Föderales IT-
Standardisierungsboard

IT-PLANUNGSRAT
Gemeinsam wirksam.

Unterlagen für die 7. Sitzung (Remote)

Stand: 02.07.2025

Agenda

- **TOP 01** – Begrüßung und Feststellung der Beschlussfähigkeit
- **TOP 02** – Mitteilungen des Vorsitz
  - 02.1 – Bericht aus dem IT-Planungsrat
  - 02.2 – SPT-Projekte mit Standardisierungsbezug
  - 02.3 – Allgemeine Mitteilungen
- **TOP 03** – Bericht aus dem Föderalen IT-Architekturboard
  - 03.1 – Bericht zu Aktivitäten im Föderalen IT-Architekturboard
- **TOP 04** – Aktuelle IT-Standardisierungsvorhaben und –bedarfe
  - ~~04.1 – Aufweitung des Standards XPlanung um den Anwendungsfall „kommunale Wärmeplanung“~~ *~~(Wiedervorlage, TOP wurde zurückgezogen)~~*
  - 04.2 – Bedarf für einen Meta-Standard *(→ siehe Sitzungsunterlagen)*
  - 04.3 – Studie zur zukünftigen Ausrichtung von Nachrichtenaustausch von B2G und G2G *(→ siehe Sitzungsunterlagen)*
  - 04.4 – Offene Austauschformate für den länderübergreifenden Austausch von Dokumenten
  - 04.5 – Verschiebung verbindliche Nutzung von XBezahldienste
- **TOP 05** – Bewertungsmethoden
  - 05.1 – Konformitätskriterien des Föderalen IT-Standardisierungsboards für gute IT-Standards *(→ siehe Sitzungsunterlagen)*
- **TOP 06** – Verschiedenes
  - 06.1 – FIT-SB und XÖV-Konferenz 2025
- **TOP 07** – Organisatorisches

VITAKO

SACHSTANDSBERICHT DER UAG

2. Juli 2025

Arne Baltissen

VORGEHENSWEISE DER UAG

- **Externer Input**
  - Best Practices aus den Bereichen Bibliotheken, Wissenschaft, Medizin, RegMo und XÖV Interop-Matrix
- **Erarbeitung Handlungsfelder im Präsenzworkshop**
  - Organisation: Entwurf fertiggestellt – wartet auf Synchronisation
  - Rechtliches: Entwurf fertiggestellt – wartet auf Synchronisation
  - Semantik: Entwurf in Erarbeitung
  - Technik: Wartet auf Semantik
- **Arbeit in den „UUAGs“**
  - An den Handlungsfeldern zur Fertigung einer Vorlage

- **Ziel**

  Erste Vorlage Ende Q3 / Anfang Q4 2025

Zusammenfassung Workshop Berlin

- Was wollen wir erreichen? Was braucht es dazu? Wie wollen wir gemeinsam weiterarbeiten?
- Erkenntnis: Viele der Anforderungen und Ideen werden bereits im Rahmen der RegMo bearbeitet. Daher ist ein intensiver Austausch sinnvoll.
- Zielsetzung: Welche Anforderungen an die RegMo ergeben sich aus Sicht der UAG? Welche Weiterentwicklung ist sinnvoll?
- Handlungsfelder
  - Organisation – Wie kann ein Metastandard für den Datenaustausch gepflegt und gelebt werden?
  - Semantik – Wie kann ein Metastandard aufgebaut sein? Wie kann dabei auch europäisch gedacht werden?
  - Technik – Wie kann ein Metastandard technisch umgesetzt werden?
  - Rechtliches – Welche rechtlichen Aspekte lassen sich als Hebel nutzen?

Arne Baltissen

Geschäftsführer der Prosoz

+49 152 0203 2179

a.baltissen@prosoz.de

VITAKO

Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e.V.

Charlottenstraße 65
10117 Berlin
Tel. 030 2063 156 12
info@vitako.de
www.vitako.de

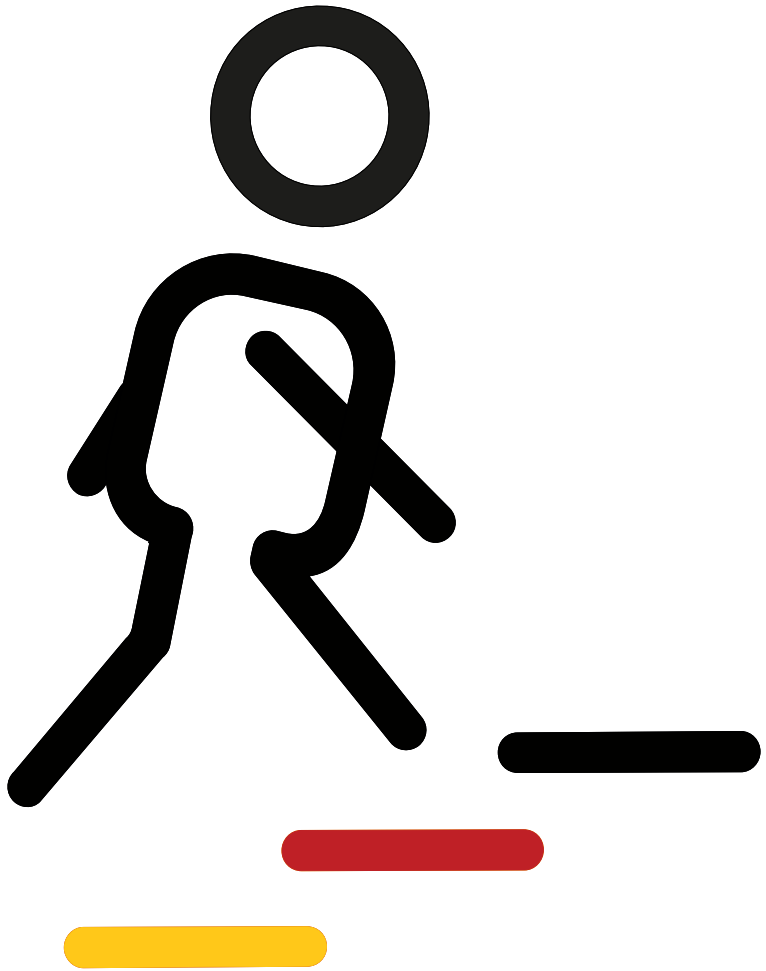
VIELEN DANK!

Studie zur zukünftigen Ausrichtung von Nachrichtenaustausch von B2G und G2G

TOP 04.3 - FIT-SB-Sitzungsunterlage

02.07.2025 | FIT-SB-Sitzung | Tobias Schuh

Inhalt



1. Ausgangslage
2. Anforderungen an die Studie
3. Stakeholdergruppen und Querbezüge
4. Zeitplanung
5. Beteiligung FIT-SB bei Studie

Ausgangslage

Beschluss 2025/18 des IT-Planungsrats

- In seiner **46. Sitzung** hat der **IT-Planungsrat** mit dem Beschluss 2025/18 zur Eskalationsentscheidung OSCI/XTA folgende Entscheidung getroffen:
  - *Der IT-Planungsrat unterstützt die Durchführung einer unabhängigen Studie, um die Fragestellung hinsichtlich der zukünftigen Ausrichtung von Nachrichtenaustausch von B2G (Business to Government) und G2G (Government to Government) inklusive (OSCI und XTA, FIT-Connect, AS4, NOOTS, etc.) verbindlich zu klären. Die Studie erfolgt in Abstimmung mit dem SPT Digitale Anwendungen, dem föderalen IT-Standardisierungsboard und dem föderalen IT-Architekturboard.*

- Die Studie soll durch eine neutrale wissenschaftliche Organisation durchgeführt werden.
  - Die Beauftragung der Studie wird seitens des FIT-SB-Vorsitzes und Themenpaten *„Digitale Transformation“* erfolgen.
  - Die FIT-SB-Geschäftsstelle bei der FITKO unterstützt bei der Vorbereitung beratend.

Anforderungen an die Studie

Inhalte und Vorgehen

Abstimmung Studiendesign

- Abstimmung der Studienziele und Fragestellungen mit:
  - SPT Digitale Anwendungen
  - Gemeinsame Arbeitsgruppe von FIT-AB und FIT-SB

Analyse vorliegender Informationen

- OSCI-Studie des BVA zur Registermodernisierung
- OSCI-Praxistest in NRW
- Fortiss-Studie zu Plattformarchitekturen
- Dokumentationen aktuell eingesetzter IT-Standards, Produkte, etc.
- Weitere?

Ermittlung und Befragung von Stakeholdergruppen

- Direkte Interviews
- Online-Umfragen

Erarbeitung Ausrichtungsvorschlag

- Wissenschaftliche Empfehlungen nach aktuellem und zukunftsorientiertem Stand der Technik
- Best Practices

Ergebnisabstimmung

- Abstimmung der Ergebnisse mit
  - SPT Digitale Anwendungen
  - FIT-AB und FIT-SB
  - Ggf. besonders betroffene Stakeholdergruppen

Fertigstellung Studienbericht

- Beschlussvorschlag für IT-PLR zum weiteren Vorgehen

Stakeholdergruppen und Querbezüge

Ein Überblick

Stakeholdergruppen

IT-Planungsrat
- Bund
- Länder
- SPT Digitale Anwendungen
- FIT-AB
- FIT-SB

Kommunen

Fachministerkonferenzen
- Digital AGs und BLKs

IT-PLR Produkte
- DVDV
- Anwendung Governikus
- FIT-Connect
- Weitere

Gesamtleitung NOOTS

AG CSB

Rechenzentrumsbetreiber

IT-Dienstleister für
- Onlinedienste
- Fachverfahren

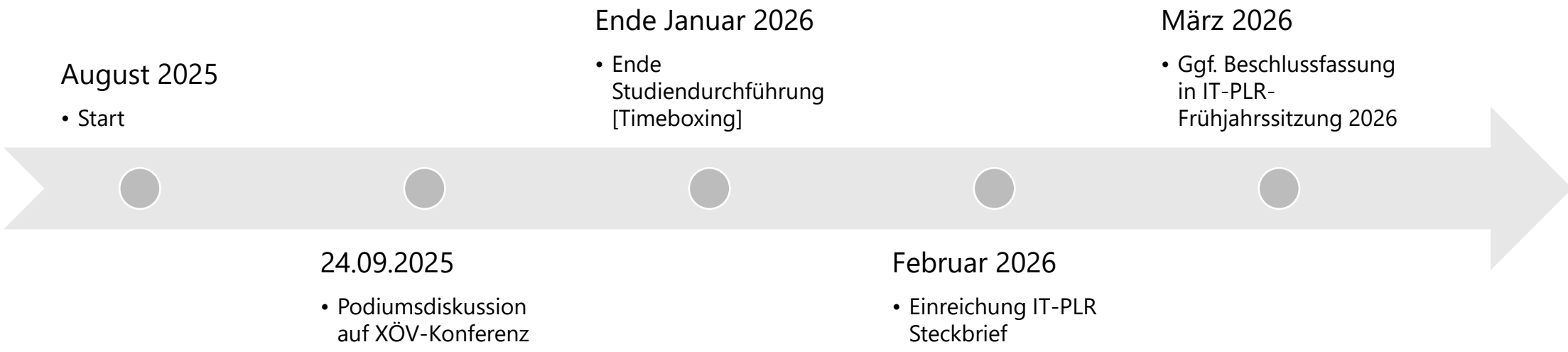
Weitere …

Querbezüge zu anderen Vorhaben

Deutschland-Architektur	• IT-PLR Digitalstrategie • SPT Digitale Anwendungen • FIT-AB
Deutschland-Stack	• Bund
API First	• SPT Digitale Anwendungen
Registermo-dernisierung/ NOOTS	• FITKO • BVA

Zeitplanung

Zeitliche Eckdaten für die Durchführung der Studie



Beteiligung FIT-SB bei der Studie

Beschlussvorschlag

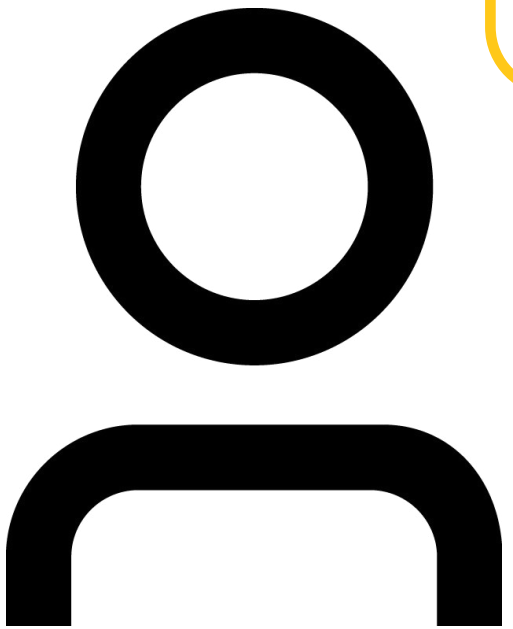
- Die Studie zum Nachrichtenaustausch soll unter anderem in Abstimmung mit dem FIT-AB und dem FIT-SB erfolgen. Dazu wird von den beiden Vorsitzenden des FIT-AB und des FIT-SB eine übergreifende Arbeitsgruppe vorgeschlagen. Diese Arbeitsgruppe soll dann durch die beauftragte wissenschaftliche Organisation in das weitere Vorgehen einbezogen werden.

