, sondern auf einen Verband? Ggf. kann das BSI auf solche Empfehlungen eines Verbandes verweisen, wie die BNetzA auf den BDEW / edi@energy, aber damit obliegt die laufende Kontrolle weiter der Behörde.	KISTERS AG
3.3.	Backups & Disaster Recovery	Wiederherstellungszeit o Zulässige Zeitspanne bis zur Wiederherstellung bei Ausfall von Systemkomponenten, -diensten, -prozessen, & -funktionen als Recovery Time Objective (RTO): o Kernsysteme: ≤ 22min o Unterstützende Systeme: ≤ 2h	Unterscheidung zwischen Art des Ausfalls. Bei einem Komplettausfall eines Rechenzentrums ist innerhalb von 22 min auch bei Snapshots des Datenstandes ein Recovey der Kubernetes / OS-Umgebung, als Backup aus "nicht Snapshot" Backups nur durch weitere Geo-Redundanz leistbar. Im Fall des Ausfalls einzelner Komponenten können die Snapshots ausreichend sein.	Kosteneffizienz kann durch Orientierung der Wiederherstellungszeit an den durchgeführten Geschäftsprozessen erzielt werden.	KISTERS AG
3.3.	Backups & Disaster Recovery	Disaster Recovery Plans (DRP) sind zu erstellen, umzusetzen, kontinuierlich zu testen und zu überprüfen in Bezug auf o Szenarien: Systemkomplettausfall, Sicherheitsvorfall, Rechenzentrumsausfall	Was heißt in diesem Zusammenhang kontinuierlich? Sind z.B. durch automatisiert provozierte Ausfälle einzelner Komponenten bis zu ganzen Rechenzentren im laufenden Betrieb durchzuführen. Ist in einem solchen laufenden Testausfall eines Rechenzentrums gleichzeitig immer noch die Anforderung der Georedundanz sicherzustellen?		KISTERS AG

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
3.3.	Backups & Disaster Recovery	* Backups * Grundlegend: […]	Konkretisierung ist notwendig.	Im Abschnitt wird das 3-2-1-Prinzip mit einem georedundanten Backup („1 Backup an einem anderen Ort“) gefordert. Wir bitten um Klarstellung, ob das georedundante Backup ebenfalls in die geforderte Wiederanlaufzeit (RTO/RPO) einzubeziehen ist oder ob sich die RTO/RPO ausschließlich auf die lokal am primären Standort verfügbaren Sicherungen bezieht. Hintergrund: Eine Wiederherstellung aus einem georedundanten Backup über eine WAN-Strecke ist in der Regel mit längeren Transferzeiten verbunden und kann daher nicht dieselbe RTO/RPO wie ein lokales Backup erfüllen. Die RTO sollte anhand des BSI-Standarts für BCM 200-4 definiert werden bzw. sich die Vorgaben darauf beziehen.	Schleupen SE
3.3.	Backups & Disaster Recovery	* Backups * Durchführung: […]	Konkretisierung ist notwendig.	Im Abschnitt werden konkrete Backup-Mechanismen (Snapshots, inkrementelle und vollständige Backups) genannt. Wir bitten um Klarstellung, ob diese Angaben als verbindliche technische Vorgaben zu verstehen sind oder lediglich die funktionalen Anforderungen (z. B. Sicherungsintervall, maximaler Datenverlust, Aufbewahrungsfristen und Wiederherstellbarkeit) beschreiben sollen. Sollte Letzteres zutreffen, bitten wir um präzisierende Angabe, welche funktionalen Mindestanforderungen (RPO/RTO) verbindlich einzuhalten sind, sodass die konkrete Backup-Technologie durch den Auftragnehmer frei wählbar bleibt. Die RTO sollte anhand des BSI-Standarts für BCM 200-4 definiert werden bzw. sich die Vorgaben darauf beziehen.	Schleupen SE
3.3.	Backups & Disaster Recovery	* Backups * Test und Verifizierung: […]	Bitte um Klarstellung zum Punkt „Test und Verifizierung – Funktions- und Backuptests des/der Systems(e) sind halbjährlich durchzuführen und zu protokollieren“:	Bezieht sich diese Anforderung ausschließlich auf Funktionsprüfungen des Backup-Systems und die stichprobenartige Wiederherstellung gesicherter Daten (Überprüfung der Lesbarkeit und Integrität der Backups), oder ist eine vollständige Wiederherstellung des gesamten Services inklusive aller angebundenen Systeme und externer Kommunikation gemeint? Für den Fall, dass Letzteres gefordert ist, bitten wir um Änderung, dass eine jährliche Durchführung als ausreichend angesehen wird, da der Aufwand für einen vollständigen Service-Test erheblich ist. Bezieht sich die Aussage der Funktionstest auf die Backup-Lösung oder auf ein konkret Wiederhergestelltes Backup-Szenario? Wenn das Backup-Szenario gemeint ist, müssen vollständige End-2-End-Funktionstest durchgeführt werden? Nach aktuellen Regeln der Marktkommunikation ist in ein Test im Echtsystem nicht möglich.	Schleupen SE

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
3.3.	Backups & Disaster Recovery	* Wiederherstellungszeit * Kernsysteme: ≤ 22min	Anpassung ist notwendig.	Die genannte Wiederherstellungszeit (RTO) von ≤ 22 Minuten ist grundsätzlich für den Ausfall einzelner Systemkomponenten, Container oder Netzwerkdienste erreichbar. Im Falle einer Beschädigung oder Korruption der zugrunde liegenden Datenbank ist dieser Wert jedoch als nicht realistisch einzuschätzen, da eine vollständige Wiederherstellung aus einem Backup – insbesondere bei größeren Datenbeständen – in der Regel mehr Zeit erfordert. Eine RTO von ≤ 22 Minuten wäre in diesem Szenario nur durch ein aktives Failover mit synchroner Replikation erreichbar. Dies stellt jedoch kein Backup im eigentlichen Sinne dar, da fehlerhafte oder korrupte Datenbankinhalte in diesem Fall ebenfalls auf das Zweitsystem übertragen würden. Eine asynchrone Replikation (z. B. über Read-Replica-Mechanismen) kann in diesem Zusammenhang eine sinnvolle Ergänzung darstellen, da sie eine zeitversetzte Kopie der Datenbank bereitstellt, die im Falle einer Korruption auf der Primärinstanz noch einen konsistenten Datenstand enthält. Dabei ist jedoch zu berücksichtigen, dass ein solches Verfahren sowohl die Kosten als auch die Komplexität der Umgebung deutlich erhöht und die Recovery-Point-Objective (RPO) separat zu bewerten ist. Wenn ein Fehler auf der Primärdatenbank nicht rechtzeitig erkannt wird, besteht das Risiko, dass der fehlerhafte Zustand mit der nächsten Replikation auch auf die Zweitinstanz übertragen wird, sodass nur ein älterer, zeitlich weiter zurückliegender Datenbankstand wiederhergestellt werden kann. Die RTO sollte anhand des BSI-Standarts für BCM 200-4 definiert werden bzw. sich die Vorgaben darauf beziehen.	Schleupen SE
4.1.	Technische Voraus-setzungen	mandantenfähige Architektur	Mandantenfähigkeit streichen	Was sind die Mandanten hier? Laut Spezifikation soll es zwei Kernsysteme geben, eines für die MV-Rolle, eines für die BA-Rolle. Von diesen Rollen gibt es nur eine Instanz, also scheinen Mandanten nicht nötig. Oder sollen in Zukunft auch andere Marktrollen mit eigenen Mandanten vertreten sein? Z.B. NB-Mandanten, unter denen NB jeweils ihre Stammdaten ablegen und pflegen können?	decarbon1ze GmbH
4.1.	Technische Voraus-setzungen	cloud-native	Konsequenz auf andere Anforderungen überdenken und konsistent anwenden. Technische Detailanforderungen streichen, aber dafür die Ziele klar formulieren (siehe die Kommentare zur Performance und Verfügbarkeit). Anforderungen an die Data-Center und Betreiber präzisieren	Unter dem Begriff "Cloud-native" können sehr unterschiedliche Anforderungen gemeint sein. Grundsätzlich ist es richtig, für die erwartete Last ein hoizontal skalierbares System vorzusehen. Ob dies in Containern läuft oder auf VMs sollte aber auf technischer Ebene entschieden werden, ebenso die Frage der Orchestrierung (Kubernetes, Rancher, etc.). Wichtig wären Anforderungen an den Betrieb: Dürfen US-Hyperscaler als Betriebs-Infrastruktur verwendet werden trotz der Gefahren durch den US Cloud-Act? Braucht es eigene Data-Center?	decarbon1ze GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
4.1.	Technische Voraus-setzungen	Cloud-native, mandantenfähige und containerisierte Architektur • Unterstützung von horizontaler und vertikaler Skalierung • Nutzung standardisierter Plattformtechnologien (z. B.Kubernetes,OpenShift) • Lose Kopplung der Komponenten zur Verbesserung von Wartbarkeit und Erweiterbarkeit	Bitte ergänzen: • Container bzw. virtuelle Konstrukte (VM), sind auf mindestens 3 räumlich getrennte Rechenzentren zu verteilen. Der physische Abstand der Zentren muss mindestens 100 Kilometer betragen und innerhalb der Grenzen der europäischen Union liegen. • Container sind „loadbalanced“ und „recoverable”. D. h. es gibt Ersatzendpunkte, sollte es zu Ausfällen kommen.	Zu "Räumlich getrennte Rechenzentren": • Georedundanz und Katastrophenschutz o Durch räumlich getrennte Rechenzentren wird verhindert, dass regionale Ausfälle (z. B. Stromausfall, Naturkatastrophe, Brand, Überflutung) alle Instanzen gleichzeitig betreffen. o Ein Mindestabstand von 100 km stellt sicher, dass Zentren unterschiedlichen Risikozonen angehören (andere Energieversorgung, Telekommunikation, geologische Risiken). • EU-Datenhoheit und regulatorische Anforderungen o Speicherung und Verarbeitung innerhalb der EU ist essenziell zur Einhaltung der DSGVO, des EU Data Act, der NIS2-Richtlinie und branchenspezifischer Vorgaben (z. B. BNetzA-IT-Sicherheitskatalog, ENTSO-E/ACER-Regeln). o Es wird sichergestellt, dass kein Datentransfer in Drittstaaten erfolgt, der zusätzlichen Compliance-Aufwand oder rechtliche Unsicherheit verursachen würde. • Verfügbarkeit nach BSI- und ISO-Standards o Hochverfügbare Dienste nach BSI-IT-Grundschutz oder ISO 27001/22301 fordern mehrfache Standorte mit unabhängiger Infrastruktur (Netze, Strom, Kühlung). o Eine Dreifach-Redundanz erlaubt Failover- und Wiederanlaufstrategien ohne Datenverlust (Recovery Point ≈ 0, Recovery Time ≈ kurz). • Betriebliche und organisatorische Trennung o Unterschiedliche Rechenzentren ermöglichen getrennte Betreiber- oder Verantwortlichkeitsbereiche, was das Risiko von Fehlkonfigurationen und Insider-Threats reduziert. Zu Loadbalancing & Recoverability: • Load Balancing – gleichmäßige Lastverteilung und Fehlertoleranz o Durch Load Balancing wird sichergestellt, dass keine einzelne Instanz überlastet wird. o Bei Ausfall oder Wartung einzelner Container erfolgt die automatische Umschaltung auf andere, aktive Endpunkte. o Dies erhöht Performance und Stabilität, besonders bei hohen Transaktionsvolumina • Recoverability	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				o Container-Orchestrierungssysteme (z. B. Kubernetes, OpenShift) erkennen defekte Instanzen und starten automatisch neue Container auf verfügbaren Ressourcen. o Dies ermöglicht automatisches Failover ohne manuellen Eingriff, wodurch die SLA-Verfügbarkeit (z. B. 99,9 %) eingehalten werden kann. • Business Continuity & Disaster Recovery o Durch Kombination von Loadbalancing und Recoverability wird eine kontinuierliche Dienstbereitstellung (HA-Cluster) erreicht, selbst bei Hardware- oder Netzwerkausfällen. o Für kritische Marktkommunikationssysteme (z. B. BIKO- oder Aggregationsdienste) ist dies Voraussetzung für regulatorisch geforderte Wiederanlaufzeiten < 2 h. • Effiziente Nutzung der Infrastruktur o Lastverteilung erlaubt dynamische Skalierung je nach Bedarf (z. B. Spitzenlast bei Monatsabrechnungen). o Dies reduziert Kosten, ohne die Ausfallsicherheit zu beeinträchtigen.	
4.1.	Technische Voraus-setzungen	Lose Kopplung der Komponenten zur Verbesserung von Wartbarkeit und Erweiterbarkeit	Die in den Leitlinien geforderte lose Kopplung der Komponenten wird durch eine modulare, ressourcenorientierte Architektur – wie sie bei modernen Microservice-Ansätzen üblich ist und häufig auf REST basiert – besonders gut unterstützt. REST-APIs fördern klare, stabile Schnittstellen zwischen fachlich abgegrenzten Modulen und ermöglichen damit eine flexible Erweiterbarkeit des Gesamtsystems.	Eine strikt modularisierte Architektur mit sauber abgegrenzten Verantwortlichkeiten reduziert Abhängigkeiten zwischen Komponenten. REST-APIs tragen wesentlich dazu bei, da sie: •auf klar definierten Ressourcen und standardisierten HTTP-Methoden basieren, •eindeutige und langlebige Schnittstellen bereitstellen, •und einen technologieneutralen, leicht verständlichen Kommunikationsstil ermöglichen.	Hochfrequenz Unternehmensberatung GmbH
4.1.	Technische Voraus-setzungen	Technische Voraussetzungen • Cloud-native, mandantenfähige und containerisierte Architektur • Nutzung standardisierter Plattformtechnologien (z. B. Kubernetes, OpenShift) • Lose Kopplung der Komponenten zur Verbesserung von Wartbarkeit und Erweiterbarkeit		Diese Aussagen limitieren den Implementierer auf auf spezifische, gerade aktuelle Technologien ("cloud-native", "containerisierte Architektur", "lose Kopplung") und sind nicht technologieoffen formuliert und können auf unterschiedlichste Art und Weise interpretiert werden wobei es keine klaren Entscheidungskriterien gibt, ob eine konkrete Implementierung diesen Voraussetzungen nun genügt oder nicht. Weiterhin ist unklar, was "standardisierte Plattformtechnologien" sind. Sind hier eher verbreitete Plattformtechnologien gemeint oder welche Standardisierung ist hier konkret gefordert? Bitte diese Voraussetzungen streichen.	SAP SE
4.2.	Neue Funktionen und Services	Erweiterbarkeit	Anstatt Erweiterbarkeit lieber leichte Anpassbarkeit (Refactoring) fordern.	Die aufgeführten Anforderungen sind eher Wunschdenken als praktikabel. Natürlich sollen Systeme erweiterbar sein. Aber Anpassungen an unbekannte neue Gesetze und Regelungen ohne Re-Design zu versprechen, ist unseriös. Ein sehr wichtiger Punkt moderner Software-Architektur ist das "you ain't gonna need it" Prinzip (YAGNI) – also entgegen der Anforderungen hier sollte nur das entworfen und gebaut werden, was aktuell tatsächlich gebraucht wird. Denn alle Vorhalten erzeugen zusätzliche Komplexität. Daher ist es besser, die Software auf sowieso unausweichliche Änderungen am Code vorzubereiten (einfaches Refactoring), anstatt eine sehr komplexe modulare Architektur zu entwerfen, die später dennoch nicht zu neuen Anforderungen passt.	decarbon1ze GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
4.2.	Neue Funktionen und Services	Anpassung an gesetzliche oder regulatorische Änderungen ohne Re-Design	Wenn das Marktmodell und das Modell in der Software auseinanderlaufen, führt das zu ggf. deutlich erhöhten Pflegeaufwänden, wegen Unübersichtlichkeit und Fehleranfälligkeit. Daher sollte das so nicht gefordert werden. Besser wäre "Anpassungen an gesetzliche oder regulatorische Änderungen sind mit minimalen Ausfallzeiten, idealerweise im laufenden Betrieb umzusetzen."	Da die Software Geschäftsprozesse abbildet, wird eine grundlegende Änderung dieser Prozesse sinnvollerweise eine Designanpassung der Software nach sich ziehen. Zusätzlich sollte eine Weiterentwicklung des Systems hinsichtlich interner technischer Realisierungen ermöglicht werden.	KISTERS AG
4.2.	Neue Funktionen und Services	Systemarchitektur ist modular und erweiterbar ausgelegt: o Neue Funktionen sollen als eigenständige Module ergänzt werden können o Keine tiefgreifenden Änderungen am bestehenden Kernsystem erforderlich		Diese Forderungen können für ein konkretes Design auf verschiedenste Art und Weise bewertet und interpretiert werden. Aus Sicht eines Implementierers eines MaBis Hubs ist unklar wer diese Kriterien unter welchen Standards bewertet. Bitte anpassen und auf die Forderung Erweiterbarkeit konzentrieren, aber nicht versuchen vorzuschreiben wie die Erweiterbarkeit erreicht wird.	SAP SE
4.2.	Neue Funktionen und Services	Erweiterbarkeit betrifft etwa: o Anpassung an gesetzliche oder regulatorische Änderungen ohne Re-Design		Seriös kann niemand diese Forderung erfüllen, da zukünfige gesetzliche oder regulatorische Änderungen unbekannt sind und damit nicht abgeschätzt werden kann ob dadurch Designänderungen notwendig werden. Bitte diese Anforderung steichen.	SAP SE
4.3.	Verhalten bei Last		Anforderungen konsistent anpassen zu Anforderungen an Konsistenz, Transaktionshandling, Backup, etc.	Die Anforderungen hier sind generisch sinnvoll für horizontal skalierbare Cloud-Systeme. Sie stehen aber im Widerspruch zu anderen Anforderungen – insbesondere zur ACID-Anforderungen, zum Handling von Transaktionen, und auch die Backup- und Performance-Anforderungen passen nicht zu einer Cloud-Architektur – wie bereits ausgeführt.	decarbon1ze GmbH
4.3.	Verhalten bei Last	Es müssen beliebig viele Instanzen von Services im Live-Betrieb möglich sein	Formulierung anpassen: Die Systemarchitektur muss eine horizontale Skalierung der Services im Live-Betrieb ermöglichen. Die Anzahl der Instanzen darf nicht durch die Softwarearchitektur limitiert sein. Technische und wirtschaftliche Grenzen (z.B. verfügbare Ressourcen, Kosten) sind zu berücksichtigen	"beliebig viele" ist sehr unspezifisch	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
4.3.	Verhalten bei Last	Services und Dienste müssen stateless bereitgestellt werden, um eine maximale horizontale Skalierung gewährleisten zu können	Der geforderte Grundsatz der Statelessness ist ein zentrales Architekturprinzip moderner, ressourcenorientierter REST-APIs. Ein REST-konformes Design fördert von Natur aus stateless Interaktionen zwischen Client und Server und unterstützt damit ideal die in den Leitlinien geforderte horizontale Skalierbarkeit.	Nur durch die konsequente Umsetzung zustandsloser Webservices kann eine Infrastruktur effizient horizontal skaliert werden. Stateless REST-APIs stellen sicher, dass: •jeder Request vollständig verarbeitet werden kann, unabhängig davon, welcher Serverknoten ihn übernimmt, •Lastverteilung flexibel und dynamisch erfolgen kann, ohne komplexe Session- oder Kontextübertragung, •Containerisierung, Cloud-native Skalierungsmechanismen (z. B. Kubernetes Horizontal Pod Autoscaler) und resiliente Betriebsmodelle voll ausgeschöpft werden können. REST ist hierfür besonders geeignet, da das Architekturmodell klar vorsieht, dass jede Ressourcendarstellung alle relevanten Informationen zur Verarbeitung enthält, ohne serverseitige Sitzungskontexte zu benötigen. Dies bildet die Grundlage für kosteneffiziente, hochverfügbare und fehlertolerante Betriebsmodelle, wie sie dem MaBiS-Hub als kritischer Marktinfrastruktur gerecht werden müssen.	Hochfrequenz Unternehmensberatung GmbH
4.3.	Verhalten bei Last	Leistungsfähigkeit insbesondere garantiert bei: o Stark steigendem Transaktionsvolumen von Messwerten o Hohem Änderungsaufkommen von Stammdatenänderungen o Hinzufügen neuer Marktteilnehmer o Ausfällen von einzeln Komponenten bis zu Rechenzentren	Ausfall eines Rechenzentrums: Damit nicht nur Geo-Redundanz (hot-stand-by) sondern laufender Betrieb auf mehreren RZ / Standorten		KISTERS AG
4.3.	Verhalten bei Last	Horizontale und vertikale Skalierbarkeit: Es müssen beliebig viele Instanzen von Services im Live-Betrieb möglich sein		"beliebig viele Instanzen" ist eine rein theoretische Forderung, die kein reales System erfüllen kann. Bitte Anforderung streichen oder präzisieren.	SAP SE
4.3.	Verhalten bei Last	Horizontale und vertikale Skalierbarkeit: Services und Dienste müssen stateless bereitgestellt werden		Wenn hier die externen API gemeint sind, hängt diese Forderung am Design der Marktprozesse. Falls hier interne API gemeint sein sollten, greift diese Forderung stark in das Design der Lösung und ist schwer zu prüfen bzw. zu verifizieren. Bitte präzisieren ob hier öffentliche oder auch interne APIs gemeint sind.	SAP SE