- **Beschlussvorschlag**
  - Das föderale IT-Standardisierungsboard benennt folgende Mitglieder für eine übergreifende Arbeitsgruppe zusammen mit dem föderalen IT-Standardisierungsboard für die Abstimmungen zur Studie zum Nachrichtenaustausch gemäß IT-PLR-Beschluss 2025/18:
    - xxx

Kontakt

Digitale Verwaltung. Intelligent vernetzt.

www.fitko.de



Tobias Schuh
Standardisierungsmanagement | FIT-SB-Geschäftsstelle

Tobias.Schuh@fitko.de

+49 (69) 401270 142

Mastodon: social.bund.de/@fitkofoederal
LinkedIn: www.linkedin.com/company/fitko-föderale-it-kooperation

Koordinierungsstelle
für IT-Standards

Bewertung von IT-Standards durch das Föderale Standardisierungsboard

Arbeitsfassung des Föderalen Standardisierungsboards

27. 6. 2025

KoSIT

Bewertung von IT-Standards durch das Föderale Standardisierungsboard

27. 6. 2025
KoSIT
Entwurf zur Diskussion am 2.7.2025 im FIT.SB

Die Bewertung von IT-Standards vor einer verbindlichen Vorgabe ist eine der Hauptaufgaben des Föderalen Standardisierungsboards. CAMSS ist ein Rahmenwerkhen Kommission für die neutrale und ergebnisoffene Bewertung von IT-Standards (sowohl Normen und als auch Spezifikationen).

Eine Anpassung an konkrete Fragestellungen und nationale Anforderungen erfolgt mit *Profilen*. Die EU Kommission stellt zwei Profile für europäische Kommunikationsszenarien zur Verfügung. In diesem Dokument werden zwei weitere Profile für den nationalen Kontext vorgeschlagen. So soll erreicht werden, dass nationale Gremien Beschlüsse zu IT-Standards auf der Basis einer neutralen und objektiven Bewertung treffen können mit einer Methodik, die auch von der europäischen Kommission angewandt wird.

Zeitpunkt der Erstellung dieses Dokuments: 27.6.2025 12:11 Uhr.

Inhaltsverzeichnis

Abbildungsverzeichnis

Einführung

Auf der Grundlage des § 2 IT-Staatsvertrag legt der IT-Planungsrat gemeinsame IT-Standards fest. Hierbei ist vorrangig auf bestehende Marktstandards abzustellen. Vor einer Beschlussfassung soll der Bedarf für einen solchen Beschluss sowie die IT-fachliche Qualität und Widerspruchsfreiheit des vorgesehenen Standards durch das Föderale Standardisierungsboard geprüft werden. Der IT-Planungsrat entscheidet unter Einbeziehung der Ergebnisse der Prüfung, ist aber nicht daran gebunden. Die Prüfung muss insbesondere umfassen:

a. Die Prüfung des Bedarfs für einen solchen Beschluss;
b. die Prüfung der IT-fachlichen Qualität und Widerspruchsfreiheit des vorgesehenen Standards;
c. Die Prüfung, ob der Bedarf durch einen Marktstandard gedeckt werden kann.

Im Kontext der Normierungsstrategie der EU 2022 und der europäischen Multi-Stakeholder-Plattform (MSP) werden seitens der Europäischen Kommission vergleichbare Aufgabenstellungen der Prüfung und Bewertung von IT-Standards wahrgenommen. Die EU-Kommission nutzt in diesem Zusammenhang den europäischen "Common Assessment Method for Standards and Specifications (CAMSS)" Ansatz. Der Ansatz bietet einen effizienten und effektiven Prozess zur neutralen und ergebnisoffenen Bewertung von IT-Standards und ist im Einklang mit der Verordnung [EU 1025/2012] zur europäischen Normung. Die Bewertung anhand der CAMSS Methodik unterstützt bei der Entscheidung für bestimmte IT-Standards, ist aber in der Regel nicht die einzige begründende Unterlage. In diesem Dokument wird die Anwendung der CAMSS Methodik auf nationaler Ebene erläutert. So soll erreicht werden, dass der IT-Planungsrat, zuständige Fachministerkonferenzen oder Bundesministerien Beschlüsse zu IT-Standards auf der Basis einer neutralen und objektiven Bewertung treffen können, mit einer Methodik, die auch von der europäischen Kommission angewandt wird.

Europäische und nationale Profile

Die CAMSS Methodik zur Bewertung von IT-Standards ist generisch. Eine Anpassung an konkrete Anforderungen erfolgt mittels Profilen. Mit dem "Profil für den Europäischen Interoperabilitätsrahmen EIF" und dem "Profil für die Multi-Stakeholder Platform" stellt die EU-Kommission zwei Profile zur Verfügung, die zur Bewertung auf der Grundlage *europäischer Anforderungen zur Interoperabilität* geeignet sind. Für das Föderalen Standardisierungsboard ist insbesondere der "EIF Profil" relevant, weil der IT-Planungsrat sich mit dem Beschluss ITPLR 2024/05 zu den 12 Prinzipien des *European Interoperability Frameworks* [EIF 2017] bekannt hat.

Mit dem *EIF Profil* kann bewertet werden, wie sehr ein IT-Standard die Ziele des europäischen Interoperabilitätsrahmens unterstützt. Dies kann für eine Beschlussfassung auf nationaler Ebene eine wichtige Information sein, es müssen aber auch die nationalen Vorgaben berücksichtigt werden. So kann beispielsweise die Konformität zur nationalen / föderalen Architekturrichtlinie wichtiger sein als der Bezug zur *Europäische Interoperabilitäts- Referenzarchitektur (EIRA)* des EIF Profils (siehe Beschluss 2025/17). Zudem gibt es für IT-Standards, die auf dem XÖV Rahmenwerk des IT-Planungsrats basieren, ein seit langem bewährtes Verfahren zu deren Bewertung und Zertifizierung. Deshalb definiert dieses Dokument zusätzliche Profile für eine Bewertung auf der Basis nationaler Vorgaben:

- Das “Profil zur Feststellung der XÖV Konformität” bildet die bewährte Zertifizierung als “XÖV konformer IT-Standard” in der CAMSS Methodik ab. Es kann nur für solche IT-Standards genutzt werden, die mit dem XÖV Rahmenwerk entwickelt werden. Das XRepository weist derzeit 24 XÖV zertifizierte IT Standards aus (Stand Juni 2025). Manche davon sind fachübergreifend, und deshalb im Zuständigkeitsbereich des IT-Planungsrats.
- Das neu entwickelte “Profil für fachunabhängige und fachübergreifende IT Standards” soll zur Bewertung von IT-Standards im Zuständigkeitsbereich des IT-Planungsrats genutzt werden, sofern es sich nicht um XÖV Standards handelt oder solche, bei denen die Interoperabilität mit europäischen Verfahren im Vordergrund steht. Es basiert auf dem *EIF Profil,* referenziert aber nationale Vorgaben zur Digitalisierung.
- Die Existenz zweier unterschiedlicher Profile ist dem Umstand geschuldet, dass das XÖV Rahmenwerk des IT-Planungsrats und die zugehörige XÖV Zertifizierung schon seit Jahren im Praxiseinsatz ist. Die Nutzung der CAMSS Methodik wird hingegen erst seit 2025 erwogen. Daraus entstand einerseits der Bedarf, die XÖV Zertifizierung mit den Mitteln von CAMSS nachzubilden, und andererseits die Notwendigkeit für ein Bewertungsprofil für IT-Standards, die nicht auf dem XÖV Rahmenwerk basieren. Mittelfristig wird Konvergenz mit dem Ziel angestrebt, dass es neben den beiden europäischen Profilen nur eines für nationale IT-Standards im Zuständigkeitsbereich des IT-Planungsrats geben soll, welches gut auf die Prozesse der Standardisierungsagenda abgestimmt ist.

Standardisierungsagenda als Voraussetzung zur Anwendung der nationalen Profile

Die beiden nationalen Profile gehen von funktionierenden Prozessen der in Kapitel 1 dargestellten Standardisierungsagenda aus. Bei der Entscheidung des Föderalen Standardisierungsboards zur Aufnahme eines IT-Standards auf die Standardisierungsagenda werden Kriterien geprüft, die in nationalen CAMSS Profilen ebenfalls genannt werden (dies gilt insbesondere für das Profil für fachunabhängige und fachübergreifende IT Standards), oder implizit vorausgesetzt werden (dies gilt insbesondere für das Profil zur Feststellung der XÖV Konformität).

Die Auflösung von Redundanzen und die transparente Darlegung der Abhängigkeiten ist Gegenstand einer Fortschreibung dieses Dokuments.

Durchführung der Bewertung

Die Bewertung von IT-Standards durch das Föderale Standardisierungsboard soll vor folgenden Entscheidungen des Föderalen Standardisierungsboards erfolgen:

1. Bei der Entscheidung zur Aufnahme eines IT-Standards auf die Standardisierungsagenda.
2. Vor einer Empfehlung an den IT-Planungsrat für einen Beschluss gemäß § 2 IT-Staatsvertrag, oder der Empfehlung des IT-Standards durch das föderale Standardisierungsboard.

Abbildung 1. Prozessmodell der Standardisierungsagenda

Die Entscheidung des Standardisierungsboards folgt nicht automatisch aus der Bewertung, sie soll aber bei der Entscheidungsfindung unterstützen und diese begründen. Vor der Bewertung ist das CAMSS Profil zu bestimmen:

a. Wenn die Interoperabilität zu europäischen Verfahren im Vordergrund steht, soll das Profil für den Europäischen Interoperabilitätsrahmen EIF genutzt werden.

b. Sofern in Ausschreibungen die Konformität zu Normen oder Standards der EU-Kommission gefordert werden soll, ist das Profil für die Multi-Stakeholder Platform einschlägig.

c. Für einen auf der Grundlage des XÖV Standardisierungsrahmens entwickelen IT-Standard soll das Profil zur Feststellung der XÖV Konformität (die XÖV Zertifizierung) angewandt werden.

d. Wenn ein IT-Standard für den nationalen Kontext bewertet werden soll, der nicht auf der Grundlage des XÖV Standardisierungsrahmens entwickelt wurde, soll das Profil für fachunabhängige und fachübergreifende IT Standards gewählt werden.