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.	IT- und Daten-sicherheit		Abwägung der Anforderungen gegen Entwicklungsgeschwindigkeit und der Zeit zur Behebung von Schwachstellen.	Die sehr umfangreiche Liste an zertifizierbaren Sicherheitsvorkehrungen klingt auf dem Papier gut, kann aber die Entwicklung und vor allem die Wartung lähmen. Wenn tatsächlich Sicherheitslücken entdeckt werden – typischerweise in einer externen Bibliothek – geht es darum, möglichst rasch einen Patch einzuspielen. Langwierige Freigaben und Genehmigungsprozesse verhindern dies oft. Generell sollte bei einem derart komplexen System das eigentliche Ziel nicht aus dem Auge verloren werden: Das Energiesystem soll dadurch besser funktionieren, und relevante neue Funktionen sollen schneller bereitgestellt werden. Der Branche und dem Land ist nicht geholfen, wenn der Freigabe-Prozess so lange dauert, dass neue gesetzliche Anforderungen nicht in unter einem Jahr umgesetzt werden können.	decarbon1ze GmbH
5.	IT- und Daten-sicherheit		keine spezifischen Anforderungen zum Schutz vor Ransomware	Das mit Abstand größte praktische Risiko derzeit sind Ransomware-Angriffe. Hierzu explizit findet sich in der abstrakten Anforderungsliste nichts.	decarbon1ze GmbH
5.	IT- und Daten-sicherheit		Neben den per SM-PKI authentisierten Marktrollen gibt es keine weiteren Anforderungen an ein Rollenmodell. Welche weiteren Parteien gibt es? (BNetzA, Administratoren verschiedener Kategorien, Auditoren, zukünftig ggf. ein Berechtigungs-Service für Endnutzer?). Es sollten Anforderunge für diese weiteren Rollen und deren Berechtigungen aufgestellt werden.		decarbon1ze GmbH
5.	IT- und Daten-sicherheit	IT- und Datensicherheit	In diesem Kapitel wird IT-Sicherheit und Informationssicherheit vermischt. Die Unterkapitel sollten sachgerecht aufgeteilt werden		Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.	IT- und Daten-sicherheit	5.1. Strategische Ebene: Sicherheitsrahmen und Governance […] * Zertifizierung MaBiS-Hub gem. ISO/IEC 27001 auf Basis BSI IT-Grundschutz […]	Konkretisierung ist notwendig.	Entweder ist eine ISO 27001 oder eine Zertifizierung nach BSI-Grundschutz möglich. Das sind zwei getrennte Dinge.	Schleupen SE
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Umsetzung berücksichtigt die Empfehlungen der Handreichung „Stand der Technik“ des Bundesverband IT-Sicherheit in der jeweils aktuell geltenden Fassung • Zertifizierung MaBiS-Hub gem. ISO/IEC 27001 auf Basis BSI IT-Grundschutz	Verweis auf Bundesverband IT-Sicherheit e.V. streichen. Auf Basis BSI IT-Grundschutz streichen.	Aspekte der Informationssicherheit sollten sich mit den IT-Sicherheitskatalogen der BNetzA decken und sich an den internationalen Standards der ISO 27001 oder anderen orientieren. Der BSI-Grundschutz als Grundlage festzulegen ist nicht geeignet und widerspricht teilweise bestehenden Regelwerken der BNetzA.	BDEW
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Etablierung eines ISMS (ISO/IEC 27001, BSI 200-1 bis 200-3), u.a.:	Verweis auf BSI 200-1 bis 200-3 streichen.	Aspekte der Informationssicherheit sollten sich mit den IT-Sicherheitskatalogen der BNetzA decken und sich an den internationalen Standards der ISO 27001 oder anderen orientieren. Der BSI-Grundschutz als Grundlage festzulegen ist nicht geeignet und widerspricht teilweise bestehenden Regelwerken der BNetzA.	BDEW