Wichtig

Die CAMSS Methodik ermöglicht eine neutrale und ergebnisoffene Bewertung von IT-Standards hinsichtlich der im IT-Staatsvertrag genannten Fragestellungen (Bedarfsprüfung, IT-fachliche Qualität und Widerspruchsfreiheit, Marktstandard). Sie berücksichtigt nicht:

- die Akzeptanz und / oder Durchsetzbarkeit beim Bund und den Ländern;
- die mit einer verbindlichen Vorgabe verbundenen Entwicklung- und Betriebskosten

Teil I. Nationale Profile

Inhaltsverzeichnis

Kapitel 1. Die Prozesse der Standardisierungsagenda

Im Folgenden wird das in Abbildung 1 dargestellte Prozessmodell skizziert. Dieses soll von der FITKO gemeinsam mit dem Standardisierungsboard weiterentwickelt werden. Der Text stammt aus dem Dokument “Die Standardisierungsagenda des IT-Planungsrats” vom 5.2.2024, welches dem Beschluss ITPLR 2024/05 zugrunde liegt.

1.1. Übergreifende Prozesse und Aufgaben

Das Prozessmodell gibt einen Plan für den Lebenszyklus von IT-Standards vor. Darin enthalten sind spezifische Phasen, die jeder IT-Standard im Laufe seines Lebenszyklus durchläuft.

Strategische Leitlinien wirken übergreifend auf die spezifischen Prozesse und Aufgaben der Standardisierungsagenda und werden unterstützt durch die Impulse eines Standardisierungsradars.

1.1.1. Standardisierungsradar

Die FITKO betreibt und pflegt (ggf. mit Hilfe Dritter) ein öffentlich zugängliches Standardisierungsradar, das technologische Entwicklungen und Trends der Standardisierung möglichst frühzeitig und proaktiv aufgreift und öffentlich zugänglich präsentiert. Von Seiten des Bundes werden dazu ergänzend erkennbare Trends auf europäischer Ebene eingebracht, bei denen eine Auswirkung auf Standardisierungsbedarfe in Deutschland zu erwarten ist.

Für die Ausgestaltung des Standardisierungsradars wird ein Konzept erarbeitet und mit dem Standardisierungsboard abgestimmt. Eine Orientierung geben bereits existierende Technologieradare.

1.1.2. Strategische Leitlinien

Die strategischen Leitlinien föderaler IT regeln die Ausrichtung gemeinsamer IT- Standardisierung und geben Auskunft, was nicht Gegenstand der gemeinsamen Standardisierungsagenda ist.

Sie sichern u.a. die Anschlussfähigkeit an die europäische Ebene ab und berücksichtigen dabei die „Underlying principles“ des „European Interoperability Frameworks“ (EIF)[1].

Ebenso spiegeln die Leitlinien die strategisch-politische Prioritätensetzung des IT- Planungsrates wider (strategische Bedarfe).

Diese Leitlinien werden mit mehrjähriger Gültigkeit erarbeitet und spätestens nach fünf Jahren zyklisch angepasst. Die Federführung für die initiale Formulierung obliegt dem fachlich zuständigen Bundesministerium des Innern und für Heimat.

Die strategischen Leitlinien werden dem IT-Planungsrat zum Beschluss vorgelegt.

[1] Siehe: interoperability-framework-detailThe European Interoperability Framework in detail

1.2. Lebenszyklusprozess

Zentrales Element der Standardisierungsagenda ist der Lebenszyklusprozess eines föderalen IT-Standards, wie er in der obenstehenden Grafik dargestellt ist.

Er enthält folgende Prozessschritte:

- Identifizierung und Bedarfsmeldung
- Aufnahme, Prüfung, Bewertung und Entscheidung
- Umsetzung
- Genehmigung
- Überführung in Regelbetrieb
- Regelbetrieb und Monitoring
- Dekommissionierung

1.2.1. Identifizierung und Bedarfsmeldung

Im Rahmen eines Anforderungsmanagements nimmt die FITKO Bedarfsmeldungen für IT- Standards auf. Die Bedarfe können dabei proaktiv vom Standardisierungsboard identifiziert oder von anderen Stakeholdern aus der öffentlichen Verwaltung, Wirtschaft oder Zivilgesellschaft gemeldet werden.

1.2.2. Aufnahme, Prüfung, Bewertung und Entscheidung

Die FITKO systematisiert die Eingänge und überprüft den Standardisierungsbedarf anhand klarer Kriterien hinsichtlich Qualität und Nachvollziehbarkeit.

Sie eröffnet ein Beteiligungsverfahren und stellt alle relevanten Informationen effizient und transparent an zentraler Stelle bereit.

Die Umsetzungsverantwortlichen (FITKO, KoSIT, o.a.) bereiten alle erforderlichen Informationen zur Entscheidung über die Umsetzung des Standardisierungsbedarfs vor. Dabei klären diese auch die Erfordernisse notwendiger Ressourcen und Finanzmittel.

Basierend auf den strategischen Leitlinien und anderen Vorgaben des IT-Planungsrat entscheidet das Standardisierungsboard über die Umsetzung eines Standardisierungsbedarfs.

1.2.3. Umsetzung

Die Umsetzungsverantwortlichen initiieren unmittelbar Umsetzungsaufträge zur Normung oder Standardisierung an die private Wirtschaft, öffentliche IT-Dienstleister, Hochschulen oder weitere Akteure.

Die FITKO begleitet die Umsetzung der Standardisierungsvorhaben beratend und berichtet aggregiert über deren Fortschritt.

1.2.4. Genehmigung

Soll ein IT-Standard oder ein Verbund von IT-Standards im föderalen Kontext verbindlich eingeführt werden, dann ist nach §2 Abs. 2 des IT-Staatsvertrags ein Beschluss des IT- Planungsrats erforderlich. Dieser entscheidet auf Grundlage einer Entscheidungsempfehlung des Standardisierungsboards.

Über einen ausschließlich empfohlenen Einsatz eines IT-Standards kann das Standardisierungsboard eigenständig einen Beschluss treffen.

1.2.5. Überführung in Regelbetrieb

Nach der Genehmigung erfolgt die Überführung des IT-Standards in den Regelbetrieb. Die Betriebsüberführung wird gemeinsam vom Umsetzungsteam und dem vorgesehenen Betreiber des IT-Standards durchgeführt.

1.2.6. Regelbetrieb und Monitoring

Die FITKO übernimmt das zentrale Monitoring und überprüft regelmäßig die IT-Standards im Regelbetrieb. Dazu werden verschiedene Kenngrößen ermittelt, um Entscheidungsbedarfe des Standardisierungsboards und anderer Stakeholder zu unterstützen. Die Ergebnisse werden veröffentlicht.

1.2.7. Dekommissionierung

Ergibt die Prüfung, dass ein IT-Standard am Ende seines Lebenszyklus angekommen ist, entscheidet das Standardisierungsboard über dessen Dekommissionierung und macht diese frühzeitig öffentlich bekannt.

Kapitel 2. Profil für fachunabhängige und fachübergreifende IT Standards

Anwendungsbereich

Das Profil für fachunabhängige und fachübergreifende IT Standards dient der Bewertung eines IT-Standards vor einer Beschlussfassung des IT-Planungsrats gemäß § 2 IT-Staatsvertrag. Es soll die IT-fachliche Qualität und Widerspruchsfreiheit des vorgesehenen Standards bewerten. Es kommt zum Einsatz, wenn

a. die Zuständigkeit des IT-Planungsrats gegeben ist;

b. es sich nicht um einen neu entwickelten oder wesentliche geänderten IT-Standard auf Basis des XÖV Rahmenwerks handelt (für den das *XÖV Profil für CAMSS* bzw. die XÖV Zertifizierung einschlägig ist);

c. die Interoperabilität zu europäischen IT-Verfahren keine oder nur eine geringfügige Rolle spielt (andernfalls soll das *CAMSS-Profil für EIF* oder – im Rahmen einer öffentlichen Auftragsvergabe - das CAMSS Profil für die Multi-Stakeholder Plattform MSP, genutzt werden).

ITPLR_01-01	Es handelt sich um einen fachunabhängigen oder fachübergreifenden IT Standard.
ITPLR_01-02	Es gibt in der öffentlichen Verwaltung keinen anderen, bereits beschlossenen IT-Standard mit gleichem oder ähnlichem Standardisierungsgegenstand.
ITPLR_01-03	Der Bedarf an einem IT-Standard ist nachgewiesen
ITPLR_01-04	Der Bedarf an der verbindlichen Vorgabe eines IT-Standardisierungsbedarfs ist nachgewiesen
ITPLR_01-05	Die Möglichkeit der Vorgabe eines Marktstandards im Sinne des § 2 Abs 1 Satz 2 IT-Staatsvertrag wurde geprüft
ITPLR_02-01	Alle Interessensträger können sich diskriminierungsfrei an der Entwicklung und Weiterentwicklung des IT-Standards beteiligen.
ITPLR_02-02	Eine öffentliche Überprüfung ist Teil des Releasezyklus
ITPLR_02-03	Die Lizenzierung der geistigen Eigentumsrechte an dem IT-Standard erfolgt zu FRAND -Bedingungen
ITPLR_02-04	Der IT-Standard unterstützt die Bereitstellung offener Verwaltungsdaten
ITPLR_03-01	Inwieweit geht der IT-Standard nachvollziehbar auf Abläufe, Bestimmungen, Daten und Dienstleistungen der Verwaltung ein?
ITPLR_04-01	Werden verbindlich beschlossene Kerndatenmodelle angemessen berücksichtigt?

ITPLR_04-02	Werden bewährte Datenobjekte, Codelisten und Prozessmuster in angemessenem Umfang wiederverwendet?
ITPLR_05-01	Ist der IT-Standard technologieneutral?
ITPLR_06-01	Inwieweit ermöglicht der IT-Standard einen sicheren Datenaustausch?
ITPLR_06-02	Inwieweit gewährleistet der IT-Standard die Authentizität und Authentifizierung der an einem Datenaustausch beteiligten Akteure?
ITPLR_07-01	Wird die DIN 91379 für die Schreibweise von Namen angemessen berücksichtigt?
ITPLR_08-01	Trägt der IT-Standard zur Umsetzung des Once Only Prinzips bei?
ITPLR_09-01	Inwieweit ermöglicht der IT-Standard die langfristige Bewahrung von Daten/Informationen/Wissen?
ITPLR_10-01	Ist der IT-Standard geeignet, den gemeldeten Bedarf zu decken?
ITPLR_10-02	Ist der IT-Standard detailliert genug, konsistent und vollständig für die Verwendung und Entwicklung von Produkten und Dienstleistungen?
ITPLR_10-03	Basiert der IT-Standard auf Normen oder Marktstandards im Sinne des § 2 Abs. 1 Satz 2 IT-Staatsvertrag
ITPLR_10-04	Basiert der IT-Standard auf einem Fachmodell, welches etablierte Modellierungsmethoden nutzt?
ITPLR_10-05	Hat der IT-Standard die notwendige Reife
ITPLR_11-01	Die öffentliche Verwaltung muss die Entwicklung und Weiterentwicklung des IT-Standards ausreichend kontrollieren und steuern können.
ITPLR_11-02	Ist der dauerhafte Betrieb des IT-Standards gewährleistet?
ITPLR_11-03	Entspricht der IT-Standard den einschlägigen Vorgaben der föderalen Architekturrichtlinie?
ITPLR_12-01	Wird der IT-Standard von verschiedenen Anbietern/Lieferanten für unterschiedliche Implementierungen verwendet?

2.1. Subsidiarität und Verhältnismäßigkeit

2.1.1. ITPLR_01-01: Es handelt sich um einen fachunabhängigen oder fachübergreifenden IT Standard.

Der IT-Planungsrat ist gemäß IT-Staatsvertrag nur für fachunabhängige oder fachübergreifende IT Standards zuständig.

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft die Bedarfsbeschreibung und die funktionale Beschreibung des IT-Standards daraufhin, ob dieser frei von fachlichen Aspekten ist (fachunabhängig), oder ob unterschiedliche fachliche Bereiche / Ressorts betroffen sind (fachübergreifend).

2.1.2. ITPLR_01-02: Es gibt in der öffentlichen Verwaltung keinen anderen, bereits beschlossenen IT-Standard mit gleichem oder ähnlichem Standardisierungsgegenstand.

Zu betrachten sind:

- Beschlüsse oder Empfehlungen des IT-Planungsrats zu IT-Standards gemäß IT-Staatsvertrag;
- Technische Richtlinien des BSI;
- Vorgaben zur Nutzung von IT-Standards im Fachrecht (Zuständigkeitsbereich von Fachministerkonferenzen);

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Die FITKO ist Geschäftsstelle des IT-Planungsrats und hat den Überblick über alle vom IT-Planungsrat beschlossenen IT-Standards. Sie führt außerdem die Standardisierungsagenda des IT-Planungsrats, und das Standardisierungsradar, das technologische Entwicklungen und Trends der Standardisierung möglichst frühzeitig und proaktiv aufgreift und öffentlich zugänglich präsentiert.
Bund	Von Seiten des Bundes werden erkennbare Trends auf europäischer Ebene eingebracht, sowie Informationen zu technischen Richtlinien des BSI.
DIN	DIN prüft das Deutsche Informationszentrum für technische Regeln (DITR).
KoSIT	Die KoSIT prüft das XRepository hinsichtlich XÖV Standards und Standardisierungsinitiativen.

2.1.3. ITPLR_01-03: Der Bedarf an einem IT-Standard ist nachgewiesen

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Im Rahmen des Anforderungsmanagements für die Standardisierungsagenda systematisiert FITKO die Bedarfsmeldungen und überprüft den Standardisierungsbedarf anhand klarer Kriterien hinsichtlich Qualität und Nachvollziehbarkeit. Sie eröffnet ein Beteiligungsverfahren und stellt alle relevanten Informationen effizient und transparent an zentraler Stelle bereit.

2.1.4. ITPLR_01-04: Der Bedarf an der verbindlichen Vorgabe eines IT-Standardisierungsbedarfs ist nachgewiesen

215 Ggfs. ist eine Empfehlung ausreichend.

Zuständigkeiten im Rahmen der Prüfung	
216 Standardisierungs- 217 board	Prüft, ob es zur Erreichung der Ziele zwingend einer verbindlichen Vorgabe des IT-Planungsrats auf der Grundlage des § 2 IT-Staatsvertrag bedarf.

2.1.5. ITPLR_01-05: Die Möglichkeit der Vorgabe eines Marktstandards im Sinne des § 2 Abs 1 Satz 2 IT-Staatsvertrag wurde geprüft

218 Gemäß § 2 Abs. 1 Satz 2 ist vorrangig auf bestehende Marktstandards abzustellen.

Zuständigkeiten im Rahmen der Prüfung	
219 DIN	prüft, ob der Standardisierungsbedarf mit einer Norm gedeckt werden kann.
220 FITKO	prüft, ob der Standardisierungsbedarf mit einem Markstandard gedeckt werden kann.

2.2. Offenheit

2.2.1. ITPLR_02-01: Alle Interessensträger können sich diskriminierungsfrei an der Entwicklung und Weiterentwicklung des IT-Standards beteiligen.

Zuständigkeiten im Rahmen der Prüfung	
221 FITKO	prüft das Betriebskonzept, sofern vorhanden, und die verfügbaren Unterlagen zur Organisation der Entwicklung bzw. Weiterentwicklung.

2.2.2. ITPLR_02-02: Eine öffentliche Überprüfung ist Teil des Releasezyklus

222 Eine Überprüfung durch die Öffentlichkeit kann zur Offenheit des IT-Standards beitragen, sofern
223 Interessen der öffentlichen Verwaltung nicht entgegenstehen.

Zuständigkeiten im Rahmen der Prüfung	
224 FITKO	prüft das Betriebskonzept, sofern vorhanden, und die verfügbaren Unterlagen zur Organisation der Entwicklung bzw. Weiterentwicklung.

2.2.3. ITPLR_02-03: Die Lizenzierung der geistigen Eigentumsrechte an dem IT-Standard erfolgt zu FRAND -Bedingungen

die Lizenzierung der geistigen Eigentumsrechte an der Spezifikation soll fair, angemessen und diskriminierungsfrei in einer Weise erfolgen, die eine Integration sowohl in proprietäre als auch quelloffene Software zulässt, und dies vorzugsweise in gebührenfreier Form.

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft die Lizenzbedingungen

2.2.4. ITPLR_02-04: Der IT-Standard unterstützt die Bereitstellung offener Verwaltungsdaten

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft die Bedarfsbeschreibung und die funktionale Beschreibung des IT-Standards daraufhin, ob die Bereitstellung offener Verwaltungsdaten unterstützt wird. Wenn das der Fall ist, **muss** der Beschluss 2018/11 zur Metadatenstruktur für offene Verwaltungsdaten mit dem Standard DCAT-AP.de beachtet werden.

2.3. Transparenz

2.3.1. ITPLR_03-01: Inwieweit geht der IT-Standard nachvollziehbar auf Abläufe, Bestimmungen, Daten und Dienstleistungen der Verwaltung ein?

Zuständigkeiten im Rahmen der Prüfung	
Standardisierungsboard	Prüft die Bedarfsbeschreibung und die funktionale Beschreibung des IT-Standards daraufhin, ob Abläufe, Bestimmungen, Daten und Dienstleistungen der Verwaltung umfassend, zutreffend und verständlich modelliert sind.

2.4. Wiederverwendung

2.4.1. ITPLR_04-01: Werden verbindlich beschlossene Kerndatenmodelle angemessen berücksichtigt?

Kerndatenmodelle tragen erheblich zur Interoperabilität bei. Derzeit gibt es mindestens zwei Kerndatenmodelle, die zu berücksichtigen sind:

- Das Kerndatenmodell XUnternehmen
- Das Kerndatenmodell elektronischer Rechnungen (gemäß EN 16931 bzw. XRechnung)

Zuständigkeiten im Rahmen der Prüfung	
FITKO und KoSIT	Prüfen die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards daraufhin, ob verbindlich beschlossene Kerndatenmodelle angemessen berücksichtigt werden.

2.4.2. ITPLR_04-02: Werden bewährte Datenobjekte, Codelisten und Prozessmuster in angemessenem Umfang wiederverwendet?

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DIN und KoSIT oder anderer Mitglieder des FIT.SB – die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards daraufhin, ob bewährte Datenobjekte, Codelisten und Prozessmuster in angemessenem Umfang wiederverwendet werden. Bei der Prüfung sollen auch europäische Datenmodelle wie SEMIC Core Vocabularies und Terminologien berücksichtigt werden.

2.5. Technologieneutralität

2.5.1. ITPLR_05-01: Ist der IT-Standard technologieneutral?

Bei der Beurteilung kann die EIF Empfehlung 8: “Bürgern und Unternehmen und anderen Verwaltungseinrichtungen sollten keine technischen Lösungen aufgezwungen werden, die eine bestimmte Technik vorschreiben oder in keinem Verhältnis zu ihren tatsächlichen Bedürfnissen stehen” zugrunde gelegt werden.

Ggfs. ist die verbindliche Vorgabe bestimmter Produkte unvermeidlich oder sogar durch die öffentliche Verwaltung erwünscht, beispielsweise die Verwendung des vom BVA entwickelten “Sicheren Anschlussknotens (SAK)” als Bestandteil der Anschlussbedingungen an das NOOTS.

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO, KoSIT oder anderer Mitglieder des FIT.SB – die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards daraufhin, ob der IT-Standard technologieneutral ist.

2.6. Sicherheit und Privatsphäre

2.6.1. ITPLR_06-01: Inwieweit ermöglicht der IT-Standard einen sicheren Datenaustausch?

Dieses Kriterium ist nur bei solche IT-Standards einschlägig, die dem Datenaustausch zwischen oder mit öffentlichen Stellen dienen. Der Nachweis kann geführt werden

- indem der IT-Standard selbst die erforderlichen Sicherheitsmaßnahmen definiert;
- oder indem er auf andere IT-Standards referenziert, die den sicheren Datenaustausch ermöglichen (beispielsweise die vom IT-Planungsrat für diese Zwecke herausgegebenen IT-Standards XTA und OSCI).

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO, KoSIT oder anderer Mitglieder des FIT.SB und ggfs. des BSI – die Selbstauskunft der Betreiber des IT-Standards und ggfs. die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards hinsichtlich der Schutzstufe der Daten, die übermittelt werden, und ob der sichere Datenaustausch sichergestellt ist.

2.6.2. ITPLR_06-02: Inwieweit gewährleistet der IT-Standard die Authentizität und Authentifizierung der an einem Datenaustausch beteiligten Akteure?

Dieses Kriterium ist nur bei solche IT-Standards einschlägig, die dem Datenaustausch zwischen oder mit öffentlichen Stellen dienen. Der Nachweis kann geführt werden

- indem der IT-Standard selbst die erforderlichen Maßnahmen der Authentizität und Authentifizierung definiert;
- oder indem er auf andere IT-Standards oder Produkte referenziert, die entsprechende Maßnahmen ermöglichen (z. B. IAM für Behörden, Service- und Unternehmenskonto, eID Produkte etc.)

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO, KoSIT oder anderer Mitglieder des FIT.SB und ggfs. des BSI – die Selbstauskunft der Betreiber des IT-Standards und ggfs. die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards hinsichtlich der Schutzstufe der Daten, die übermittelt werden, und ob die Authentizität und Authentifizierung der an einem Datenaustausch beteiligten Akteure angemessen festgestellt werden kann.

2.7. Mehrsprachigkeit

Hinweis: vor verschiedenen Seiten wurde angemerkt, dass es weiterer Kriterien bedarf, um die EIF-Prinzip “Mehrsprachigkeit” angemessen zu prüfen. Konkrete Formulierungsvorschläge für weitere Kriterien werden gern entgegengenommen.

2.7.1. ITPLR_07-01: Wird die DIN 91379 für die Schreibweise von Namen angemessen berücksichtigt?

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO, KoSIT oder anderer Mitglieder des FIT.SB – die Selbstauskunft der Betreiber des IT-Standards und

Zuständigkeiten im Rahmen der Prüfung	
	ggfs. die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards daraufhin, ob Datenfelder für Namen von Personen, Produkten etc. die DIN 91379 in Verbindung mit dem Beschluss 2022/51 des IT-Planungsrats angemessen umsetzen.

2.8. Verwaltungsvereinfachung

2.8.1. ITPLR_08-01: Trägt der IT-Standard zur Umsetzung des Once Only Prinzips bei?

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO, KoSIT oder anderer Mitglieder des FIT.SB – die Selbstauskunft der Betreiber des IT-Standards und ggfs. die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards daraufhin, ob der IT-Standard zur Umsetzung des Once Only Prinzips beiträgt.