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	▪ Regelmäßige Risikoanalysen und -bewertungen, in jedem Fall immer vor geplanten Änderungen am IT-Verbundsystem sowie bei neuerkannten Bedrohungsszenarien	Änderung von "IT-Verbundsystem" im Satz: "▪ Regelmäßige Risikoanalysen und -bewertungen, in jedem Fall immer vor geplanten Änderungen am Kernsystem einschließlich deren unterstützdenden Systemen des MV bzw. des BA sowie bei neuerkannten Bedrohungsszenarien"	Verwendung vorhandener Definitionen, um Missverständnisse zu vermeiden. Wir vermuten Sie meinten mit IT-Verbundsystem das von uns vorgeschlagene.	BDEW
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	▪ Regelmäßige Risikoanalysen und -bewertungen, in jedem Fall immer vor geplanten Änderungen am IT-Verbundsystem sowie bei neuerkannten Bedrohungsszenarien	Änderung von "IT-Verbundsystem" im Satz: "▪ Regelmäßige Risikoanalysen und -bewertungen, in jedem Fall immer vor geplanten Änderungen am Kernsystem einschließlich deren unterstützdenden Systemen des MV bzw. des BA sowie bei neuerkannten Bedrohungsszenarien"	Verwendung vorhandener Definitionen, um Missverständnisse zu vermeiden. Wir vermuten Sie meinten mit IT-Verbundsystem das von uns vorgeschlagene.	Bielefelder Netz GmbH
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Zertifizierung MaBiS-Hub gem. ISO/IEC 27001 auf Basis BSI IT-Grundschutz	Formulierung anpassen: Zertifizierung MaBiS-Hub gem. ISO/IEC 27001	"auf Basis BSI IT-Grundschutz" streichen. Hintergrund die 4ÜNB sind auf Basis der internationalen Norm der ISO27001 zertifiziert. (vgl. EnWG)	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Einrichtung eines BCM gemäß BSI 200-4	Formulierung anpassen: Einrichtung eines BCM gemäß eines anerkannten Standards (z.B. ISO 22301)	Es sollte dem Betreiber hier die Wahlfreiheit gelassen werden, welchen anerkannten Standard er anwenden möchte.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Die Umsetzung muss die relevanten Gesetze und Richtlinien, insbesondere NIS2-Gesetz, IT- Sicherheitsgesetz 2.0, DSGVO, EU AI Act, EU Data Act berücksichtigen	Reduzieren in "Die Umsetzung muss die relevanten und gültigen Gesetze und Richtlinien berücksichtigen."	Verhindern dass neue oder sich ändernde Gesetzteslagen hier keine Berücksichtigung finden	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Schaffung einer automatisierten Datenexportfunktion bis auf Basis Messstellen- granularer Datensätze zur Erfüllung der Vorgaben des EU AI Acts	Gesamten Satz streichen	Wir können die Anforderung nicht nachvollziehen	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Etablierung eines ISMS (ISO/IEC 27001, BSI 200-1 bis 200-3), u.a.:	Verweis auf BSI 200-1 bis 200-3 streichen.	Aspekte der Informationssicherheit sollten sich mit den IT-Sicherheitskatalogen der BNetzA decken und sich an den internationalen Standards der ISO 27001 oder anderen orientieren. Der BSI-Grundschutz als Grundlage festzulegen ist nicht geeignet und widerspricht teilweise bestehenden Regelwerken der BNetzA.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	(neuer zweiter Aufzählungspunkt)	(neuer zweiter Aufzählungspunkt) Die Umsetzung muss eine IT-Architektur aufweisen, die grundsätzlich zu laufenden europäischen Binnenmarktinitiativen anküpfen bzw. erweiterbar ist, insbesondere zum EUDI-Wallet, European Business Wallet (EUBW) und einem europäischen, branchenübergreifenden Ökosystem.	Die EU ist derzeit dabei, den Binnenmarkt für die Energiewirtschaft aufzubauen und definiert dafür von den Nationalstaaten einzuhaltende Richtlinien. Es ist erforderlich, dass die Neuausrichtung der Marktkommunikation dieser Entwicklung folgt.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Umsetzung berücksichtigt die Empfehlungen der Handreichung „Stand der Technik“ des Bundesverband IT-Sicherheit in der jeweils aktuell geltenden Fassung	Bitte streichen	IT-Sicherheit entsteht nicht, wenn zu viele unterschiedliche Regelsetzer gleichzeitig berücksichtigt werden sollen. Mit der Vorgabe des Folge-Spiegelstriches "Zertifizierung MaBiS-Hub gem. ISO/IEC 27001 auf Basis BSI IT-Grundschutz" ist alles gesagt und mit Teilnehmer der SM-PKI (vom BSI) sogar verschärft.	E.ON Netze
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Verwendung von Signaturen und Hashes, die stets dem aktuellen Stand der Technik genügen müssen (aktuell SHA-2)	Bitte streichen.	Das Thema IT-Security besteht nicht nur aus Algortihmen, sondern insbesondere auch aus der Anwendung moderner Protokollversionen und Security by Design. Mit vorherigen Spiegelstrich Zertifizierung gemäß IT-Grundschutz ist Stand der Technik als Minimum vorgeschrieben. Als Teilnehmer der SM-PKI verpflichtet das BSI gleichzeitig die Anwendung modernster Algorithmen (oft als weltweiter Vorreiter vom Forschungsstadium in Industriemaßstab).	E.ON Netze
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	▪ Regelmäßige Risikoanalysen und -bewertungen, in jedem Fall immer vor geplanten Änderungen am IT-Verbundsystem sowie bei neuerkannten Bedrohungsszenarien	Änderung von "IT-Verbundsystem" im Satz: "▪ Regelmäßige Risikoanalysen und -bewertungen, in jedem Fall immer vor geplanten Änderungen am Kernsystem einschließlich deren unterstützdenden Systemen des MV bzw. des BA sowie bei neuerkannten Bedrohungsszenarien"	Verwendung vorhandener Definitionen, um Missverständnisse zu vermeiden. Wir vermuten, Sie meinten mit IT-Verbundsystem, das von uns vorgeschlagene.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Schaffung einer automatisierten Datenexportfunktion bis auf Basis Messstellengranularer Datensätze zur Erfüllung der Vorgaben des EU AI Acts	Wir können die Anforderung nicht nachvollziehen: * Um welche Datenexportfunktion handelt es sich? * Wir gehen bei dem Begriff "Messstelle" von der Messlokation aus. Was bedeutet "bis auf Basis der Messlokation granularer Datensätze"? Um welche Art von Daten handelt es sich dabei? Bezieht sich die Aussage also nur auf den MV, denn nur dieser kennt Messlokationen. Welche Lokationen sind des Weiteren gemeint? * Wer ist der Empfänger der Daten? Warum agiert dieser Empfänger nicht mit API? * Wir sind nicht in der Lage zu erkennen, in welchem Zusammenhang die Datenexportfunktion mit den Vorgaben des AI Acts zusammenhängen soll. Wir vermuten, dass Sie eigentlich den EU Data Act meinten. In diesem Fall sehen wir ebenfalls keine Bewandniss, dass der MV oder BA eine solche Schnittstelle zur Verfügung stellen muss, da die für Kunden relevanten Daten, bei den mit dem Kunden in Kontakt stehenden Marktpartner vorliegen und der Kunde diese dort erfragen kann (ggf. gegen Entgeld). Bei diesen, mit dem Kunden im Vertragsverhältnis stehenden Marktpartnern, sind auch die entsprechenden Ansprechpartner für Kundenkontakt etabliert. Marktparnter hingegen erhalten sowieso die für sie relevanten Daten automatisch über die Marktkommunikationsprozesse und wir gehen daher davon aus, dass Marktpartner die Funktion nicht benötigen.	Konkretisierung, um Missverständnisse zu vermeiden. Wir sehen eine Streichung des Punktes, da wir weder bei dem EU AI Act, noch beim Data Act die Bewandnis von Datenexportstellen für einen Kunden bzw. Marktpartner sehen.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Die Umsetzung muss die relevanten Gesetze und Richtlinien, insbesondere NIS2-Gesetzt, IT-Sicherheitsgesetz 2.0,, DSGVO, EU AI Act, EU Data Act berücksichtigen	Unvereinbarkeit mit DSGVO	Es bleibt unklar, wer als Verantwortlicher i.S. von Art 4 Nr. 7 DSGVO auftritt. Hub-Betreiber agiert als zentraler Auftragsverarbeiter während Marktteilnehmer Datenhoheit verlieren. Damit einher geht ein Konflikt mit Art. 28 DSGVO, wenn keine abgrenzenden Verantwortlichkeiten durch eine Auftragsverarbeitungsvereinbarung festgelegt sind.	Hausheld AG
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Etablierung eines ISMS	Stärkung bestehender Systeme wünschenswert	Hausheld verfügt bereits über einen vollintegrierten Hausheld-Hub, der alle MaBiS-Hub Funktionen abbildet - inklusive Aggregation, Validierung, Redundanz, Monitoring und Reporting. Aufbau, Integratiion und der Betrieb eines zusätzlichen Hubs verursachen signifikante Kosten.	Hausheld AG
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Klare Regelung aller Rollen	Nicht gesichert	Unklare Datenverantwortung und fehlende Zugriffskontrolle.	Hausheld AG
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Umsetzung berücksichtigt die Empfehlungen der Handreichung „Stand der Technik“ des Bundesverband IT-Sicherheit in der jeweils aktuell geltenden Fassung	Referenzierung des Verbandes IT-Sicherheit.	Es sollte auf die Vorgabe z.B. des BSI referenziert werden. Das BSI kann dann auf Empfehlungen eines Verbandes verweisen, wie die BNetzA auf den BDEW / edi@energy, aber damit obliegt die laufende Kontrolle weiter der Behörde.	KISTERS AG
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Schaffung einer automatisierten Datenexportfunktion bis auf Basis Messstellen- granularer Datensätze zur Erfüllung der Vorgaben des EU AI Acts	Es ist nicht ganz klar, wie hier der Bezug zur Anforderung und Rechtsgrundlage besteht. Bitte erläutern/präzisieren		Mako365 GmbH
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	Verwendung von Signaturen und Hashes, die stets dem aktuellen Stand der Technik genügen müssen (aktuell SHA-2)	Punkt unter Etablierung einer wirksamen Data Governance	Bitte präzisieren, was als "aktueller Stand der Technik" gemeint ist. Sind BSI vorgaben gemeint?	SAP SE
5.1.	Strategische Ebene: Sicherheits-rahmen und Governance	letzer Punkt: Verwendung von Signaturen und Hashes, die stets dem aktuellen Stand der Technik genügen müssen (aktuell SHA-2)	Wie folgt anpassen: Die Verwendung von Signaturen und Hashes, sollen stets dem aktuellen Stand der Technik genügen (aktuell SHA-2). Die Nutzung der Signaturen und Hashes werden im Rahmen einer kontinuierlichen Weiterentwicklung durch edi@energy und deren untergeordneten PG erarbeitet und in einer spezifischen MaBiS-Hub-RzÜ festgelegt.	Der Wechsel von Signaturen und Hashes bedarf bei der Vielzahl an Beteiligten eines geordneten Überganges um die Prozesse nicht zu gefährden und die MaKo mit dem MaBiS-Hub aufrecht zu erhalten. Je nach Kompatibilität müssen Wechsel zu einem Stichtag bei allen beteiligten, durch auslaufen lassen oder Wechsel in einem Übergangszeitraum erfolgen. Die Vorgehensweise sollte im Verband durch edi@energy und deren untergeordneten PG erarbeitet und nicht einseitig durch den MaBiS-Hub-Betreiber festgelegt werden.	Vattenfall Euope Sales GmbH
5.2.	Operative Maßnahmen: Sicherheits-management und Prozesse	Anfertigung eines (Fach-)Sicherheitskonzepts nach Standard 200-2 BSI und regelmäßige Aktualisierung; dabei insbesondere bereits in der Konzeptionsphase Feststellung des Schutzbedarfs auf Basis des Architekturkonzepts für Ableitung des Schutzbedarfsniveaus	Verweis auf Standard 200-2 BSI streichen.	Aspekte der Informationssicherheit sollten sich mit den IT-Sicherheitskatalogen der BNetzA decken und sich an den internationalen Standards der ISO 27001 oder anderen orientieren. Der BSI-Grundschutz als Grundlage festzulegen ist nicht geeignet und widerspricht teilweise bestehenden Regelwerken der BNetzA.	BDEW

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.2.	Operative Maßnahmen: Sicherheits-management und Prozesse	•Anfertigung eines (Fach-)Sicherheitskonzepts nach Standard 200-2 BSI und regelmäßige Aktualisierung; dabei insbesondere bereits in der Konzeptionsphase Feststellung des Schutzbedarfs auf Basis des Architekturkonzepts für Ableitung des Schutzbedarfsniveaus	Formulierung anpassen Anwendung des risikobasierten Ansatzes nach ISO27000 Familie	Die ÜNB arbeiten entlang dem risikobasierten Ansatz der ISO27000. Der BSI-Grundschutz als Grundlage festzulegen ist nicht geeignet und widerspricht teilweise bestehenden Regelwerken der BNetzA.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.2.	Operative Maßnahmen: Sicherheits-management und Prozesse	Einrichtung eines effektiven Sicherheits-Patches- und Schwachstellenmanagements gem. der aktuell geltenden Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V.	Einrichtung eines effektiven Sicherheits-Patches- und Schwachstellenmanagements gem. eines anerkannten Standards	Der Begriff „Stand der Technik“ ist ein gängiger juristischer Begriff, hierbei empfehlen wir, nicht auf eine Veröffentlichung eines Bestimmten Bundesverbandes zu verweise, vielmehr soll auf die jeweiligen anerkannten ISO-Normen verwiesen werden	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.2.	Operative Maßnahmen: Sicherheits-management und Prozesse	• Anfertigung eines (Fach-)Sicherheitskonzepts nach Standard 200-2 BSI und regelmäßige Aktualisierung; dabei insbesondere bereits in der Konzeptionsphase Feststellung des Schutzbedarfs auf Basis des Architekturkonzeptsfür Ableitung des Schutzbedarfsniveaus • Etablierung Incident-Response-Prozesse und Notfallpläne inkl. Erstellung interner und externer Informationsketten • Einrichtung eines effektivenen Sicherheits-Patches- und Schwachstellenmanagements gem. der aktuell geltenden Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V.	Bitte ergänzen: • Der Betrieb des MaBiS-Hubs ist nach ITIL Vorgaben aufzubauen (z. B. Incidentmanagement, Changemanagement, Servicedesign, Problemmanagement, ….) • Klare Trennung von Betrieb (Production) und Entwicklung (Laboratory)	Die beiden zu ergänzenden Punkte gehören zu den Grundprinzipien eines kontrollierten, revisionssicheren und stabilen IT-Betriebs, wie er für kritische Infrastrukturen (KRITIS), Datenplattformen vorgeschrieben ist. Betrieb nach ITIL: • Standardisierung und Prozessqualität o ITIL stellt ein international anerkanntes Rahmenwerk für den lebenszyklus-orientierten IT-Betrieb dar. o Durch standardisierte Prozesse (Incident-, Problem-, Change-, Release-, Service-Level-Management etc.) wird eine einheitliche Vorgehensweise in Betrieb und Support gewährleistet. • Nachvollziehbarkeit und Audit-Fähigkeit o Regulatorische und zertifizierungsrelevante Anforderungen (z. B. ISO 20000, ISO 27001, BSI-Grundschutz, NIS2) verlangen dokumentierte Verfahren und Verantwortlichkeiten. o ITIL-basierte Prozesse ermöglichen lückenlose Nachvollziehbarkeit von Änderungen, Störungen und Wiederherstellungen. • Stabilität und Service-Kontinuität	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
				o Durch klare Trennung von Störungsbehebung (Incident), Ursachenanalyse (Problem) und strukturierten Änderungen (Change) werden ungeplante Ausfälle minimiert. o ITIL-Prozesse sichern die Wiederanlaufzeiten (RTO) und Verlustgrenzen (RPO) in kritischen Umgebungen ab. • Kunden- und Nutzerorientierung o Das ITIL-Service-Design stellt sicher, dass IT-Services auf Geschäftsanforderungen abgestimmt sind und deren Qualität messbar bleibt (Service Level Agreements, SLAs). o Dadurch können Services im Sinne der Marktrollen (z. B. BKV, BIKO, NB) zuverlässig bereitgestellt werden. • Kontinuierliche Verbesserung (CSI) o ITIL integriert ein Modell zur laufenden Qualitätsverbesserung („Continuous Service Improvement“) basierend auf Kennzahlen, Audits und Lessons Learned. o Damit wird der Betrieb an veränderte regulatorische und technologische Rahmenbedingungen anpassbar gehalten. Klare Trennung von Betrieb („Production“) und Entwicklung („Laboratory“) • Schutz der Produktionsumgebung o Änderungen in produktiven Systemen ohne Freigabe gefährden die Verfügbarkeit und Datenintegrität. o Eine strikte Trennung verhindert, dass experimentelle oder nicht getestete Softwarekomponenten in den Betrieb gelangen. • Risikominimierung und Change-Kontrolle o Nur freigegebene, getestete Änderungen dürfen über definierte Change-Prozesse (nach ITIL) in die Produktion übernommen werden. o Dadurch werden Risiken durch Fehlkonfigurationen, Sicherheitslücken oder ungetestete Funktionen minimiert. • Revisionssicherheit und Nachvollziehbarkeit o Audits und Sicherheitsprüfungen verlangen eine klare Trennung von Verantwortlichkeiten und Umgebungen („Segregation of Duties“). o Nur autorisierte Personen dürfen Änderungen in der Produktionsumgebung durchführen. • Daten und Datenschutz o Entwicklungs- und Testsysteme dürfen keine produktiven personenbezogenen oder vertraulichen Daten enthalten. o So wird die Einhaltung der DSGVO und interner Sicherheitsrichtlinien gewährleistet. • Stabilität und Kontinuität im laufenden Betrieb o Entwicklungszyklen können unabhängig von produktiven Prozessen laufen. o Updates und Releases werden erst nach vollständiger Validierung und Freigabe integriert. Hieraus entstehen geplante, kontrollierte Produktivsetzungen.	