2.9. Informationsbewahrung

2.9.1. ITPLR_09-01: Inwieweit ermöglicht der IT-Standard die langfristige Bewahrung von Daten/Informationen/Wissen?

Wie wird geprüft?

Als Nachweis dieses Kriteriums muss in der Dokumentation der Spezifikation der Schwerpunkt auf die langfristige Bewahrung von Informationen gelegt und diese sichergestellt werden.

2.10. Qualität, Effektivität und Effizienz

2.10.1. ITPLR_10-01: Ist der IT-Standard geeignet, den gemeldeten Bedarf zu decken?

Zuständigkeiten im Rahmen der Prüfung	
Bedarfsträger	Prüft – ggfs. mit Unterstützung von Mitgliedern des Standardisierungsboards und dem Betreiber des IT-Standards, der geprüft wird – ob der IT-Standard geeignet ist, den gemeldeten Bedarf zu decken.

2.10.2. ITPLR_10-02: Ist der IT-Standard detailliert genug, konsistent und vollständig für die Verwendung und Entwicklung von Produkten und Dienstleistungen?

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO, KoSIT oder anderer Mitglieder des FIT.SB – die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards daraufhin, ob die detailliert genug, konsistent und vollständig für die Verwendung und Entwicklung von Produkten und Dienstleistungen ist.

2.10.3. ITPLR_10-03: Basiert der IT-Standard auf Normen oder Marktstandards im Sinne des § 2 Abs. 1 Satz 2 IT-Staatsvertrag

Dieses Kriterium ist nur anzuwenden für IT-Standards, die nicht selbst eine Norm oder ein Marktstandard sind. In diesem Fall sollen sie zumindest auf anerkannten Normen bzw. Markstandards (z. B. solchen, die in der CAMSS Liste von Standards aufgeführt sind, wie XML, JSON, https etc.) basieren.

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO, KoSIT oder anderer Mitglieder des FIT.SB – die Selbstauskunft der Betreiber des IT-Standards und ggfs. die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards daraufhin, ob der IT-Standard auf Normen oder Marktstandards basiert.

2.10.4. ITPLR_10-04: Basiert der IT-Standard auf einem Fachmodell, welches etablierte Modellierungsmethoden nutzt?

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO, KoSIT oder anderer Mitglieder des FIT.SB – die Selbstauskunft der Betreiber des IT-Standards und ggfs. die funktionale Beschreibung daraufhin, ob der IT-Standard auf einem Fachmodell basiert, welches mit etablierten Modellierungsmethoden (UML, BPMN, TOGAF, Archimed etc.) erstellt worden ist.

2.10.5. ITPLR_10-05: Hat der IT-Standard die notwendige Reife

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO, KoSIT oder anderer Mitglieder des FIT.SB – die Selbstauskunft der Betreiber des IT-Standards und die

Zuständigkeiten im Rahmen der Prüfung	
	aktuelle Releasehistorie daraufhin, ob die notwendige Stabilität und Reise des Standards erreicht ist.

2.11. Digitale Souveränität

2.11.1. ITPLR_11-01: Die öffentliche Verwaltung muss die Entwicklung und Weiterentwicklung des IT-Standards ausreichend kontrollieren und steuern können.

Es muss ausgeschlossen werden, dass einzelne Akteure eines Standardisierungsvorhabens die Entwicklung so steuern, dass der IT-Standard für die Verwaltung unbrauchbar oder sein Einsatz unwirtschaftlich wird.

Zuständigkeiten im Rahmen der Prüfung	
FIT.SB	Prüfung des Betriebskonzepts des IT-Standards hinsichtlich der Einflussmöglichkeiten der öffentlichen Verwaltung. In manchen Anwendungsfällen kann es erforderlich sein, dass die öffentliche Verwaltung das alleinige Entscheidungsrecht hat. Dies gilt insbesondere dann, wenn der IT-Standard unmittelbare Bezüge zu fachrechtlichen Regelungen hat. In anderen Fällen, insbesondere bei Normen, kann es ausreichend sein, dass Entscheidungen nicht gegen den Willen der öffentlichen Verwaltung getroffen werden können. (“Konsens” gemäß Anhang II Nr. 3b der Normenverordnung [EU 1025/2012].

2.11.2. ITPLR_11-02: Ist der dauerhafte Betrieb des IT-Standards gewährleistet?

Zu prüfen sind:

- eine langfristig sichergestellte, ausreichende Finanzierung des Betriebs und ggfs. der Weiterentwicklung;
- eine stabile Betriebsorganisation mit klar benannten Zuständigkeiten.

Zuständigkeiten im Rahmen der Prüfung	
FIT.SB	Prüft das Betriebskonzept des IT-Standards daraufhin, ob der dauerhafte oder zumindest sehr langfristige Betrieb gewährleistet ist.

2.11.3. ITPLR_11-03: Entspricht der IT-Standard den einschlägigen Vorgaben der föderalen Architekturrichtlinie?

Zuständigkeiten im Rahmen der Prüfung	
FIT.AB	Prüft – ggfs. zusammen mit Mitgliedern des FIT.SB – die Selbstauskunft der Betreiber des IT-Standards und ggfs. die funktionale Beschreibung daraufhin, ob

Zuständigkeiten im Rahmen der Prüfung	
	der IT-Standard den einschlägigen Vorgaben der föderalen Architekturrichtlinie entspricht.

2.12. Marktakzeptanz

2.12.1. ITPLR_12-01: Wird der IT-Standard von verschiedenen Anbietern/ Lieferanten für unterschiedliche Implementierungen verwendet?

Zuständigkeiten im Rahmen der Prüfung	
FITKO	Prüft – ggfs. unter Einbeziehung von DATABUND, VITAKO oder anderer Mitglieder des FIT.SB – die Selbstauskunft der Betreiber des IT-Standards und Erkenntnisse des Standardisierungsradars, ob der IT-Standard von verschiedenen Anbietern/Lieferanten für unterschiedliche Implementierungen verwendet wird.

287

Kapitel 3. Profil zur Feststellung der XÖV Konformität

Anwendungsbereich

Das *XÖV Profil für CAMSS* dient der Bewertung, ob der jeweilige IT-Standard konform zu den Vorgaben des XÖV Rahmenwerks ist. Das XÖV Rahmenwerk ist ein Beitrag des IT-Planungsrats für eine Stärkung der Interoperabilität durch Wiederverwendung bewährter fachlicher Komponenten. Bewertet werden in der Regel fachliche oder fachübergreifende IT-Standards für Datenübermittlungen zwischen und mit öffentlichen Stellen. Aufgrund verbindlicher technischer Vorgaben ist das XÖV Profil faktisch nur für IT-Standards nutzbar, die im Auftrag der öffentlichen Verwaltung neu entwickelt oder wesentlich verändert werden.

Viele XÖV Standards werden nicht vom IT-Planungsrat, sondern der jeweils zuständigen Fachministerkonferenz oder einem Bundesministerium verantwortet. Daher kann das XÖV Profil für CAMSS auch anderen Stellen als dem IT-Planungsrat bei der Bewertung von Spezifikationen dienen, beispielsweise vor einer verbindlichen Vorgabe eines IT-Standards in fachrechtlichen Regelungen zu elektronischen Datenübermittlungen.

Dieses Profil bildet den seit langem bestehenden Prozess der XÖV Zertifizierung mit der CAMSS Methodik nach. Die technischen Vorgaben der XÖV Methodik erleichtern eine teilautomatisierte Bewertung der Standards.

XÖV steht für die Bestrebung, vorhandene IT-Verfahren stärker als bisher durch den Einsatz standardisierter Technologien und Verfahren zu vernetzen. Hierzu stellt die Koordinierungsstelle für IT-Standards (KoSIT) im Auftrag des IT-Planungsrats ein Rahmenwerk zur Entwicklung von XÖV-Standards bereit. Es besteht aus bewährten Methoden und Werkzeugen zur Entwicklung von IT-Standards, wiederverwendbaren Lösungen (Kerndatenmodellen, Datenstrukturen und Codelisten), dem zentralen XRepository sowie den in diesem Abschnitt dargestellten Anforderungen an IT-Standards. In einem transparenten Zertifizierungsverfahren wird überprüft, ob ein IT-Standard den Anforderungen entspricht. Nur wenn es erfolgreich verlaufen ist, darf der Standard als “XÖV Standard” bezeichnet werden.

Der XÖV Standardisierungsrahmen kann und soll angewandt werden, wenn ein Standardisierungsbedarf bestätigt wurde, und die Recherche zum Ergebnis führt, dass kein geeigneter Martktstandard zur Verfügung steht, so dass die Neuentwicklung eines IT-Standards geboten ist. Da man in dieser Situation keine Rücksicht auf bereits bestehende Lösungen und Abwärtskompatibilität nehmen muss, gibt der XÖV Standardisierungsrahmen viele technische Eigenschaften des neuen IT-Standards vor. Dadurch entstehen viele Vorteile wie z. B. die automatisierte Auswertung der Fachmodelle. Das XÖV Szenario unterscheidet sich in diesem Aspekt deutlich von den anderen CAMSS Szenarien, die technologisch offener sind (mit dem Nachteil der aufwändigeren Prüfung aufgrund des geringeren Automatisierungsgrades).

XÖV Standards dienen typischerweise der Modellierung von Datenübermittlungen auf der Basis fachrechtlicher Regelungen der öffentlichen Verwaltung. Ihre Nutzung wird in der Regel rechtlich vor-

gegeben. Die Zuständigkeit für den XÖV-Standard liegt häufig bei der für den jeweiligen Rechtsbereich zuständigen Fachministerkonferenz, alternativ beim IT-Planungsrat.

Die Charakterisierung von XÖV Standards soll an einem typischen Beispiel erläutert werden:

- Nach der Änderung des Melderechtsrahmengesetzes im Jahr 2003 beschließt der zuständige Arbeitskreis der Innenministerkonferenz das Ziel, "die Geschäftsprozesse im Meldewesen möglichst elektronisch abzuwickeln". Dies soll ohne Eingriff in den Markt auf Basis offener Standards geschehen. Damit hat die IMK einen Standardisierungsbedarf für den Bereich des Melderechts formuliert.
- Die Recherche führt zu dem Ergebnis, dass kein Marktstandard für das nationale Melderecht vorhanden ist, so dass zur Erreichung der Ziele eine Neuentwicklung geboten ist. Diese erfolgt innerhalb des XÖV Standardisierungsrahmens mit den vorgegebenen Werkzeugen und Technologien, und führt zum Ergebnis “XMeld”. Der neue IT-Standard enthält Datenstrukturen (“Name”, “Meldeanschrift” etc.) und Codelisten (“Geschlecht”, “Familienstand”, “Gemeindeschlüssel”). Die fachliche Erarbeitung und Qualitätssicherung erfolgt durch Expertinnen und Experten des Melderechts aus allen Verwaltungsebenen. Seine technischen Eigenschaften werden erfolgreich zertifiziert, damit wird XMeld zu einem XÖV Standard.
- Die IMK als zuständige Fachministerkonferenz baut eine Gremienstruktur auf, um die Fortentwicklung des IT-Standards anhand fachlicher Anforderungen zu organisieren, und stellt sicher, das rechtliche Regelungen und die Möglichkeiten der Digitalisierung auf Basis des IT-Standards aufeinander abgestimmt werden. Sie finanziert die Entwicklung und den Betrieb von XMeld. Dessen verpflichtende Nutzung wird in Übermittlungsverordnungen des Bundes verbindlich vorgegeben.

  Inzwischen ist XMeld zusammen mit anderen Standards für Sachverhalte des Ausländer- oder Personenstandswesens ein Fachmodul im XÖV Standard “XInneres” geworden.

Das Prinzip der Wiederverwendung, das dem XÖV-Standardisierungsrahmen zugrunde liegt, sowie die Erschließung der damit verbundenen Nutzenpotenziale erfordern bestimmte Voraussetzungen. Die Regelungen des XÖV-Standardisierungsrahmens wurden entwickelt, um diese Voraussetzungen zu erfüllen und dadurch sowohl für einzelne Vorhaben als auch für die öffentliche Verwaltung insgesamt Nutzen zu stiften. Sie sind in die Bereiche *Konformitätskriterien* und *Namens- und Entwurfsregeln (Naming and Design Rules, NDR)* strukturiert. Konformitätskriterien decken die unterschiedlichen methodischen, organisatorischen und technischen Bereiche eines Standardisierungsvorhabens ab. Demgegenüber wird mit den Namens- und Entwurfsregeln ausschließlich die technische Ausgestaltung des Standards geregelt. Deren Einhaltung wird durch die Konformitätskriterien gefordert.

XÖV-Konformitätskriterien sind konkrete Prüfkriterien, die ein XÖV-Standard erfüllt. Sie sind in vier Bereiche unterteilt

- Bereitstellungspflichten,
- Auskunftspflichten der entwickelnden und betreibenden Stellen,
- Wiederverwendung der XÖV-Bausteine, sowie
- technische Kriterien.

Es wird zwischen den Verbindlichkeitsstufen *MUSS* und *SOLL* unterschieden:

- *MUSS*: Kriterien dieser Verbindlichkeitsstufe müssen durch ein XÖV-Vorhaben und seinen Standard eingehalten werden.
- *SOLL*: Kriterien dieser Verbindlichkeitsstufe ermöglichen die Abweichung des XÖV-Vorhabens und seines Standards. Der Ansatz der kontinuierlichen Verbesserung erfordert allerdings, dass die Begründung für die Abweichung zur Zertifizierung dokumentiert wird.

Die normative Quelle für die XÖV Kriterien ist das von der KoSIT herausgegebene XÖV Handbuch in der jeweils aktuellen Fassung. Sie werden hier zwecks Vergleichbarkeit mit anderen CAMSS Szenarien wiederholt, und bilden die Grundlage für die Zertifizierung der XÖV-Konformität.

Anwendung im Zusammenhang mit der Standardisierungsagenda

Bei der Bewertung von IT-Standards für den IT-Planungsrat setzt die XÖV Zertifizierung, und damit auch die Anwendung des CAMSS Profils zur Feststellung der XÖV Konformität, die Prozesse der Standardisierungsagenda voraus. Kriterien, die im Rahmen der Entscheidung zur Aufnahme eines IT-Standards auf die Standardisierungsagenda geprüft werden, wie beispielsweise der Nachweis des Bedarfs, werden in diesem Profil nicht wiederholt, sondern implizit vorausgesetzt.

Die transparente Darlegung der Abhängigkeiten ist Gegenstand einer Fortschreibung dieses Dokuments.

XOEV-01 (muss)	Eigentümerin des XÖV-Standards muss die öffentliche Verwaltung sein, d. h. sie bestimmt seine Inhalte und hat alle Rechte am Standard inne. Weiter entscheidet sie über Entwicklung und Pflege sowie über die Verwendung des Standards.
XOEV-02 (muss)	Der XÖV-Standard muss frei von Rechten Dritter sein. Er muss innerhalb der öffentlichen Verwaltung der Bundesrepublik Deutschland und für die Nutzer ihrer Dienstleistungen uneingeschränkt und unentgeltlich verwendbar sein und bleiben.
XOEV-03 (muss)	Ein XÖV-Standard muss alle Informationen bereitstellen, die erforderlich sind, um eine standard-konforme Schnittstelle für IT-Verfahren entwickeln zu können. Hierzu gehören zwingend die Beschreibung des Standards durch seine Metadaten sowie die Bereitstellung der XSD-Schemata und eines dazu konsistenten Spezifikationsdokuments.
XOEV-04 (muss)	Die Zertifizierung ist ausschließlich über das XRepository zu beantragen. Der XÖV-Standard muss mit seinem Spezifikationsdokument als PDF-Datei, seinen XSD-Schemata, seines XÖV-Fachmodells sowie seinem Pflegekonzept nach erfolgter Zertifizierung unverzüglich im XRepository veröffentlicht werden. Darüber hinaus müssen alle durch den Standard genutzten Codelisten, wenn sie durch den Standard herausgegeben werden, im XRepository veröffentlicht sein.
XOEV-05 (muss)	Für den XÖV-Standard muss ein Pflegekonzept vorliegen, aus dem erkennbar wird, dass eine langfristige Wartung und Fortschreibung gewährleistet wird.
XOEV-06 (muss)	Der Beginn der Entwicklung eines XÖV-Standards muss der Öffentlichkeit so früh wie möglich durch Angabe der Metadaten des Standards im XRepository angezeigt werden.

		Bei Bedarf können ergänzende Informationen zum Standard mittels weiterer im XRepository bereitgestellter Dokumente zur Verfügung gestellt werden.
386	XOEV-07 (muss)	Die für die Entwicklung und die Pflege des XÖV-Standards zuständige Stelle (Organisationseinheit der öffentlichen Verwaltung) muss die Metadaten des Standards im XÖV-Fachmodell des Standards und im XRepository pflegen und aktuell halten.
387	XOEV-11 (muss)	Die Beziehungen der fachlichen Bausteine eines XÖV-Standards zu den durch die XÖV-Koordination in der XÖV-Bibliothek veröffentlichten XÖV-Kernkomponenten sollen identifiziert und ausgezeichnet werden. Hierfür ist die im XÖV Handbuch beschriebene Methodik anzuwenden.
388	XOEV-12 (muss)	Bei fachlicher Eignung sollen XÖV-Standards die mit der XÖV-Bibliothek herausgegebenen XÖV-Datentypen anstelle eigener Datentypen verwenden. Hierzu ist die im XÖV Handbuch dargelegte Methodik anzuwenden.
389	XOEV-13 (muss)	Bei fachlicher, organisatorischer und rechtlicher Eignung soll eine im XRepository bereitgestellte Codeliste der im XÖV Handbuch beschriebenen Methodik folgend wiederverwendet und damit der Entwicklung einer neuen Codeliste vorgezogen werden.
390	XOEV-08 (soll)	Die Prozesse in deren Rahmen die durch den XÖV-Standard spezifizierten Nachrichten übermittelt werden, sollen unter Verwendung der UML-Notation als Aktivitätsdiagramme beschrieben werden. Bei der Beschreibung ist der Fokus auf die Aktivitäten und Abläufe, die zum Erstellen, Übermitteln und Verarbeiten der Nachrichten führen zu setzen.
391	XOEV-09 (muss)	Die Modellierung der Datenstrukturen des XÖV-Standards muss in einem XÖV-Fachmodell unter Verwendung der XÖV-Modellierungssprache in der Notation *XÖV classic* oder *XÖV lite* erfolgen.
392	XOEV-10 (muss)	XÖV-Namens- und Entwurfsregeln müssen entsprechend ihrer Verbindlichkeit bei der Spezifikation eins XÖV-Standards berücksichtigt werden. Das schließt die Verwendung der von der XÖV-Koordination veröffentlichten XÖV Produktionsumgebung in der zum Zeitpunkt der Beantragung der Zertifizierung jeweils gültigen Version ein.
393	XOEV-14 (muss)	Das XÖV-Fachmodell muss fehlerfrei durch die von der XÖV-Koordination herausgegebenen XÖV Produktionsumgebung in der zum Zeitpunkt der Beantragung der Zertifizierung jeweils gültigen Version verarbeitet werden können. Dies beinhaltet die Prüfung der automatisiert auswertbaren XÖV-Regelungen und die fehlerfreie Erzeugung der XSD-Schemata.
394	XOEV-15 (soll)	Ein XÖV-Standard soll zur Erfüllung der in dem jeweiligen fachlichen Kontext notwendigen Sicherheitsanforderungen die im Auftrag der öffentlichen Verwaltung und insbesondere des IT-Planungsrats betriebenen Lösungen in angemessenem Umfang berücksichtigen. Hierzu zählen unter anderem:

3.1. Bereitstellungspflichten

Diese Kriterien klären von wem und wie ein XÖV-Standard bereitzustellen ist. Insbesondere werden die Mindestanforderungen an die Offenheit eines XÖV-Standards festgelegt.

3.1.1. XOEV-01: Eigentümerin des XÖV-Standards muss die öffentliche Verwaltung sein, d. h. sie bestimmt seine Inhalte und hat alle Rechte am Standard inne. Weiter entscheidet sie über Entwicklung und Pflege sowie über die Verwendung des Standards.

Begründung: Die Entscheidung der öffentlichen Verwaltung über ihre Prozesse soll nicht durch kommerzielle Abhängigkeiten geprägt werden.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüft den Im XRepository bereitgestellter Standard mit beantragter XÖV-Zertifizierung hinsichtlich einer expliziten Bestätigung, dass sich der Standard im Besitz der öffentlichen Verwaltung der Bundesrepublik Deutschland befindet.

3.1.2. XOEV-02: Der XÖV-Standard muss frei von Rechten Dritter sein. Er muss innerhalb der öffentlichen Verwaltung der Bundesrepublik Deutschland und für die Nutzer ihrer Dienstleistungen uneingeschränkt und unentgeltlich verwendbar sein und bleiben.

Begründung: Mit der freien Verfügbarkeit möchte man die Herstellerunabhängigkeit von Schnittstellen und deren Wiederverwendbarkeit fördern.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestellte Bestandteile des Standards und seiner Version Prüfinhalt: Alle Bestandteile des Standards und seiner Version sind frei von Rechten Dritter

3.1.3. XOEV-03: Ein XÖV-Standard muss alle Informationen bereitstellen, die erforderlich sind, um eine standard-konforme Schnittstelle für IT-Verfahren entwickeln zu können. Hierzu gehören zwingend die Beschreibung des Standards durch seine Metadaten sowie die Bereitstellung der XSD-Schemata und eines dazu konsistenten Spezifikationsdokuments.

Begründung: Eine standard-konforme Schnittstelle für IT-Verfahren kann nur (weiter-) entwickelt werden, wenn der XÖV-Standard und seine Version über ihre Metadaten eindeutig identifiziert und beschrieben werden können und alle zur Implementierung notwendigen Informationen zur Verfügung stehen.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestelltes XÖV Fachmodell[a], XSD-Schemata und Spezifikationsdokument des Standards liegen vollständig und konsistent vor Prüfinhalt: XÖV-Fachmodell, Spezifikationsdokument und zugehörige XSD-Schemata des Standards

[2]

3.1.4. XOEV-04: Die Zertifizierung ist ausschließlich über das XRepository zu beantragen. Der XÖV-Standard muss mit seinem Spezifikationsdokument als PDF-Datei, seinen XSD-Schemata, seines XÖV-Fachmodells sowie seinem Pflegekonzept nach erfolgter Zertifizierung unverzüglich im XRepository veröffentlicht werden. Darüber hinaus müssen alle durch den Standard genutzten Codelisten, wenn sie durch den Standard herausgegeben werden, im XRepository veröffentlicht sein.

Begründung: Das XRepository ist die zentrale Distributionsplattform des XÖV-Standardisierungsrahmens.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im Repository bereitgestelltes XÖV Fachmodell, die im Kontext des Standards herausgegebenen Codelisten und Bestandteile des Standards und seiner Version Prüfinhalt: Existenz von XSD-Schemata, Spezifikationsdokument in PDF, XÖV-Fachmodell, im Kontext des Standards herausgegebenen Codelisten sowie Pflegekonzept

3.1.5. XOEV-05: Für den XÖV-Standard muss ein Pflegekonzept vorliegen, aus dem erkennbar wird, dass eine langfristige Wartung und Fortschreibung gewährleistet wird.