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.2.	Operative Maßnahmen: Sicherheits-management und Prozesse	Einrichtung eines effektiven Sicherheits-Patches- und Schwachstellenmanagements gem. der aktuell geltenden Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V.	Bitte streichen.	Gemäß der aktuell geltenden Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V.". IT-Sicherheit entsteht nicht, wenn zu viele unterschiedliche Regelsetzer gleichzeitig berücksichtigt werden sollen. Mit der Vorgabe des Spiegelstriches "Zertifizierung MaBiS-Hub gem. ISO/IEC 27001 auf Basis BSI IT-Grundschutz" ist alles gesagt und mit Teilnehmer der SM-PKI (vom BSI) sogar verschärft.	E.ON Netze
5.2.	Operative Maßnahmen: Sicherheits-management und Prozesse	Ergreifung und Dokumentation von technischen und organisatorischen Maßnahmen (TOM) für den Informationsverbund gem. Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V. (jeweils aktuelle Fassung)	Bitte streichen.	Gemäß Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V. (jeweils aktuelle Fassung)". IT-Sicherheit entsteht nicht, wenn zu viele unterschiedliche Regelsetzer gleichzeitig berücksichtigt werden sollen. Mit der Vorgabe des Spiegelstriches "Zertifizierung MaBiS-Hub gem. ISO/IEC 27001 auf Basis BSI IT-Grundschutz" ist alles gesagt und mit Teilnehmer der SM-PKI (vom BSI) sogar verschärft.	E.ON Netze
5.2.	Operative Maßnahmen: Sicherheits-management und Prozesse	Einrichtung eines effektiven Sicherheits-Patches- und Schwachstellenmanagements gem. der aktuell geltenden Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V.	Referenzierung des Verbandes IT-Sicherheit.	Es sollte auf die Vorgabe z.B. des BSI referenziert werden. Das BSI kann dann auf Empfehlungen eines Verbandes verweisen, wie die BNetzA auf den BDEW / edi@energy, aber damit obliegt die laufende Kontrolle weiter der Behörde.	KISTERS AG
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Die verwendeten Verschlüsselungsverfahren müssen stets dem aktuellen Stand der Technik entsprechen und sowohl die Anforderungen des BSI IT-Grundschutz Kompendiums Baustein CON.1 als auch die Vorgaben der DSGVO erfüllen	Verweis auf BSI-Grundschutz Kompendiums Baustein CON.1 streichen.	Aspekte der Informationssicherheit sollten sich mit den IT-Sicherheitskatalogen der BNetzA decken und sich an den internationalen Standards der ISO 27001 oder anderen orientieren. Der BSI-Grundschutz als Grundlage festzulegen ist nicht geeignet und widerspricht teilweise bestehenden Regelwerken der BNetzA.	BDEW
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur		Einfphrung eines Bug-Bounty Programms	Die meisten großen IT-Unternehmen pflegen ein Bug-Bounty Programm – damit Schwachstellen gemeldet werden anstatt auf dem Schwarzmarkt verkauft.	decarbon1ze GmbH
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	oDie verwendeten Verschlüsselungsverfahren müssen stets dem aktuellen Stand der Technik entsprechen und sowohl die Anforderungen des BSI IT-Grundschutz-Kompendiums Baustein CON.1 als auch die Vorgaben der DSGVO erfüllen	Ändern in: Die verwendeten Verschlüsselungsverfahren müssen stets dem aktuellen Stand der Technik entsprechen	Aspekte der Informationssicherheit sollten sich mit den IT-Sicherheitskatalogen der BNetzA decken und sich an den internationalen Standards der ISO 27001 oder anderen orientieren. Der BSI-Grundschutz als Grundlage festzulegen ist nicht geeignet und widerspricht teilweise bestehenden Regelwerken der BNetzA.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	oEnde-zu-Ende-Verschlüsselung aller Datenübertragungen	Umformulieren: Datenübertragungen haben immer verschlüsselt zu erfolgen	Begründung: Dies ist eine sehr pauschale Aussage und technisch „noch“ nicht immer vollständig umzusetzen. Abfragen auf Datenbankebene sind bspw. nicht vollständige Ende zu Ende verschlüsselbar. Dies würde dem so genannten Homomorphen Verschlüsselungsansatz entsprechen, der technisch heute noch nicht performant umgesetzt werden kann.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	oVerschlüsselung ruhender Daten (aktueller Standard ist AES-256)	Umformulieren in: Verschlüsselung ruhender Daten, nach aktuellem Stand der Technik		Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Technisch-organisatorische Maßnahmen (TOMs) o Ergreifung und Dokumentation von technischen und organisatorischen Maßnahmen (TOM) für den Informationsverbund gem. Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V. (jeweils aktuelle Fassung)	Verweis auf Bundesverband IT-Sicherheit e.V. streichen	Es existiert aktuell keine Verpflichtung auf den Stand der Technik des Bundesverband IT-Sicherheit. Das BSI reklamiert ebenfalls die Definition des Stands der Technik für sich. Wenn dann sollte es nur als Empfehlung aber nicht als verpflichtend berücksichtigt werden.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	• Identity & Access Management (IAM) o Verwendung der SM-PKI als Authentifizierung der Markteilnehmer	Bitte ändern: • Identity & Access Management (IAM) o Verwendung der SM-PKI zur Authentifizierung der Markteilnehmer	Es geht um die Authentifizierung der Marktteilnehmer, deshalb "zur" anstelle "als"	E.ON Netze
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	• Monitoring o Einrichtung von Systemen zur effektiven Angriffserkennung (Intrusion Detection System, IDS) und -verhinderung (Intrusion Prevention System, IPS)	Bitte ergänzen: • Monitoring o Einrichtung von Systemen und Betrieb zur effektiven Angriffserkennung (Intrusion Detection System, IDS) und -verhinderung (Intrusion Prevention System, IPS), sowie Etablierung von Eskalationsmechanismen.	Einrichtung ist nicht ausreichend, es fehlt der Betrieb. Zudem sind Eskalationsmechanismen einzurichten.	E.ON Netze
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Verwendung der SM-PKI als Authentifizierung der Markteilnehmer	Verwendung der SM-PKI für die Authentifizierung der Markteilnehmer (maschinelle Accounts).	Korrektur der Formulierung	E.ON Netze
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Einsatz von 2FA / MFA bei besonders schützenswerten Bereichen (beispielsweise im Administrationsbereich des Betreibers)	Bitte ändern in - Einsatz von 2FA / MFA für alle natürlichen Personen (z. B. alle Mitarbeiter des Hubs und für Accounts von Marktpartnern).	Stand der Technik; weil Hacker auch diese Wege zum Einbruch nutzen.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Ende-zu-Ende-Verschlüsselung aller Datenübertragungen	Wir begrüßen dies und möchten darauf hinweisen, dass der derzeitige API-Webservice in Abstimmung mit dem BSI derzeit nur eine einfache Transportsicherung (TLS) umfasst für die bisherigen einfachen API-Anwendungsfälle.	Hinweis: Der derzeitige API-Webservice umfasst in Abstimmung mit dem BSI nur eine einfache Transportsicherung (TLS). Eine Ende-zu-Ende-Verschlüsselung, wie beim Übertragungsweg AS4, gibt es derzeit nicht beim BDEW API-Webservice. Der BDEW-Projektgruppe Technologien in der Marktkommunikation (TiM) fehlt derzeit ein Arbeitsauftrag, in dieser Richtung eine Weiterentwicklung vorzunehmen. Weiteres: Von der EU-Kommission gibt es neue API-Transportprotokolle, welche kompatibel mit der SM-PKI sind, gleichzeitig auch schon standardisiert die Inhaltsdatensicherungsebene enthalten und zusätzlich eine dritte Kontrollsicherungsebene, mit der der jeweilige Datenzugriff auch vom Protokoll automatisch geprüft werden kann, anstatt in der Fachapplikation im Nachgang zu prüfen.	E.ON Netze
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Einsatz von 2FA / MFA bei besonders schützenswerten Bereichen (beispielsweise im Administrationsbereich des Betreibers)	Es sollte angestrebt werden eine 2FA/MFA für alle Logins zu benutzen und nicht nur für den Administrationsbereich.	Entspricht den aktuellen Sicherheitsstandards	EWE NETZ GmbH & wesernetz Bremen GmbH
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Verschlüsselung	Unklar	Ende-zu-Ende Verschlüsselung/Signaturkette bleibt undefiniert. Die Konzentration sämtlicher bilanzierungsrelevanter Daten in einer zentralen Infrastruktur widerspricht dem Grundsatz der Datensparsamkeit und dem Defense-in-Depth-Ansastz der ISO 27001. Die Hubeinbindung erzeugt Redundanz und Mehrfachhaltung sensibler Daten.	Hausheld AG
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Ergreifung und Dokumentation von technischen und organisatorischen Maßnahmen (TOM) für den Informationsverbund gem. Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V. (jeweils aktuelle Fassung)	Referenzierung des Verbandes IT-Sicherheit.	Es sollte auf die Vorgabe z.B. des BSI referenziert werden. Das BSI kann dann auf Empfehlungen eines Verbandes verweisen, wie die BNetzA auf den BDEW / edi@energy, aber damit obliegt die laufende Kontrolle weiter der Behörde.	KISTERS AG
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Kryptoagile Gestaltung des Systems, insb. durch Vorbereitung des Einsatzes von Post-Quanten-sicheren Verfahren	Auch hier sollte auf das BSI verwiesen werden, z.B. TR 02102-1 und Leitfaden „Kryptografie quantensicher gestalten“	Da hier das BSI die relevante Behörde ist, halten wir einen konkreten Verweis für sinnvoll.	KISTERS AG
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Verschlüsselung: Ende-zu-Ende-Verschlüsselung aller Datenübertragungen		Bitte präzisieren ob sich die Verschlüsselung ausschließlich auf exteren Kommunikation bezieht, oder auch System-interne Kommunikation gemeint ist (z.B. zwischen Systemkomponenten oder zwischen Applikation und Datenbank)	SAP SE

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.3.	Technische Umsetzung: Schutzmaßnahmen und Infrastruktur	Verschlüsselung […] * Nutzung der SM-PKI Zertifikate für die Verschlüsselung * Verschlüsselung ruhender Daten (aktueller Stand ist AES-256)	Wir schlagen vor, dass diese Regelungen weiterhin durch die EDI@Energy Dokumente vorgegeben werden. Daher ist die Aussage aus den IT-Leitlinien zu streichen.	Diese Regelungen sollten nicht in einer Prozessbeschreibung festgelegt werden. Stattdessen sollten die Relegungen immer wieder überprüft und Änderungen über die halbjährlichen Konsultationen eingebracht werden können.	Schleupen SE
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Verschlüsselung […] * Ende-zu-Ende-Verschlüsselung aller Datenübertragungen […]	Wir schlagen vor, dass diese Regelungen weiterhin durch die EDI@Energy Dokumente vorgegeben werden. Daher ist die Aussage aus den IT-Leitlinien zu streichen.	Die Verschlüsselung auf der Payload-Ebene wird durch die RzÜ API der EDI@Energy derzeit kategorisch ausgeschlossen. Ist eine Verschlüsselung notwendig - was eine Anforderung auf der fachlichen Ebene sein sollte -, dann müssen die Vorgaben dazu in der RzÜ noch spezifiziert werden, inkl. der Nutzung des Verzeichnisdiensts zum Austausch der Metadaten, d.h. des zu nutzenden Verschlüsselungszertifikats.	Schleupen SE
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	* Technisch-organisatorische Maßnahmen (TOMs) * Ergreifung und Dokumentation von technischen und organisatorischen Maßnahmen (TOM) für den Informationsverbund gem. Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V. (jeweils aktuelle Fassung)	Punkt ist zu streichen	Der Inhalt aus dem Dokument "Stand der Technik" enthält Aussagen, die bereits in den IT-Leitlinien explizit genannt sind. Um Dopplung und Widersprüche zu vermeiden, sollten alle Anforderung ausschließlich in den IT-Leitlinien enthalten sein.	Schleupen SE
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Identity & Access Management (IAM) o Verwendung der SM-PKI als Authentifizierung der Markteilnehmer o Einsatz von 2FA / MFA bei besonders schützenswerten Bereichen (beispielsweise im Administrationsbereich des Betreibers)	Verbindliche zertifikatsbasierte 2FA/MFA für alle nutzerinitiierten Zugriffe (Admin/GUI/API) mittels mTLS (ClientAuthentication-EKU) und SM-PKI-Clientzertifikaten; Besitzmerkmal über PIV-Hardware-Token (z. B. PIV-Hardwaretoken (Yubikey, iShield Key 2 Pro oder andere/Smartcard) inkl. PIV-Attestierungsprüfung.	Konkretisierung Kap. 5.3 „Technische Umsetzung“: Die IT-Leitlinien verlangen SM-PKI-basierte Authentisierung und 2FA/MFA. Zertifikatsbasierte MFA mit PIV-Token (PIN + on-token Key, nicht exportierbar) und PIV-Attestierung (Nachweis Hardware-Ursprung, Schlüssel auf Token generiert) reduziert Phishing/Credential-Theft signifikant. mTLS mit Online-Sperrprüfung (OCSP/CRL) und kurze Laufzeiten (≤12 Monate, bevorzugt kürzer) erhöhen die Resilienz. Optional kann die Attestierungsprüfung gegen eine vertrauenswürdige Instanz (z. B. Trust-Store/Policy der SM-PKI) gespiegelt werden. Rechts-/Normrahmen: NIS-2 Art. 21 (Stand der Technik, risikoadäquate Maßnahmen); TeleTrusT „Stand der Technik“ 2025 (MFA, PKI-geschützter Datenverkehr, Kryptoagilität).	Vattenfall Euope Sales GmbH
5.3.	Technische Umsetzung: Schutz-maßnahmen und Infrastruktur	Identity & Access Management (IAM) - Verwendung der SM-PKI als Authentifizierung der Markteilnehmer - Einsatz von 2FA / MFA bei besonders schützenswerten Bereichen (beispielsweise im Administrationsbereich des Betreibers)	Dienstleister müssen sich mit einer einzigen Zugangsberechtigung am Hub authentifizieren können. Die jeweils (fachliche) Berechtigung muss in einem darunter liegenden Rechtekonzept verwaltet werden.	Dienstleister, die für Dritte die Marktkommunikation durchführen, verwalten heute hunderte AS4-Zertifikate; das führt zu nicht notwendigen Aufwänden und steigenden Kosten.	VKU e.V.
5.4.	Qualitäts-sicherung und Kontrolle	•Jährliche externe Security Audits •Risikoanalysen und Updates hinsichtlich Anlass, Turnus und Inhalt gem. Zertifizierungsbedingungen •Mindestens jährliche Durchführung externer Penetrationstests	streichen der links stehenden Punkte da über ISO 27001 abgedeckt	Die Anforderungen ergeben sich aus der entsprechend gewählten ISO 27001 Zertifizierung. Entsprechend müssen Auditprozess etabliert werden und jeweils aus den Risikoanalysen resultierende Maßnahmen auf die Wirksamkeit hin geprüft werden. Nichtkonformitäten die im Rahmen von Audits oder Pentests identifiziert werden, müssen im Rahmen der Standardprozess zu „nicht-Konformitäten“ Analysiert und abgestellt werden. Siehe Kommentar 22	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
5.4.	Qualitäts-sicherung und Kontrolle	Code Reviews sicherheitskritischer Module	Vorschlag: "Herstellerseitige Code Reviews sicherheitskritischer Module"	Hier sollte klar formuliert werden, wer die CodeReviews durchführt.	KISTERS AG