Begründung: Investitionssicherheit für implementierende IT-Verfahrenshersteller sowie für Standards, die explizit auf anderen Standards aufbauen, soll sichergestellt werden.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestellte Bestandteile des Standards Prüfinhalt: Existenz eines Pflegekonzeptes mit Angaben zu den Aufgaben, Rollen und Verantwortlichkeiten, zur für die Pflege zuständigen Stelle sowie zur Finanzierung des Pflegebetriebs

[2] [a] Das XÖV-Fachmodell muss für die prüfende Stelle in der Notation *XÖV classic* (XMI-Format und proprietäres Format des genutzten UML-Modellierungswerkzeugs) oder *XÖV lite* (Format XML) bereitgestellt werden

3.2. Auskunftspflichten der entwickelnden und betreibenden Stellen

Auskunftspflichten beziehen sich auf Kriterien, bei denen die Verantwortlichen eines Standards Informationen zu ihrem Vorhaben aufbereiten und veröffentlichen. Diese Informationen dienen im Wesentlichen der Transparenz zu Inhalten und Rahmenbedingungen des Standardisierungsvorhabens und sollen die Wiederverwendung fördern.

3.2.1. XOEV-06: Der Beginn der Entwicklung eines XÖV-Standards muss der Öffentlichkeit so früh wie möglich durch Angabe der Metadaten des Standards im XRepository angezeigt werden. Bei Bedarf können ergänzende Informationen zum Standard mittels weiterer im XRepository bereitgestellter Dokumente zur Verfügung gestellt werden.

Begründung: Redundante Entwicklungen für dieselben fachlichen Anforderungen sollen vermieden und eine Beteiligung weiterer Stakeholder ermöglicht werden.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestellte Informationen zum Standard Prüfinhalt: Metadaten zum Standard liegen vollständig vor

3.2.2. XOEV-07: Die für die Entwicklung und die Pflege des XÖV-Standards zuständige Stelle (Organisationseinheit der öffentlichen Verwaltung) muss die Metadaten des Standards im XÖV-Fachmodell des Standards und im XRepository pflegen und aktuell halten.

Begründung: Schaffen von Transparenz hinsichtlich der XÖV-Standards. Redundante Entwicklungen für denselben fachlichen Sachverhalt sollen vermieden und Synergien ermöglicht werden.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository verfügbare Metadaten des Standards und seiner Version Prüfinhalt: Die Metadaten des Standards und seiner Version sind aktuell und regelkonform

3.3. Wiederverwendung der XÖV-Bausteine

Die Nutzung der XÖV-Bausteine in XÖV-Standards unterstützt die standardübergreifende Interoperabilität und stellt damit einen zentralen Aspekt der XÖV-Konformität dar.

3.3.1. XOEV-11: Die Beziehungen der fachlichen Bausteine eines XÖV-Standards zu den durch die XÖV-Koordination in der XÖV-Bibliothek veröffentlichten XÖV-

Kernkomponenten sollen identifiziert und ausgezeichnet werden. Hierfür ist die im XÖV Handbuch beschriebene Methodik anzuwenden.

Begründung: Die Auszeichnung der Beziehungen ermöglicht der XÖV-Koordination die Auswertung der Gemeinsamkeiten und Unterschiede zwischen den Bausteinen von Standards und den XÖV-Kernkomponenten, sowie deren fachliche Motivation. Die Ergebnisse der Auswertung werden über die im XRepository verfügbare Interopmatrix für alle XÖV-Vorhaben bereitgestellt. Die Interopmatrix macht die Bausteine eines Standards und seine fachliche Ausgestaltung sichtbar und mit den Bausteinen anderer Standards vergleichbar und fördert so sowohl die Wiederverwendung als auch die Harmonisierung der bereitgestellten XÖV-Kernkomponenten.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestelltes XÖV Fachmodell; Begründung eventuell unvollständiger Auszeichnung Prüfinhalt: Fachspezifische Bausteine (Datenstrukturen) des Standards hinsichtlich ihrer Beziehungen zu XÖV-Kernkomponenten; Begründung eventuell unvollständiger Auszeichnung

3.3.2. XOEV-12: Bei fachlicher Eignung sollen XÖV-Standards die mit der XÖV-Bibliothek herausgegebenen XÖV-Datentypen anstelle eigener Datentypen verwenden. Hierzu ist die im XÖV Handbuch dargelegte Methodik anzuwenden.

Begründung: Die Verwendung einheitlicher XÖV-Datentypen verbessert die Interoperabilität und erleichtert die Implementierung. Die einheitliche Wiederverwendung existierender Bausteine anderer Standards und Normen wird durch die Bereitstellung von XÖV-Adaptern gefördert.

Datentypen anderer XML-Fachstandards und Normen dürfen in XÖV-Standards genutzt werden. Falls für sie in der XÖV-Bibliothek ein XÖV-Adapter zur Verfügung steht, soll eine Nutzung über den entsprechenden Adapter erfolgen.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestelltes XÖV Fachmodel, ggfs. Begründung von Abweichungen Prüfinhalt: Datentypen des Standards; Begründung eventueller Abweichungen

3.3.3. XOEV-13: Bei fachlicher, organisatorischer und rechtlicher Eignung soll eine im XRepository bereitgestellte Codeliste der im XÖV Handbuch beschriebenen Methodik folgend wiederverwendet und damit der Entwicklung einer neuen Codeliste vorgezogen werden.

Begründung: Verbesserung der Interoperabilität durch einheitliche Verwendung von Codes.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestelltes XÖV Fachmodell, Begründung eventueller Abweichungen Prüfinhalt: Datenstrukturen hinsichtlich der verwendeten Codelisten; Begründung eventueller Abweichungen

3.4. Technische Kriterien

Die technischen Kriterien der XÖV-Konformität beziehen sich auf das XÖV-Fachmodell und seine Abbildung in XSD. Diese Kriterien sind durch die Verwendung der XÖV Produktionsumgebung weitestgehend automatisiert überprüfbar.

3.4.1. XOEV-08: Die Prozesse in deren Rahmen die durch den XÖV-Standard spezifizierten Nachrichten übermittelt werden, sollen unter Verwendung der UML-Notation als Aktivitätsdiagramme beschrieben werden. Bei der Beschreibung ist der Fokus auf die Aktivitäten und Abläufe, die zum Erstellen, Übermitteln und Verarbeiten der Nachrichten führen zu setzen.

Begründung: Das gemeinsame Verständnis der Prozesse ist wichtig für die Spezifikation konkreter Nachrichten. Die Dokumentation der Prozesse im Spezifikationsdokument des Standards stellt eine wichtige Grundlage für die Umsetzung der korrekten Abläufe, Prüfungen und Entscheidungen sowie einer kontextspezifischen Befüllung von Nachrichten in einem IT-Verfahren dar. UML ist eine anerkannte Notation für die Modellierung von Prozessen.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestelltes Spezifikationsdokument des Standards; Begründung eventueller Abweichungen Prüfinhalt: UML-Aktivitätsdiagramme; Begründung eventueller Abweichungen

3.4.2. XOEV-09: Die Modellierung der Datenstrukturen des XÖV-Standards muss in einem XÖV-Fachmodell unter Verwendung der XÖV-Modellierungssprache in der Notation *XÖV classic* oder *XÖV lite* erfolgen.

Begründung: Die XÖV-Modellierungssprache umfasst genau die für die Modellierung der Inhalte des XÖV-Fachmodells erforderlichen Sprachelemente und erlaubt damit eine zielgerichtete, einheitliche und wohldefinierte Entwicklung. Sie bietet eine geeignete Abstraktion für die Beschreibung von Datenstrukturen und erlaubt eine integrierte Sicht auf die Bestandteile eines XÖV Fachmodells. Die Verwendung der XÖV-Modellierungssprache ist eine Voraussetzung für die Verarbeitung durch die XÖV Produktionsumgebung. Das XÖV Fachmodell ist Grundlage für die XÖV-Konformitätsprüfung.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestelltes XÖV Fachmodell.

Zuständigkeiten im Rahmen der Prüfung	
	Prüfinhalt: Fehlerfreie Verarbeitung des XÖV Fachmodell[a] durch den XGenerator und die XÖV Produktionsumgebung

3

3.4.3. XOEV-10: XÖV-Namens- und Entwurfsregeln müssen entsprechend ihrer Verbindlichkeit bei der Spezifikation eins XÖV-Standards berücksichtigt werden. Das schließt die Verwendung der von der XÖV-Koordination veröffentlichten XÖV Produktionsumgebung in der zum Zeitpunkt der Beantragung der Zertifizierung jeweils gültigen Version ein.

459 Begründung: Die Interoperabilität von XÖV-Standards soll bereits auf der Modellebene unterstützt
460 werden. Die Anwendung der XÖV-Namens- und Entwurfsregeln leistet auf der einen Seite einen
461 Beitrag zur korrekten Anwendung der XÖV-Modellierungssprache und stellt auf der anderen Seite die
462 konkrete Umsetzung grundleger XÖV-Prinzipien und -Methodik im XÖV-Fachmodell sicher.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestelltes XÖV Fachmodell. Prüfinhalt: Validierung des XÖV-Fachmodells und Generierung der XSD Schemata durch Einsatz der XÖV Produktionsumgebung

463

3.4.4. XOEV-14: Das XÖV-Fachmodell muss fehlerfrei durch die von der XÖV-Koordination herausgegebenen XÖV Produktionsumgebung in der zum Zeitpunkt der Beantragung der Zertifizierung jeweils gültigen Version verarbeitet werden können. Dies beinhaltet die Prüfung der automatisiert auswertbaren XÖV-Regelungen und die fehlerfreie Erzeugung der XSD-Schemata.

464 Begründung: Die Qualitätsziele des XÖV-Standardisierungsrahmens können nur durch einen hohen
465 Automatisierungsgrad bei Erzeugung und Qualitätssicherung der Bestandteile eines XÖV-Standards
466 erreicht werden.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestelltes XÖV Fachmodell. Prüfinhalt: Einhaltung der technisch implementierten XÖV-Regelungen

467

3.4.5. XOEV-15: Ein XÖV-Standard soll zur Erfüllung der in dem jeweiligen fachlichen Kontext notwendigen Sicherheitsanforderungen die im Auftrag der öffentlichen Verwaltung und insbesondere des IT-Planungsrats betriebenen

[3] [a] Die zertifizierende Stelle nutzt für XÖV Fachmodelle in der Syntax *XÖV classic* das von der XÖV-Koordination empfohlene Long-Term-Release des Modellierungswerkzeugs MagicDraw oder eine aktuelle Version des Open-Source-Modellierungswerkzeugs Papyrus zur Verarbeitung des XÖV Fachmodells. Weitere Editionen und Versionen der Modellierungswerkzeuge sind nach Absprache möglich.

Lösungen in angemessenem Umfang berücksichtigen. Hierzu zählen unter anderem:

Begründung: Die öffentliche Verwaltung entwickelt und betreibt Infrastrukturkomponenten, die sich an sicheren elektronischen Diensten (Secure Web Services) orientieren. Neben der dafür erforderlichen Standardisierung elektronischer Dienste auf fachlicher Ebene ist vor allem auch die Sicherheit bei der Inanspruchnahme und Erbringung der Dienste zu gewährleisten. Methodische und technische Grundlagen der fachlichen Standardisierung und der Infrastrukturkomponenten sind aufeinander abgestimmt. Die Wirtschaftlichkeit von Infrastrukturkomponenten ist umso höher, je größer die Zahl der Nutzenden ist. Aus diesem Grund, und wegen der abgestimmten Weiterentwicklung fachlicher und sicherheitstechnischer Standards im Sinne sicherer elektronischer Dienste, empfehlen die KoSIT und das Bundesministerium des Innern (BMI) die angemessene Nutzung der von der öffentlichen Verwaltung entwickelten Infrastrukturkomponenten.