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
5.4.	Qualitäts-sicherung und Kontrolle	Sicherheitsanalysen bei jeder wesentlichen Systemänderung	Was wird unter "Sicherheitsanalyse" verstanden, wer soll diese durchführen und was wird als "wesentliche Systemänderung" verstanden?	Hier sollte klarer sein, was darunter zu verstehen ist.	KISTERS AG
6.1.	Modulare Strukturierung des Quellcodes			Wie an anderer Stelle der Anforderungsliste auch sollten hier besser die Ziele im Vordergrund stehen als konkrete technische Vorgaben. Also: Warum die Vorgaben, anstatt genau welche. - Z.B. könnte ein Ziel sein, dass möglichst viele Entwickler:innen sich im Code zurechtfinden, auch ohne Spezialwissen in der Energiewirtschaft. - Sollten Deutschkenntnisse Voraussetzung sein für Entwickler:innen? - Was ist die erwartete Lebensdauer das Software-Systems bis zum ersten großen "Rewrite"? 5 Jahre? 10 Jahre? 20 Jahre? - Wo auf der "Technology Curve" soll die Entwicklung stattfinden – alte, bekannte und stabile Technologie mit wenig Risiko aber ggf. ineffizient und mit abnehmender Beliebtheit bei Entwickler:innen, oder ganz vorne dran an der technischen Entwicklung, mit ggf. mehr Risiko aber erwartbar längere Lebensdauer?	decarbon1ze GmbH
6.1.	Modulare Strukturierung des Quellcodes	Hohe Kommentierung des Codes	sinnvolle Kommentierung von Entwurfsentscheidungen statt viel Kommentierung	Kommentare im Code sind kein Qualitätsmerkmal per se. Die schlimmsten Kommentare sind veraltet und nicht mehr gültig. Wie bei Code gilt auch bei Kommentaren: Jede Zeile weniger reduziert den Wartungsaufwand und die Möglichkeit von Fehlern. Der beste Code ist so expressiv, dass er keine Kommentare braucht.	decarbon1ze GmbH
6.1.	Modulare Strukturierung des Quellcodes	Modulare Strukturierung des Quellcodes • Klare Trennung von Fachlogik, Infrastruktur, Schnittstellen und technischen Hilfsklassen • Einhaltung von Modularitätsprinzipien: kleine, wiederverwendbare, klar abgegrenzte Komponenten • Verwendung von standardisierten Frameworks und Architekturmustern (z.B. MVC, Microservices) • Hohe Lesbarkeit und Kommentierung des Codes • Rückverfolgbarkeit der Fachlogik durch sprechende Methodennamen, strukturierte Module und Dokumentationen		Prinzipell ist jede reale Implementierung unter diesen sehr allgemein formulierten Kriterien angreifbar bzw. kann individuellen Ansprüchen nicht genügen. Da es keine allgemeingültigen Normen für diese Punkte gibt, bitte diese Punkte streichen.	SAP SE
6.1.	Modulare Strukturierung des Quellcodes	Gesamtes Kapitel 6.1	Kapitel ist zu streichen	Die modulate Strukturierung des Quellcodes ist anzustreben, ist allerdings ein Implementierungsdetail welches nur im Fall einer Open-Source-Lösung nur Relevanz für dieses Papier hat, siehe Beitrag zu Kapitel 1.1.	Schleupen SE

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
6.1.	Modulare Strukturierung des Quellcodes		Anpassung notwendig.	1. Wie der Quellcode strukturiert ist, hätte nur bei Open-Source-Lösungen Relevanz. Es ist darauf zu achten, dass Anforderungen wie diese dem effizienten Erstellen und Warten der Lösung nicht entgegenstehen. Dies könnte z. B. dann der Fall sein, wenn Software-Generatoren zum Einsatz kommen. 2. Auch Vorgaben, wie die Implementierung als "Microservice" werden von uns als kritisch eingestuft. Es existieren alternative Architekturmuster, die einige Nachteile (Modulith), von Microservice-Architekturen beseitigen möchten. Generell befürworten wir die Strukturierung von Quellcode und die Verwendung von Microservices, sind aber der Ansicht, dass in diesem Dokument die zu erreichenden Ziele (Anforderungen) beschrieben werden sollten, ohne die Möglichkeiten der technischen Realisierung einzuschränken (eher das "Was" beschreiben als das "Wie").	Schleupen SE
6.1.	Modulare Strukturierung des Quellcodes	Gesamtes Kapitel 6.1	Anpassung notwendig.	Das Dokument sollte aus unserer Sicht die zu erreichenden Ziele beschreiben (Anforderungen), ohne die Möglichkeiten der technischen Realisierung einzuschränken (eher das "Was" beschreiben als das "Wie").	Schleupen SE
6.2.	Dokumentation sanforderungen	• Lebende Systemdokumentation in einem zentralen, versionierten Repository (z.B. GitLab, Confluence) o Zielgruppenorientierte Dokumentation: ▪ Anwenderdokumentation (Nutzer, Marktpartner) ▪ Betriebsdokumentation (Systemadministration, IT-Operations) ▪ Entwicklerdokumentation (Modulstruktur, Codebeispiele, API) • Automatisierte Dokumentation technischer Schnittstellen mittels OpenAPI-Spezifikation o Bereitstellung für alle Datenzulieferer und Marktpartner o Versionierung und Änderungsverfolgung	• Lebende Systemdokumentation in einem zentralen, versionierten Repository (z.B. GitLab, Confluence) o Zielgruppenorientierte Dokumentation: ▪ Anwenderdokumentation (Nutzer, Marktpartner) ▪ Betriebsdokumentation (Systemadministration, IT-Operations) ▪ Entwicklerdokumentation (Modulstruktur, Codebeispiele, API) ▪ Marktintegrationsdokumentation (Technische Integration der EDI@Energy-Schnittstellen)	Da Marktpartner, die auch Datenzulieferer sind, ausschließlich über EDI@Energy dokumentierte Schnittstellen angebunden werden, genügt die Dokumentation der technischen Integration dieser.	BDEW
6.2.	Dokumentation sanforderungen	•Lebende Systemdokumentation in einem zentralen, versionierten Repository (z.B. GitLab, Confluence)	Lebende Systemdokumentation in einem zentralen, versionierten Repository (z.B. GitLab).	Confluence streichen, da kein Repository: Confluence ist ein Dokumentationssystem, während ein Repository ein Versionsverwaltungssystem für Quellcode oder Dateien darstellt.	BDEW
6.2.	Dokumentation sanforderungen	Entwicklerdokumentation	Es fehlt die Forderng nach einer guten Architekturdokumentation sowie Dokumentation der wichtigsten Entwurfsentscheidungen und Design-Prinzipien	Es ist viel wichtiger, zu dokumentieren warum Entscheidungen getroffen wurden, als wie der Code letztendlich aussieht. Code ist Text, der für sich selbst steht. Die Struktur von Modulen zu beschreiben ist überflüssig, denn jedes gute Werkzeug kann diese Übersicht automatisch erzeugen. Aber die Gründe für die Wahl der Struktur, für die Wahl eines Frameworks, eines Architekturmusters, etc. ist essenziell für die spätere Wartung und Weiterentwicklung. Daher sollten vor allem diese Entscheidungen dokumenitert werden – z.B. in der Form von sog. Architecture Decision Records (ADR).	decarbon1ze GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
6.2.	Dokumentation sanforderungen	Lebende Systemdokumentation in einem zentralen, versionierten Repository (z.B. GitLab, Confluence)	Formulierung anpassen: Lebende Systemdokumentation in einem zentralen, versionierten Repository (z.B. GitLab)	Confluence streichen, da kein Repository	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
6.2.	Dokumentation sanforderungen	Lebende Systemdokumentation in einem zentralen, versionierten Repository (z.B. GitLab, Confluence)	Sehr begrüßenswert, wir empfehlen grundsätzlich die Verwendung einer souveränen, EU-basierten Plattform - bspw. https://codeberg.org/		Mako365 GmbH
6.2.	Dokumentation sanforderungen	Bereitstellung für alle Datenzulieferer und Marktpartner	Punkt unter Automatisierte Dokumentation technischer Schnittstellen mittels OpenAPI-Spezifikation	Die Bereitstellung nur für alle Datenzulieferer und Marktpartner wiederspricht der Open Source Forderung aus Kap 1.1, bitte ensprechend klarstellen.	SAP SE
6.3.	Testkonzept	Erster Aufzählungspunkt: Definition und Pflege eines umfassenden Testkonzepts für: o Unit-Tests(Modul-/Funktionslogik) o Integrationstests(Systemverhalten, Schnittstellen) o End-to-End-Tests(Nutzerprozesse) o Last- und Performancetests(bei Releases und Simulationen)	Ergänzung der Aufzählung um Regressions-Tests: Definition und Pflege eines umfassenden Testkonzepts für: o Unit-Tests(Modul-/Funktionslogik) o Regressions-Tests(Modul-/Funktionslogik) o Integrationstests(Systemverhalten, Schnittstellen) o End-to-End-Tests(Nutzerprozesse) o Last- und Performancetests(bei Releases und Simulationen)	Die Durchführung von Regressionstests ist entsprechend den Umsetzungen regelmäßig in einer Testphase vorzusehen und diese sind immer als letzte „Testinstanz“ vor einer Freigabe einer Umsetzung auf die Testebene für Marktpartner und Produktivebene erfolgreich durchzuführen.	BDEW
6.3.	Testkonzept	•Definition und Pflege eines umfassenden Testkonzepts für: oUnit-Tests (Modul-/Funktionslogik) oIntegrationstests (Systemverhalten, Schnittstellen) oEnd-to-End-Tests (Nutzerprozesse) oLast- und Performancetests (bei Releases und Simulationen)	Formulierung Anpassen Definition und Pflege eines Testkonzepts anhand anerkannter Best Practices mit mindestens folgenden Testarten: oUnit-Tests (Modul-/Funktionslogik) oIntegrationstests (Systemverhalten, Schnittstellen) oEnd-to-End-Tests (Nutzerprozesse) oLast- und Performancetests (bei Releases und Simulationen)	Konkretisierung der Anforderung	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
6.3.	Testkonzept	• Definition und Pflege eines umfassenden Testkonzepts für: o Unit-Tests (Modul-/Funktionslogik) o Integrationstests (Systemverhalten,Schnittstellen) o End-to-End-Tests (Nutzerprozesse) o Last- und Performancetests(bei Releases und Simulationen) • Einsatz von automatisiertenTestroutinen(CI/CD) • Testabdeckung in % als Kennzahl für das Reporting	Bitte ergänzen: • Testmanagement folgt den ITIL-Vorgaben	Ein Testmanagement nach ITIL-Vorgaben stellt sicher, dass Tests strukturiert, nachvollziehbar und qualitätsgesichert durchgeführt werden. Dadurch werden Risiken bei Änderungen minimiert, die Systemstabiliät erhöht und die Einhaltung definierter Service- und Qualitätsstandards gewährleistet. Zudem wird eine einheitliche Vorgehensweise über alle Entwicklungs- und Betriebsphasen hinweg sichergestellt.	E.ON Netze
6.3.	Testkonzept	Erster Aufzählungspunkt: Definition und Pflege eines umfassenden Testkonzepts für: o Unit-Tests(Modul-/Funktionslogik) o Integrationstests(Systemverhalten, Schnittstellen) o End-to-End-Tests(Nutzerprozesse) o Last- und Performancetests(bei Releases und Simulationen)	Ergänzung der Aufzählung um Regressions-Tests: Definition und Pflege eines umfassenden Testkonzepts für: o Unit-Tests(Modul-/Funktionslogik) o Regressions-Tests(Modul-/Funktionslogik) o Integrationstests(Systemverhalten, Schnittstellen) o End-to-End-Tests(Nutzerprozesse) o Last- und Performancetests(bei Releases und Simulationen)	Die Durchführung von Regressionstests ist entsprechend den Umsetzungen regelmäßig in einer Testphase vorzusehen und diese sind immer als letzte „Testinstanz“ vor einer Freigabe einer Umsetzung auf die Testebene für Marktpartner und Produktivebene erfolgreich durchzuführen.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
6.3.	Testkonzept	Testabdeckung in % als Kennzahl für das Reporting		Testabdeckung sind typischerweise interne Kennzahlen die unter anderem während des Builds anfallen und relevant sind für Softwarefreigaben. Imwieweit sollen diese internen Information in welches Reporting einfließen? Bitte spezifizieren, von was für ein Reporiting hier gesprochen wird und wer der Addressatenkreis dieses Reportings ist.	SAP SE
6.3.	Testkonzept	o End-to-End-Tests (Nutzerprozesse)	Wir gehen davon aus, dass es sowohl bei Einführung als auch bei Anpassungen möglich ist, Testfälle (das beinhaltet eine Anfrage mit entsprechender Antwort) mit dem MaBiS-Hub durchführen zu können.	Um den hohen Automatisierungsgrad und die vorhandene Performance im Energiemarkt aufrecht zu erhalten und stets verbessern zu können ist das Testen mit Marktpartnern, sowie zukünftig auch mit dem MaBiS-Hub ein essentieller Baustein für den Erfolg. Daher ist es äußerst wichtig, Tests mit dem MaBiS-Hub jederzeit im aktuellen Format, sowiein einem angemessenen Zeitraum vor einem Format- oder Releasewechsel durchführen zu können.	Vattenfall Euope Sales GmbH
7.	Betrieb und Support	zweiter Aufzählungspunkt: Kein Clearing von fehlerhaften Messwerten, keine Klärung prozessualer Abwicklungsfragen	Die Erfahrungen aus der Praxis zeigen, das auch perspektivisch ein bilaterales/multilaterales Clearing zwischen allen Marktpartnern - insbesondere auch dem BA und MV möglich sein muss.	Die aktuellen Beispiele in der Geschäftsprozessabwicklung zwischen allen Marktrollen (insbesondere zwischen NB und Messstellenbetreibern) zeigen deutlich auf, dass bilaterales Clearing unumgänglich zwischen allen Marktrollen als letzte Lösungsmöglichkeit erhalten bleiben muss.	Bielefelder Netz GmbH
7.	Betrieb und Support	Kein Clearing von fehlerhaften Messwerten, keine Klärung prozessualer Abwicklungsfragen	Welches Vorgehen ist für das Clearing von fehlerhaften Messwerten bzw. Bilanzierungsergebnissen geplant?	Schon heute ist eine Fehlersuche unter Umständen schwierig, weil die Ursache für einen Fehler an einer ganz anderen Stelle zu suchen ist, als das die Fehlerstelle zunächst vermuten lässt. Desto mehr Marktrollen an dem Endergebnis beteiligt sind und wenn zusätzlich Anonymisierung erfolgt, bedarf es konkreter Clearing-Prozesse und ggf. Ausnahmen von Datenschutz, um im Ausnahmefall einen Fehler zu korrigieren. Wäre es unser diesem Gesichtspunkt nicht einfacher und praktikabler, wenn ein Marktpartner im Clearing-Fall, bei dem er ein berechtigtes Interesse an den Daten hat, die Daten bei MV oder BA z.B. für einen Zählpunkt und ein Intervall per Web-API anfordern kann? Er bekäme die Eingabe- und Ausgabewerte bzw. das „Daten-Paket“ mit zusammenhängenden Daten. Mit diesen Daten kann er in seiner lokalen Instanz des MaBiS-Hubs debuggen oder mit Hilfe der Daten rausfinden, dass der Fehler ein Stammdatenfehler ist und beim Marktpartner XY liegt. Er kann daraufhin das Clearing mit diesem Marktpartner anstoßen und braucht nicht es (ggf. bilateral) mit verschieden Stellen Kontakt aufnehmen.	cortility GmbH
7.	Betrieb und Support	Lösungszeiten: ... Normal: <3 Tage Niedrig: <5 Tage	Für unkritische Tickets sollten die Lösungszeiten deutlich länger sein um keine Hotfixes dafür einspielen zu müssen Anpassung der Zeit wie folgt: Normal < 60 Tage Niedrig < 180 Tage	Lösungen können dann ggf. in den normalen Releasezyklus mit eingepflegt werden . Wir gehen bei Incidents mit der Kategorie Normal und Niedrig davon aus, dass der MaBiS-Hub ohne relevante Einschränkung benutzt werden kann.	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
7.	Betrieb und Support	•Bereitstellung eines technischen 2nd Level Supports und eines 3rd Level Supports für Energiemarktteilnehmer	Ergänzen: Es soll ein 1. Level Support ergänzt werden Ein First-Level Support ist beim jeweiligen Marktpartnern zu etablieren. Nur vor-qualifizierte Anfragen werden an den 2nd-Level-Support weitergeleitet	Ansonsten landen alle Anforderungen direkt beim 2nd. Level. Einfache Anfragen sollten nicht vom 2nd. Level bearbeitet werden müssen. Ein fehlender 1. Level führt tendenziell zu Überlastung und längeren Durchlaufzeiten von Tickets	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
7.	Betrieb und Support	• Bereitstellung eines technischen 2nd Level Supports und eines 3rd Level Supports für Energiemarktteilnehmer.	Bitte ergänzen: • Die Supportstruktur erfüllt die Anforderungen aus dem ITIL Framework	Die Supportstruktur nach dem ITIL-Framework stellt sicher, dass Störungen, Serviceanfragen und Änderungen effizient, transparent und nach definierten Prozessen bearbeitet werden. Dadurch werden Reaktionszeiten verkürzt, Servicequalität und Kundenzufriedenheit erhöht sowie eine kontinuierliche Verbesserung des Betriebs gewährleistet.	E.ON Netze
7.	Betrieb und Support	neuer Aufzählungspunkt	Bitte neuen Aufzählungspunkt "Echtzeit-Validierung" ergänzen: Der Betreiber hat sicherzustellen, dass alle in den MaBiS-Hub eingehenden Daten einer Echtzeit-Validierung gemäß EDI@Energy OpenAPI-Vorgaben unterzogen werden. Die Validierung muss automatisiert, regelbasiert und unmittelbar beim Eingang der Daten erfolgen. Hierfür sind insbesondere folgende Prüfungen durchzuführen: o Struktur- und Formatprüfungen gemäß den definierten Schnittstellen- und Datenmodellspezifikationen, o fachliche Plausibilitätsprüfungen (z. B. Wertebereiche, Zeitintervalle, Vollständigkeit) o Konsistenzprüfungen Fehlerhafte oder unvollständige Datensätze sind zurückzuweisen bzw. mit qualifizierten Fehlermeldungen an den liefernden Marktpartner zu adressieren. Der Betreiber hat sicherzustellen, dass sämtliche Validierungsvorgänge protokolliert, revisionssicher dokumentiert und im Rahmen des Monitorings auswertbar sind. Die Verfahren und Regelwerke der Echtzeit-Validierung sind regelmäßig zu überprüfen und an geänderte Markt- oder Prozessanforderungen anzupassen.	In modernen Hub-Architekturen werden Daten (z. B. Messwerte, Zeitreihen, Stammdaten) sofort beim Eingang oder bei der Erzeugung automatisch auf Korrektheit, Vollständigkeit und Plausibilität geprüft, bevor sie weiterverarbeitet oder verteilt werden (Echtzeit-Validierung)	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
7.	Betrieb und Support	zweiter Aufzählungspunkt: • Kein Clearing von fehlerhaften Messwerten, keine Klärung prozessualer Abwicklungsfragen	Bitte ergänzen: • Handelt es sich um einen vom MV erzeugten Verbrauch, muss das Clearing durch den MV vorgenommen werden.	Bei fehlerhaften Messwerten oder Berechnungsformueln, die durch den verantwortlichen MSB bzw. NB ermittelt/ bereitgestellt wurden, ist das Clearing durch die verantwortlichen Rollen wahrzunehmen. Wird der Verbrauch in Frage gestellt, kann der MSB oder NB ausschließlich prüfen, ob ihre überlieferten Werte bzw. Formeln korrekt sind. Es ist nicht ihre Aufgabe zu prüfen, ob beim MV die korrekten Werte bzw. Formeln zur Anwendung gekommen sind. Dies hat der MV selbst zu überprüfen und zu verantworten. Ein reines Routing des Clearings an MSB und NB führen in diesem Fall nicht immer zur Klärung des Sachverhalts (entsprechend müsste der UseCase "Reklamation von Werten" angepasst werden). Zudem möchten wir darauf hinweisen, dass wir auch Fälle kennen, bei denen z. B. bei einem MSB-Wechsel zwei unterschiedliche Werte zum Wechseltermin ermittelt wurden und beide MSB auf ihren Wert bestehen. Auch hier bedarf es beim MV der Entscheidung, welcher Wert angewendet wird.	E.ON Netze
7.	Betrieb und Support	zweiter Aufzählungspunkt: Kein Clearing von fehlerhaften Messwerten, keine Klärung prozessualer Abwicklungsfragen	Ergänzung des Satzes: Kein bilaterales Clearing mit dem MV bzw. BA von fehlerhaften Stammdaten, Abrechnungsdaten oder Bewegungsdaten (unabhängig davon, ob die Daten in der Hoheit eines Marktpartners, dem MV (z.B. OBIS-Daten der Marktlokation) oder BA liegen), keine Klärung prozessualer Abwicklungsfragen	Klarstellung, passend zu den Aussagen zum Clearing in den zur Konsultation gestellten Dokumenten GPKE, WiM Strom, MaBiS sowie dem Dokument "Erläuterung der zentralen Prozessvorgaben". Ein bilaterales Clearing findet nicht unter Einbindung des MaBiS-Hub bzw. deren Betreiber statt. Dies Begrüßen wir auch deutlich. Systemfehler hingegen müssen über einen entsprechenden Meldeweg an den Betreiber des MaBiS-Hub meldbar sein.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
7.	Betrieb und Support	--	Ein Informationsmanagement zu Fehlerhandling und Releases an die Marktpartner gerichtet, mit ausführlicher Beschreibung des Sachverhalts, ggf. Workarrounds/weiterem Vorgehen und widerholenden Update-Informationen, ist unserer Ansicht nach einzuführen. Hinweise: * Die Aussage in Kapitel 5.2. "Etablierung Incident-Response-Prozesse und Notfallpläne inkl. Erstellung interner und externer Informationsketten" schließt die oben beschriebenen Punkte unserer Ansicht nach nicht ein, da sich diese Aussage lt. Kapitelvorgaben ausschließlich auf sicherheitsrelevante Themen bezieht. * Die Aussage in Kapitel 9.3. "Aufbau und Zurverfügungstellung einer Status Page, über die Marktteilnehmer Informationen zur historischen (90 Tage) und aktuellen technischen Verfügbarkeit abrufen können" schließt die oben beschriebenen Punkte unserer Ansicht nach nicht ein, da sich diese Aussage lt. Kapitelvorgaben ausschließlich auf technische Verfügbarkeiten (also geplante und ungeplante Ausfallzeiten) bezieht.	Ein frühzeitiges, eindeutiges Informationsmanagement ist für die Marktpartner elementar wichtig, um ihre eigenen Prozesse entsprechend ausrichten zu können. Wir schlagen vor, dass Informationen an Marktpartner bzgl. technischer Verfügbarkeiten, Fehlerhandling, Releases etc. an E-Mail-Adresse kommuniziert werden, die über die Kontaktdaten der Marktkommunikation (PARTIN) für das jeweilige Thema angegebene werden. Es wird mit dem automatischen E-Mail-Versand vermieden, * dass jeden Tag Mitarbeiter die Seiten proaktiv anschauen/abrufen müssen, um festzustellen, dass sich x Tage nichts verändert hat. * dass die Marktpartner Update-Routinen auf die Informationsseiten des Hub-Betreibers einrichten müssen, um sich upzudaten. Hierbei ist anzumerken, dass solche Routinen oft nicht einwandfreie Ergebnisse liefern. Bei einer automatischen E-Mail an die Marktpartner erhält der Marktpartner hingegen nur dann eine Info, wenn sich "etwas getan hat". In der Regel gibt der Marktpartner zudem ein Sammelpostfach in den Kontaktdaten an. Dies hat den weiteren Vorteil, dass die Information auch bei Urlaub/Krankheit einzelner Personen beim Marktpartner Berücksichtigung findet. Hinweis: Wir gehen davon aus, dass die Aussage im Governance- und Transparenz-Dokument " Verpflichtung des MaBiS-Hub bei Wartungsarbeiten, Updates, Störungen oder anderen Abweichungen vom Regelbetrieb die Marktteilnehmer und die Beschlusskammer zu informieren" auf ein entsprechendes Informationsmanagement abzielt.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
7.	Betrieb und Support	Servicezeiten: 24/7	Wird hier der Bedarf für 24/7 Support auf allen Leveln gesehen? Was ist damit dann gemeint, die Verfügbakreit des Ticketsystem oder die Erreichbarkeit eines Mitarbeiters? Was umfasst die "erste Rückmeldung" mehr, als eine Bestätigung des Eingangs eines Tickets? Gelten die Reaktionszeiten und Lösungszeiten auch 24/7? Generell können Lösungszeiten nicht grundsätzlich fix zugesagt werden.	Kosteneffizienz kann durch Orientierung der Servicezeiten an den durchgeführten Geschäftsprozessen erzielt werden.	KISTERS AG
7.	Betrieb und Support	* Bereitstellung eines technischen 2nd Level Supports und eines 3rd Lever Supports für Energiemarktteilnehmer […]	Es fehlen Aussagen zum 1st Level Support.	Aus unserer Sicht fehlen Aussagen zum 1st Level Support.	Schleupen SE

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
7.	Betrieb und Support	Erreichbarkeit o Servicezeiten: 24/7 o Kanäle: Ticketsystem	Wie folgt anpassen: Erreichbarkeit o Servicezeiten: 24/7 o Kanäle: E-Mail und Telefon Auch aus Seiten der MaBiS-Hub-Nutzer sind Ansprechpartner für den MaBiS-Hub zu etablieren.	Das manuelle erstellen eines Tickets beim MaBiS-Hub-Betreiber kann i.d.R. nur während der üblichen Geschäftszeiten erfolgen. Eine Störungsmeldung sollte aber abgesetzt werden, wenn die Störung auftritt und nicht, wenn die Störung z.B. an einem Sa. auftritt, erst am Montag. Nur so kann der MaBiS-Hub-Betreiber schnellstmöglich nach eintreten einer Störung reagieren und diese schnellstmöglich beheben. Dies ist nur automatisiert möglich. Da wir davon ausgehen, dass der MaBiS-Hub weitestgehend stabil laufen wird und es nur wenige meldungswürdige Störungen geben wird, würde eine API für eine automatisierte Ticketerstellung und Bearbeiitung (die auf einer anderen Resource laufen müsste als der MaBiS-Hub) nicht effizient betrieben werden können und die Umsetzungsaufwände für alle Beteiligten unnötig erhöhen. Daher sollte die Meldung von Störungen und deren Beantwortung per E-Mail erfolgen. Für Eskalationszwecke sollte zusätzich ein Telefonkontakt verfügbar sein. DIe Daten sollten per PARTIN übertragen werden oder im MaBiS-Hub, für alle Nutzer abrufbar hinterlegt sein, sowie zusätzlich als Information auf der Status Page (Kap. 9.3). Auch auf Seite der MaBiS-Hub-Nutzer sollten Ansprechpartner für die Hub-Kommunikation eingeführt werden, damit sowohl der Hub-Betreiber, wie auch die Nutzer untereinander die Möglichkeit haben, MaBiS-Hub Themen direkt zu klären.	Vattenfall Euope Sales GmbH
8.	Revisions-sicherheit und Auditierung	• Versionierung aller Stammdaten	Bitte ändern: • Versionierung aller Stammdaten, Schnittstellen, Schnittstellenbeschreibungen	Die Versionierung von Schnittstellen und deren Beschreibungen stellt sicher, dass Änderungen nachvollziehbar dokumentiert und kompatibel umgesetzt werden können. Sie ermöglicht den parallelen Betrieb verschiedener Schnittstellenstände, reduziert Integrationsrisiken und gewährleistet Stabilität sowie Transparenz im Datenaustausch zwischen den Marktpartnern.	E.ON Netze
8.	Revisions-sicherheit und Auditierung	8.1. Revisionssicherheit […] * Zeitstempelung aller Aktionen im Format UTC mit Zeitzone bzw. Sommer- und Winterzeit […]	8.1. Revisionssicherheit […] * Zeitstempelung aller Aktionen im Format UTC […]	Das Format UTC mit Zeitzone gibt es nicht.	Schleupen SE
8.1.	Revisions-sicherheit	• Zeitstempelung aller Aktionen im Format UTC mit Zeitzone bzw. Sommer- und Winterzeit	Zeitstempelung aller Aktionen im Format UTC (gem. ISO-8601).	Informationen zur Zeitzone sind in ISO-Standard enthalten.	BDEW
8.1.	Revisions-sicherheit	•Zeitstempelung aller Aktionen im Format UTC mit Zeitzone bzw. Sommer- und Winterzeit	Anpassung der Formulierung: Zeitstempelung aller Aktionen im Format UTC (gem. ISO8601)	Informationen zu Zeitzone sind in ISO Standard enthalten	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
8.1.	Revisions-sicherheit	• Dokumentation von: o Änderungen an Stamm- und Bewegungsdaten, Berechnungsformeln, Konfigurationen	Bitte ergänzen: • Dokumentation von: o Änderungen an Stamm- und Bewegungsdaten, Berechnungsformeln, Konfigurationen, versionierten Trainingsdaten für KI-Modelle sowie deren Epochen	Die verwendeten KI Modelle in der jeweiligen Revision sollten ebenfalls der Aufbewahrung zugeführt werden. Ebenfalls sind die Trainingsdaten revisionssicher zu speichern. Prozessabläufe und Entscheidungen können auf diesen Daten basieren. Die Trainingsepochen sind zur Nachvollziehbarkeit, warum welches Datum geändert wurde, aufzubewahren.	E.ON Netze
8.1.	Revisions-sicherheit	[…] * Aufbewahrungsfristen entsprechend der gesetzlichen Vorgaben [...]	Konkretisierung ist notwendig.	Welche Aufbewahrungsfristen sind für welche Daten einzuhalten?	Schleupen SE
8.2.	Auditierung	zu "Auditfähige Protokollierung", zweiter bis vierter Aufzählungspunkt: o Änderungen an Berechnungslogiken, Konfigurationen, Stammdaten / Nachweis über die Regulatorik-konforme Abrechnungslogik o Bearbeitung von Werten (z.B. Korrekturen, Reklamationen, Ersatzwertbildung) o Prozessdurchläufe (z.B. Aggregationen, Abrechnungsdurchläufe)	Wir möchten in diesem Zuge auf folgendes Hinweisen: Sachverhalte, die keiner regelmäßigen oder keiner Veränderung unterliegen und insbesondere eine inhaltliche Überprüfung durch unabhängige Wirtschaftsprüfer oder andere geeignete Institutionen erfahren, sind unserer Ansicht nach nicht über Verwaltungsoberflächen abzubilden (zu customizen/konfigurieren). Solche Sachverhalte sind im BA z.B. die Aggregationsvorgaben von Energiemengen oder im MV z.B. die Anwendung von Berechnungsformeln, Ersatzwertbildungs- und Plausibilisierungsverfahren.	Dieses Vorgehen führt zu einer erhöhten Sicherung des abgenommenen Zustands bis zur nächsten Überprüfung.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
9.1.	Technisches Monitoring	Bitte Aufzählungspunkt ergänzen: • Gemeinsam mit der Kontrollinstanz (Aufsichtsrat) werden einmal jährlich KPI's definiert bzw. reviewt. Die KPI's werden durch den Servicemanager der Organisation laufend überwacht. Überschreitungen der darin enthaltenen Watermarks (High-/Low-Watermark) gehen per Dringlichkeitsmeldung an den AR.	Fehlender Aufzählungspunkt, was mit dem Monitoring passieren soll. Hier fehlt ein Verfahren bzw. eine Organisationsstruktur	Es fehlt die technische Beschreibung, was mit dem Monitoring geschieht.	E.ON Netze
9.1.	Technisches Monitoring	Technisches Monitoring		Wer ist der berechtigte Personenkreis für das Technische Monitoring? Ist hier der Betreiber der Software gemeint?	SAP SE
9.1.	Technisches Monitoring	[…] * Revisionssicher, speicherbar und auswertbar	Konkretisierung ist notwendig.	Ist im Hinblick auf die zu erwartenden Datenmengen und die damit verbundenden Kosten, tatsächlich das revisionssichere Speichern von technischen Monitoringdaten wirklich erforderlich? Ggf. Konkretisierung welche Daten revisionssicher zu speichern und auswertbar sein sollen. Das Dokument sollte aus unserer Sicht die zu erreichenden Ziele beschreiben (Anforderungen), ohne die Möglichkeiten der technischen Realisierung einzuschränken (eher das "Was" beschreiben als das "Wie").	Schleupen SE
9.2.	Reporting an die Bundes-netzagentur		Bitte folgende Reports ergänzen: Monatlich: Anzahl Angriffsversuche geclustered nach Vorfall (DDos, BruteForce, …) und Geolocation Monatlich: Marktpartnerfails (z. B. Bruteforce MaloIdent, Nichterreichbarkeit von Systemen, Nichteinhaltung der EDI@Energy Datenformate, Nichtlieferung von angeforderden Daten)	Folgende Reports fehlen: Monatlich: Anzahl Angriffsversuche geclustered nach Vorfall (DDos, BruteForce, …) und Geolocation Monatlich: Marktpartnerfails (z. B. Bruteforce MaloIdent, Nichterreichbarkeit von Systemen, Nichteinhaltung der EDI@Energy Datenformate, Nichtlieferung von angeforderden Daten)	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
9.3.	Technischer Statusbericht für Markt-teilnehmer	Aufbau und Zurverfügungstellung einer Status Page, über die Marktteilnehmer Informationen zur historischen (90 Tage) und aktuellen technischen Verfügbarkeit abrufen können	Aufbau und Zurverfügungstellung einer Status Page, die ebenfalls über API ansteuerbar ist. Die Marktteilnehmer erhalten Informationen zur historischen (90 Tage), aktuellen und zukünftigen technischen Verfügbarkeit. Dies darf keine Auswirkungen auf Prozesse und Fristen (operativer Marktbetrieb) haben.	Verdeutlichung, dass diese Page ausschließlich zur Information der Marktteilnehmer dient. Über diese können keine Fristvorgaben oder andere Funktionen umgangen werden. Zusätzlich sollen diese zur Erhöhung der Automation auch über API verfügbar sein und deshalb auch geplante Nichtverfügbarkeiten anzeigen.	BDEW
9.3.	Technischer Statusbericht für Markt-teilnehmer	Aufbau und Zurverfügungstellung einer Status Page, über die Marktteilnehmer Informationen zur historischen (90 Tage) und aktuellen technischen Verfügbarkeit abrufen können	Aufbau und Zurverfügungstellung einer Status Page, die die Verfügbarkeiten den Marktpartnern zusätzlich über API aktiv übermittelt (aktives Push-Modell). Die Marktteilnehmer. Die Marktteilnehmer erhalten Informationen zur historischen (90 Tage), aktuellen und zukünftigen technischen Verfügbarkeit. Dies darf keine Auswirkungen auf Prozesse und Fristen (operativer Marktbetrieb) haben.	Verdeutlichung, dass diese Page ausschließlich zur Information der Marktteilnehmer dient. Über diese können keine Fristvorgaben oder andere Funktionen umgangen werden. Zusätzlich sollen diese zur Erhöhung der Automation auch über API verfügbar sein und deshalb auch geplante Nichtverfügbarkeiten anzeigen.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
9.3.	Technischer Statusbericht für Markt-teilnehmer	Aufbau und Zurverfügungstellung einer Status Page, über die Marktteilnehmer Informationen zur historischen (90 Tage) und aktuellen technischen Verfügbarkeit abrufen können	Die Status Page muss zwingend auf einer anderen Resource als der MaBiS-Hub laufen und sollte sowohl auf einer Oberfläche lesbar dargestellt und maschinell auslesbar sein.	Die Informationen müssen gerade im Störungsfall des MaBiS-Hub verfügbar sein. Um unnötige Störungsmeldungen an den MaBiS-Hub-Betreiber zu vermeiden müssen die Informationen maschinell auslesbar sein, um einen automatischen Abgleich der erwarteten und der tatsächlichen Verfügbarkeit zu ermöglichen.	Vattenfall Euope Sales GmbH
10.	Release- und Change Management	Release- und Change Management	Release- und Change Management des Hubs	Hierdurch soll sichergestellt werden, dass nicht das Release - und Change Management der API etc. gemeint ist	BDEW
10.1.	Release Management	zu "Rollout-Strategie", dritter Aufzählungspunkt: Bereitstellung von: ▪ Release Notes ▪ Migration Guides ▪ Testszenarien	Ergänzung der Aufzählung um Schulungskonzept: Bereitstellung von: ▪ Release Notes ▪ Migration Guides ▪ Testszenarien ▪ Schulungskonzept	Uns fehlt die Berücksichtigung von Schulungen (Schulungsunterlagen/Informationsunterlagen) für Mitarbeiter des Betreibers sowie ggf. von Marktpartner zu bestimmten Sachverhalten mit dem Umgang zum MaBiS-Hub. Schulungsaufwände dürfen in einer Releaseplanung nicht unterschätzt werden (insbesondere auch die Aufwände für die Erstellung solcher Unterlagen). Marktpartner müssen die Möglichkeit haben, sich vor Produktivsetzungen mit Neuerungen/Anpassungen vertraut machen zu können, sofern es sich um Sachverhalte handelt, die nicht bereits über die festgeleten Dokumente oder BDEW-Dokumente abgedeckt sind.	BDEW
10.1.	Release Management	oAlle Releases müssen rücksetzbar sein (Rollback oder Hotfix-Fallback). Daten müssen entsprechend aus letztem Snapshot / Sicherheitspunkt wiederhergestellt werden	Alle Releases müssen rücksetzbar sein (Rollback oder Hotfix-Fallback). Daten müssen entsprechend aus letztem Snapshot / Sicherheitspunkt wiederhergestellt werden können	Wort "können" am Ende ergänzt. Nicht jedes Rücksetzen bedarf einer Datenwiederherstellung	BDEW
10.1.	Release Management	Major Release: Neue Hauptfunktionen, potenziell breaking changes	Major Release: Neue Hauptfunktionen, potenziell Abwärtsinkompatibilität	Zur Erhöhung der Verständlichkeit des Dokuments sollte nur ein Begriff für dasselbe verwendet werden. Da unter Minor Release der Begriff "Abwärtsinkompatibilität" bzw. nun "Abwärtskompatibilität" verwendet wird, sollte dieser auch hier verwendet werden.	BDEW
10.1.	Release Management	Minor Release: Erweiterungen, neue Schnittstellen, keine Abwärtsinkompatibilität	Minor Release: Erweiterungen, neue Schnittstellen, Abwärtskompatibilität	Vermeidung doppelter Verneinung zur Erhöhung der Verständlichkeit des Dokuments.	BDEW

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
10.1.	Release Management	Vorlaufzeiten	Vorlaufzeiten (rein informativ)	Die BNetzA legt fest, was und wann etwas geändert wird. Der Hub-Betreiber entscheidet, wie (technisch) und wann genau (im Rahmen der regulatorischen Fristen) ein Release eingespielt wird.	BDEW
10.1.	Release Management	Neue Releases müssen den Marktpartner mit folgender Mindestvorlaufzeit angekündigt werden: ▪ Major Release: mind. 3 Monate ▪ Minor Release: mind. 8 Wochen ▪ Patches: mind. 2 Tage ▪ Hotfix: keine	Über neue Releases infomiert der Hub-Betreiber mit folgenden Vorlaufzeiten: ▪ Major Release: mind. 3 Monate ▪ Minor Release: mind. 8 Wochen ▪ Patches: mind. 2 Tage ▪ Hotfix: keine Alle Änderungen in Prozessen und Schnittstellen erfolgen unverändert im Rahmen des bestehenden, etablierten Änderungsmanagement.	Die BNetzA legt fest, was und wann etwas geändert wird. Der Hub-Betreiber entscheidet, wie (technisch) und wann genau (im Rahmen der regulatorischen Fristen) ein Release eingespielt wird.	BDEW
10.1.	Release Management	Vorabbereitstellung auf Testumgebungen	Aus unserer Sichtweise als IT-Dienstleister sollte eine Testumgebung für das aktuelle Release sowie für das zukünftige Release zur Verfügung gestellt werden, sowie Testumgebungen für einzelne Anfragen/Prozesse (Tests auf Musterstammdaten/Testdaten).	In der Implementierungsphase eines zukünftigen Releases kann es durchaus vorkommen, dass Fehler am aktuellen Release (HotFix) behoben werden müssen. Daher ist der Zugriff auf eine Testumgebung mit dem jeweiligen Release notwendig. Die Fragestellung, wie eine Testumgebung genau aussieht, ist unzureichend beantwortet. Es handelt sich um Stammdaten, die sich laufend ändern. Daher stellt sich für uns die Frage, wie eine Testumgebung mit vielen Marktpartner aussehen kann. Für automatisierte Tests ist es sinnvoll, dass auf einer definierten Stammdatenlage getestet werden kann und dass ggf. Testfälle/Testszenarien für externe Tests bereitgestellt werden.	cortility GmbH
10.1.	Release Management	Semantische Versionierung	Einfache lineare Versionierung des Gesamtsystems	Semantische Versionierung macht Sinn bei Schnittstellen, aber nicht bei einem Gesamtsystem. - Die Schnittstellen gemäß dem aktuellen edi@energy Konzept sind nicht semantisch versioniert, passen also nicht zur Vorgabe hier. - Wegen Abhängigkeiten der Datenformate untereinander kann sich eine semantische Versionierung nur auf die komplette Schnittstelle beziehen. Hierzu hatten wir in unserem Konsultationsbeitrag zum API-Konzept einen Vorschlag unterbreitet. - Für Gesamtsysteme hat sich inzwischen eine lineare Versionierung durchgesetzt, da die Frage nach Kompatibilität immer sehr schwierig zu beantworten ist.	decarbon1ze GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
10.1.	Release Management		Releases leichtgewichtiger gestalten	Die Anforderungen an ein Release sind sehr umfangreich, wie bei konventionellen Server-Systemen. Bei modernen Cloud-native Anwendungen sollten diese Anforderungen überdacht werden zugunsten von mehr Agilität und schnelleren Iterationen. - Z.B. ist in einer Cloud-Native-Umgebung das Testen im Produktivbetrieb möglich, indem einzelne Knoten mit einer neuen Version hochgefahren werden und diese eingehende live-Daten dupliziert als Input bekommen. - Ebenso ist ein Versionswechsel oft nicht als "big-bang" Update zu sehen, sondern kann graduell erfolgen. - Bei einer gut entworfenen REST-API können die meisten Änderungen als rückwärtskompatible Erweiterungen bereitgestellt werden – siehe hierzu unsere Vorschläge im Komsultationspapier zum API-Konzept. - Wichtig ist, dass es ein für Marktpartner und IT-Dienstleister verfügbares Testsystem gibt, gegen welches entwickelt werden kann.	decarbon1ze GmbH
10.1.	Release Management	Rollback-Konzept	streichen	Bei einem komplexen Cloud-Native System mit horizontaler Skalierung ist ein komplettes Rollback nach einem Update praktisch nicht möglich – insbesondere bei einem rollierenden Update, wie im letzten Punkt angesprochen. Die Forderung hier bringt in der Praxis nichts, wäre aber extrem teuer und aufwändig in der Umsetzung. Eine bessere Forderung wäre, kontrolliert und audit-sicher Datenmigrationen einfügen zu können, um Fehler zu beheben.	decarbon1ze GmbH
10.1.	Release Management	oAlle Releases müssen rücksetzbar sein (Rollback oder Hotfix-Fallback). Daten müssen entsprechend aus letztem Snapshot / Sicherheitspunkt wiederhergestellt werden	Formulierung anpassen: Alle Releases müssen rücksetzbar sein (Rollback oder Hotfix-Fallback). Daten müssen entsprechend aus letztem Snapshot / Sicherheitspunkt wiederhergestellt werden können	Wort "können" am Ende ergänzt. Nicht jedes Rücksetzen bedarf einer Datenwiederherstellung	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
10.1.	Release Management		Bitte unter "Versionierungs-System" ergänzen: o Jede Änderung an Daten unterliegt, wie die Software, an sich einem Releasemanagement. Jede Änderung wird gekennzeichnt, welcher Prozess (KI, Schnittstelle, UI) die Änderung getriggert hat und mit welcher Softwareversion (KI, Schnittstelle, UI), die Änderung vorgenommen wurde. Selbstverständlich ist im Änderungslog auch der Zeitstempel und im Falle von Usern oder Batches die User bzw. Batch-ID bzw. Prozess-ID mitzuführen.	Jede Änderung muss nachvollziehbar sein.	E.ON Netze

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
10.1.	Release Management	• Rollout-Strategie: o Vorabbereitstellung auf Testumgebungen	Bitte ergänzen: Rollout-Strategie: o Die Vorabbereitstellung auf Testumgebungen hat spätestens drei Monate vor dem geplanten Produktionsstart zu erfolgen. o Die Testumgebungen müssen funktionsgleich zur Produktionsumgebung sein und alle relevanten Schnittstellen, Rollen und Prozesse abbilden. o Ziel ist die frühzeitige Durchführung von Integrations-, Kompatibilitäts- und Performancetests durch Marktpartner und beteiligte Systeme.	Eine frühzeitige Bereitstellung der Testumgebung ist erforderlich, • um die technische und prozessuale Integration der Marktpartner-Systeme rechtzeitig sicherzustellen, • Kompatibilitäts- und Lasttests unter realitätsnahen Bedingungen durchführen zu können, • die Qualität und Stabilität der Schnittstellenkommunikation (z. B. Validierung, Authentifizierung, Formatkompatibilität) zu prüfen und • notwendige Korrekturen oder Optimierungen vor dem Go-Live umzusetzen, ohne die Produktivumgebung zu gefährden. Durch die Bereitstellung mindestens drei Monate vor Produktionsbeginn wird gewährleistet, dass alle Marktrollen ausreichend Zeit für Testzyklen, Abnahmen und ggf. Zertifizierungen erhalten. Dies erhöht die Betriebssicherheit und Datenqualität im späteren Produktivbetrieb und entspricht den bewährten Vorgehensweisen bei nationalen Hub-Einführungen (z. B. Dänemark, Niederlande).	E.ON Netze
10.1.	Release Management	zu "Rollout-Stategie", zweiter Aufzählluntspunkt: Einhaltung definierter Release-Zyklen (z.B. quartalsweise)	Änderung des Beispiels: Einhaltung definierter Release-Zyklen (z.B. halbjährlich, passend zu den Formatvorgaben)	Reales Beispiel verwenden. Wir können keinen Releasezyklus erkennen, der außerhalb der festgelegten Dokumente liegen kann, ausgenommen es handelt sich um Fehlerbehebungen.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
10.1.	Release Management	zu "Rollout-Strategie", dritter Aufzählungspunkt: Bereitstellung von: ▪ Release Notes ▪ Migration Guides ▪ Testszenarien	Ergänzung der Aufzählung um Schulungskonzept: Bereitstellung von: ▪ Release Notes ▪ Migration Guides ▪ Testszenarien ▪ Schulungskonzept	Uns fehlt die Berücksichtigung von Schulungen (Schulungsunterlagen/Informationsunterlagen) für Mitarbeiter des Betreibers sowie ggf. von Marktpartner zu bestimmten Sachverhalten mit dem Umgang zum MaBiS-Hub. Schulungsaufwände dürfen in einer Releaseplanung nicht unterschätzt werden (insbesondere auch die Aufwände für die Erstellung solcher Unterlagen). Marktpartner müssen die Möglichkeit haben, sich vor Produktivsetzungen mit Neuerungen/Anpassungen vertraut machen zu können, sofern es sich um Sachverhalte handelt, die nicht bereits über die festgeleten Dokumente oder BDEW-Dokumente abgedeckt sind.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
10.1.	Release Management	zu "Vorlaufzeiten": o Neue Releases müssen den Marktpartner mit folgender Mindestvorlaufzeit angekündigt werden: ▪ Major Release: mind. 3 Monate ▪ Minor Release: mind. 8 Wochen ▪ Patches: mind. 2 Tage ▪ Hotfix: keine	Abänderung des Punktes: o Neue Releases werden abhängig der EDI@Energy-Veröffentlichungen und weiteren Festlegungsdokumenten unverzüglich kommuniziert. Anforderungen an den MaBiS-Hub sind immer über die BNetzA abzustimmen/freizugeben. In diesem Zuge und unter Berücksichtigung der Releaseplanung findet die Terminierung der Anforderungen statt.	Die hier beschriebenen Vorlaufzeiten sind für den Markt definitiv zu kurz. Komplette IT- und Fachbereiche müssten sich kurzfristig ausrichten. Dies ist defintiv nicht leistbar und unserer Ansicht nach auch nicht notwendig. Es sind die üblichen Zeiten durch EDI@Energy einzuhalten. Wie bereits heute, kann es unserer Ansicht nach nicht zu Anforderungen kommen, die nicht über die BNetzA "freigegeben" (festgelegt) werden. Aus diesem Grund, muss das Vorgehen in der Releaseplanung mit berücksichtigt werden. Hinweis: Unserer Ansicht nach kann man mit den Release-Arten gearbeitet werden, jedoch sind diese auf das Vorgehen von EDI@Energy zu richten. Es ist bei Fehlerfällen dabei zwischen einer Fehlerbehebung zu unterscheiden, die aufgrund eines Fehlers im Hub entstanden ist oder aufgrund einer Korrektur der Formate.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
10.1.	Release Management	Bereitstellung von: □ Release Notes □ Migration Guides □ Testszenarien	Zu ergänzen wären Schulungsunterlagen für die Betreibergesellschaft, die IT der Marktteilnehmer (API) und das Fachpersonal der Markteilnehmer.		KISTERS AG
10.1.	Release Management	Vorabbereitstellung auf Testumgebungen	Punkt unter Rollout-Strategie	Bitte präzisieren innerhalb welcher Zeitfenster vor dem Release in die produktive Umgebung ein Release in einer Testumgebung bereitzustellen ist. Bitte zudem klarstellen, inwieweit die Testumgebung von Marktpartnern für integrative Tests genutzt werden kann. Aus unserer Sicht ist die Möglichkeit für einen Ende-zu-Ende-Test neuer und geänderten Prozesse zwingend erforderlich.	SAP SE
10.1.	Release Management	"Neue Releases müssen den Marktpartner mit folgender Mindestvorlaufzeit angekündigt werden: ▪ Major Release: mind. 3 Monate ▪ Minor Release: mind. 8 Wochen ▪ Patches: mind. 2 Tage ▪ Hotfix: keine"	Über neue Releases infomiert der Hub-Betreiber mit folgenden Vorlaufzeiten: ▪ Major Release: mind. 3 Monate ▪ Minor Release: mind. 8 Wochen ▪ Patches: mind. 2 Tage ▪ Hotfix: keine Alle Änderungen in Prozessen und Schnittstellen erfolgen unverändert im Rahmen des bestehenden, etablierten Änderungsmanagement.	Die Ankündigung neuer Releases wird in der Governance in einem Releaseboard freigegben. Ein zu schaffendes ReleaseBoard in der Governance stimmt die Planung im Release- Management ab. Die BNetzA begleitet die Änderungen im Rahmen des Änderungsmanagements, was und wann geändert wird. Der Hub-Betreiber führt nach den Regeln des Release Boards entscheidet, wie (technisch) und wann genau (im Rahmen der regulatorischen Fristen) ein Release eingespielt wird.	Thüga SmartService GmbH
10.2.	Change Management	zu "Testpflicht vor Produktivsetzung", erster Aufzählnungspunkt: Jeder Change durchläuft abgestufte Tests (Unit, Integration, UAT)	Anpassung der Klammerangaben: Jeder Change durchläuft abgestufte Tests (Unit, Integration, End-to-End-Test, Regressionstests)	Einheitliches Wording zum Kapitel 6.3. und Berücksichtigung von Regressionstests. Nur Changes, die auch einen Katalog von Regressionstest erfolgreich durchlaufen haben, dürfen deployed werden (s. dazu dritter Aufzählluntspunkt von 10.2.	BDEW
10.2.	Change Management	zu "Testpflicht vor Produktivsetzung", dritter Aufzählnungspunkt: o Nur dokumentierte, geprüfte und freigegebene Changes dürfen deployed werden	Ergänzung: o Nur dokumentierte, geprüfte und freigegebene Changes dürfen deployed werden. Umgesetzt und produktivgesetzt werden nur in sich abgeschlossene Prozessabläufe.	In der Marktkommunikation ist es elementar wichtig, dass nur in sich abgeschlossene Prozessabläufe dem Markt zur Verfügung gestellt werden. Eine massengeschäftstaugliche Abwicklung nach den festgelegten Prozessvorgaben ist sonst nicht gewährleistet.	BDEW

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
10.2.	Change Management	zu "Veränderungskategorien"	Wir gehen davon aus, dass in jedem der Aufzählungspunkte ein Freigabeprozess vorausgeht und nicht nur im "Standard-Change".	Ohne einen Freigabeprozess darf keine Anpassung auf ein Produktivsystem oder auf ein Testsystem für Marktpartner durchgeführt werden. Es ist ein Freigabemanagement vorzusehen. In diesem sehen wir z.B., dass die Verantwortung einer Freigabe immer beim Betreiber liegt. Eine Freigabe wird niemals durch einen Marktpartner erteilt (Freigabetests werden nicht auf Marktpartner „ausgelagert“).	BDEW
10.2.	Change Management	Änderungskategorien	Es fehlt eine Kategorie für regelmäßige Patches und Updates von Bibliotheken.	Die wichtigste Sicherheitsmaßnahme ist, alle Sicherheits-Updates aller verwendeter Bibliotheken und Frameworks regelmäßig (mind. alle vier Wochen) einzuspielen. Dazu braucht es einen leichtgewichtigen Prozess.	decarbon1ze GmbH
10.2.	Change Management	Testpflicht	CI/CD und Infrastructure-as-Code statt schwergewichtiger Freigaben	Moderne Cloud-Systeme werden automatisiert deployed aus einer deklarativen Konfiguration heraus. Tests erfolgen immer bei jeder Änderung am Code mittels Continuous-Integration (CI) Pipelines. Idealerweise erfolgt das Deployment nach automatischen Tests ebenso automatisch (Continuous Deployment - CD).	decarbon1ze GmbH
10.2.	Change Management	•Change-Request-Verfahren: oJeder Änderungsbedarf wird als Change Request (CR) dokumentiert: □Beschreibung, Auswirkung, Verantwortlicher, Prüfdatum □Bewertung von Risiken, Testbedarf und Kommunikationsmaßnahmen oCRs werden durch ein Change Advisory Board (CAB) geprüft und freigegeben	Formulierung anpassen: •Änderungs-Verfahren: oJeder Änderungsbedarf wird in geeigneter Form strukturiert dokumentiert (z.B. Change Request, User Story, ADRs): - Die Bewertung und Freigabe von Änderungen erfolgt durch die jeweils zuständigen Rollen oder Gremien, z.B. durch ein Change Advisory Board (CAB), das Projektteam oder den Product Owner – abhängig von Projektart, Kritikalität und Organisationsstruktur. - Transparenz und Nachverfolgbarkeit werden durch geeignete Tools und Dokumentationsstandards sichergestellt	Es soll keine Vorfestlegung auf die gewählte Umsetzungsform des Projekts gemacht werden. Auch in agilen Projekten werden Änderungen strukturiert dokumentiert, geprüft und überwacht!	Die dt. Übertragungsnetzbetreiber (50Hertz Transmission GmbH, Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH)
10.2.	Change Management	zu "Veränderungskategorien"	Wir gehen davon aus, dass in jedem der Aufzählungspunkte ein Freigabeprozess vorausgeht und nicht nur im "Standard-Change"	Ohne einen Freigabeprozess darf keine Anpassung auf ein Produktivsystem oder auf ein Testsystem für Marktpartner überführt werden. Es ist ein Freigabemanagement vorzusehen. In diesem sehen wir z.B., dass die Verantwortung einer Freigabe immer beim Betreiber liegt. Eine Freigabe wird niemals durch einen Marktpartner erteilt (Freigabetests werden nicht auf Marktpartner „ausgelagert“).	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
10.2.	Change Management	zu "Testpflicht vor Produktivsetzung", erster Aufzählnungspunkt: Jeder Change durchläuft abgestufte Tests (Unit, Integration, UAT)	Anpassung der Klammerangaben: Jeder Change durchläuft abgestufte Tests (Unit, Integration, End-to-End-Test, Regressionstests)	Einheitliches Wording zum Kapitel 6.3. und Berücksichtigung von Regressionstests. Nur Changes, die auch einen Katalog von Regressionstest erfolgreich durchlaufen haben, dürfen deployed werden (s. dazu dritter Aufzählluntspunkt von 10.2.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH
10.2.	Change Management	zu "Testpflicht vor Produktivsetzung", dritter Aufzählnungspunkt: o Nur dokumentierte, geprüfte und freigegebene Changes dürfen deployed werden	Ergänzung: o Nur dokumentierte, geprüfte und freigegebene Changes dürfen deployed werden. Umgesetzt und produktivgesetzt werden nur in sich abgeschlossene Prozessabläufe.	In der Marktkommunikation ist es elementar wichtig, dass nur in sich abgeschlossene Prozessabläufe dem Markt zur Verfügung gestellt werden. Eine massengeschäftstaugliche Abwicklung nach den festgelegten Prozessvorgaben ist sonst nicht gewährleistet.	EnBW Energie Baden-Württemberg AG, Netze BW GmbH

IT- Leitlinien

Tenorziffer	Kapitel	Originaltext	Hinweis/Anmerkung	Begründung	Unternehmen
10.2.	Change Management	Change-Request-Verfahren:	Wie setzt sich das Change Advisory Board (CAB) zusammen? Wie hängen das CAB Emergency-Changes und die Lösungszeiten aus Kapitel 7 "Betrieb und Support" zusammen und wie funktionieren sie ggf. zusammen? Der Prozess muss ggf. durchlaufen werden (CAB-Review) und das für Blocker im Kernsystem < 22 Minuten und das 24/7. Dann muss das CAB auch 24/7 verfügbar sein.		KISTERS AG
10.2.	Change Management	Change Advisory Board (CAB)	Wie setzt sich das "Change Advisory Board (CAB)" zusammen?	Das Change Advisory Board (CAB) sollte in der Governance erläutert werden	Mako365 GmbH