Zur sicheren Infrastruktur gehören unter anderem:

- **Sicherheitsinfrastruktur:** Public Key Infrastructure der Verwaltung (PKI-1-Verwaltung),
- **Gesicherte Datenübermittlung:** Online Services Computer Interface (OSCI-Transport) und
- **Adressierungsdienst und Kommunikationsinfrastruktur:** Deutsches Verwaltungsdienstever-zeichnis DVDV.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage: Im XRepository bereitgestellte Informationen zum Standard; Begründung eventueller Abweichungen Prüfinhalt: Metadaten und Spezifikationsdokument des Standards, ggf. weitere zum Standard bereitgestellte Dokumente mit Angaben zur Verwendung der sicheren Infrastruktur; Begründung eventueller Abweichungen

3.5. Prüfung der XÖV-Konformität

Die Abschnitt 3.5, „Prüfung der XÖV-Konformität“ bietet allen Vorhaben und Betreibenden die Möglichkeit, die Konformität ihres Standards in einer bestimmten Version zu den XÖV-Konformitätskriterien bestätigen zu lassen.

Mit der Vergabe eines XÖV-Zertifikats durch die XÖV-Koordination wird eine formale und technische Mindestqualität eines Standards bestätigt. Dies kann zur Sicherung der Qualität der Arbeitsergebnisse innerhalb des eigenen Vorhabens genutzt werden. Zudem soll die Zertifizierung insbesondere beim Rollout des XÖV-Standards unterstützen sowie Vertrauen bei den beteiligten Behörden, Herstellern von IT-Verfahren und anderen an der Datenübermittlung Beteiligten schaffen.

Der Zertifizierungsprozess kann durch den Betreiber eines Standards nach der Bereitstellung aller zertifizierungsrelevanten Dokumente über das XRepository erfolgen.

Zertifizierungsrelevante Dokumente sind das XÖV Fachmodell, die XSD-Schemata und das Spezifikationsdokument zu einer Version des Standards. Darüber hinaus müssen das Pflegekonzept des

Standards sowie ein Dokument mit den zertifizierungsrelevanten Begründungen zur Beantragung der Zertifizierung bereitgestellt werden.

Die Prüfung der Konformität eines Standards zu den für XÖV-Standards geltenden XÖV-Regelungen, insbesondere der Namens- und Entwurfsregeln, erfolgt zu einem erheblichen Teil automatisiert anhand des XÖV Fachmodells.

Teil II. Europäische Profile

Inhaltsverzeichnis

Kapitel 4. Profil für den Europäischen Interoperabilitätsrahmen EIF

Anwendungsbereich

Das *CAMSS-Szenario für EIF* ermöglicht die Bewertung, ob die Interoperabilitätsspezifikationen in Einklang mit dem Europäische Interoperabilitätsrahmen (EIF) stehen. Ziel der Bewertung ist es festzustellen, ob die bewertete Interoperabilitätsspezifikation für die Erbringung interoperabler europäischer öffentlicher Dienste geeignet ist.

Das EIF-Szenario enthält verschiedene Abschnitte entsprechend den Erkenntnissen und Empfehlungen des Europäischen Interoperabilitätsrahmens (EIF).

Die verschiedenen Abschnitte des Szenarios sind in Kriterien untergegliedert, die als Kriterium 1 (A1), Kriterium 2 (A2) usw. angegeben werden. Für jedes Kriterium gibt es eine Anleitung oder Hilfestellung zur Beantwortung (siehe unten).

Das vorliegende Dokument bezieht sich auf die neueste Version der CAMSS-Bewertung nach EIF-Szenario – Version 6.0.0. Auch wenn das Vorgehen für verschiedene Versionen verwendet werden kann, da einige Kriterien unverändert bleiben, orientiert sich das vorliegende Dokument konkret an Version 6.0.0 des Szenarios. Wenn Sie eine frühere Version verwenden, sollten Sie auf das als Komponente des jeweiligen Szenarios bereitgestellte Vorgehen zurückgreifen.

Der Europäische Interoperabilitätsrahmen (EIF) bietet öffentlichen Verwaltungen anhand einer Reihe von Empfehlungen Orientierung dabei, wie sie die Governance ihrer Interoperabilitätsmaßnahmen verbessern, organisationsübergreifende Beziehungen herstellen, durchgehende digitale Dienste unterstützende Prozesse optimieren und sicherstellen, dass neue Rechtsvorschriften den Bemühungen um Interoperabilität nicht entgegenwirken.

Die verschiedenen Kriterien im EIF-Szenario ergeben sich aus den Empfehlungen des Europäischen Interoperabilitätsrahmens (EIF).

EIF-A01	Inwieweit wurde die Spezifikation in einen nationalen Katalog eines Mitgliedstaats aufgenommen, dessen nationaler Interoperabilitätsrahmen laut den Informationsblättern (Factsheets) der Beobachtungsstelle für die nationalen Interoperabilitätsrahmen (NIFO, National Interoperability Framework Observatory) einen hohen Entwicklungsstand aufweist?
EIF-A02	Ermöglicht die Spezifikation die Veröffentlichung von Daten im Internet?
EIF-A03	Inwieweit können die Interessenträger zur Entwicklung der Spezifikation beitragen?
EIF-A04	Inwieweit ist eine öffentliche Überprüfung Teil des Versionszyklus?
EIF-A05	Inwieweit gelten Beschränkungen und Lizenzgebühren für die Verwendung der Spezifikation?

527	EIF-A06	Inwieweit ist die Spezifikation für ihre Verwendung bei der Entwicklung digitaler Lösungen/Dienste ausreichend ausgereift?
528	EIF-A07	Inwieweit hat die Spezifikation für ihre Verwendung bei der Entwicklung digitaler Lösungen/Dienste eine ausreichende Marktakzeptanz erreicht?
529	EIF-A08	Inwieweit wird die Spezifikation von mindestens einer Gemeinschaft unterstützt?
530	EIF-A09	Inwieweit ermöglicht die Spezifikation die Sichtbarkeit von Abläufen, Bestimmungen, Daten und Dienstleistungen der Verwaltung?
531	EIF-A10	Inwieweit geht die Spezifikation nachvollziehbar auf Abläufe, Bestimmungen, Daten und Dienstleistungen der Verwaltung ein?
532	EIF-A11	Inwieweit ermöglicht die Spezifikation Schnittstellen für den Zugang zu Dienstleistungen der Verwaltung?
533	EIF-A12	Inwieweit kann die Spezifikation auch in einem anderen als dem ursprünglich angedachten Kontext verwendet, d. h. bereichsübergreifend genutzt und umgesetzt werden?
534	EIF-A13	Ist die Spezifikation technologieunabhängig?
535	EIF-A14	Ist die Spezifikation plattformunabhängig?
536	EIF-A15	Inwieweit erlaubt die Spezifikation Teilumsetzungen?
537	EIF-A16	Kann die Spezifikation angepasst werden?
538	EIF-A17	Kann die Spezifikation erweitert werden?
539	EIF-A18	Inwieweit ermöglicht die Spezifikation die Datenportabilität zwischen Systemen/Anwendungen, um die Umsetzung oder Weiterentwicklung europäischer öffentlicher Dienste unterstützen?
540	EIF-A19	Inwieweit erlaubt die Spezifikation, relevante Informationen bei Bedarf weiterzuverwenden?
541	EIF-A20	Inwieweit ermöglicht die Spezifikation einen barrierefreien Zugang?
542	EIF-A21	Inwieweit gewährleistet die Spezifikation den Schutz personenbezogener Daten, die von öffentlichen Verwaltungen verarbeitet werden?
543	EIF-A22	Sieht die Spezifikation Mittel zur Beschränkung des Zugangs zu Informationen/Daten vor?
544	EIF-A23	Ist die Spezifikation Teil eines europäischen oder nationalen Vorhabens zu Datenschutzaspekten?
545	EIF-A24	Inwieweit ermöglicht die Spezifikation einen sicheren Datenaustausch?

546	EIF-A25	Inwieweit ermöglicht die Spezifikation eine sichere Datenverarbeitung?
547	EIF-A26	Inwieweit gewährleistet die Spezifikation die Authentizität und Authentifizierung der an einem Datenaustausch beteiligten Akteure?
548	EIF-A27	Inwieweit werden Informationen vor unbefugten Änderungen geschützt?
549	EIF-A28	Inwieweit gewährleistet und ermöglicht die Spezifikation eine korrekte Datenverarbeitung?
550	EIF-A29	Inwieweit ist in der Spezifikation ein Verfahren zur Zugriffskontrolle vorgesehen?
551	EIF-A30	Inwieweit könnte die Spezifikation in einem mehrsprachigen Kontext verwendet werden?
552	EIF-A31	Erleichtert die Spezifikation die Erbringung europäischer öffentlicher Dienste?
553	EIF-A32	Ermöglicht die Spezifikation Kanäle für die Erbringung digitaler Dienste?
554	EIF-A33	Inwieweit ermöglicht die Spezifikation die langfristige Bewahrung von Daten/Informationen/Wissen (einschließlich elektronischer Aufzeichnungen)?
555	EIF-A34	Inwieweit werden Bewertungen der Effektivität der Spezifikation vorgenommen?
556	EIF-A35	Inwieweit werden Bewertungen der Effizienz der Spezifikation vorgenommen?
557	EIF-A36	Nimmt die Spezifikation Bezug auf die Europäische Interoperabilitäts-Referenzarchitektur (EIRA) oder wäre dies möglich?
558	EIF-A37	Inwieweit kann bewertet werden, ob die Umsetzungen der Spezifikation die Vorgaben einhalten?
559	EIF-A38	Wird die Spezifikation von einem europäischen Mitgliedstaat empfohlen?
560	EIF-A39	Ist die Spezifikation für ein grenzüberschreitendes europäisches Projekt/eine grenzüberschreitende europäische Initiative ausgewählt worden?
561	EIF-A40	Ist die Spezifikation in einem offenen nationalen Normenverzeichnis/-katalog enthalten?
562	EIF-A41	Ist die Spezifikation in einem offenen europäischen Normenverzeichnis/-katalog enthalten?
563	EIF-A42	Ist die Spezifikation eine europäische Norm?
564	EIF-A43	Ermöglicht die Spezifikation eine Geschäftsprozessmodellierung?
565	EIF-A44	Inwieweit ermöglicht die Spezifikation Vereinbarungen über organisatorische Interoperabilität?
566	EIF-A45	Ermuntert die Spezifikation zur Gründung von Gemeinschaften und zum Austausch ihrer Daten und Ergebnisse auf nationalen und/oder europäischen Plattformen?

4.1. Grundsätze für die Interoperabilität in der EU

Diese Kategorie beruht auf Grundsatz 1 des EIF: Subsidiarität und Verhältnismäßigkeit. Mit diesem Grundsatz soll sichergestellt werden, dass EU-Maßnahmen ergriffen oder angekündigt werden, um nationale Maßnahmen oder Entscheidungen zu verbessern. Insbesondere soll festgestellt werden, ob die nationalen Interoperabilitätsrahmen an den EIF angeglichen sind.

4.1.1. EIF-A01: Inwieweit wurde die Spezifikation in einen nationalen Katalog eines Mitgliedstaats aufgenommen, dessen nationaler Interoperabilitätsrahmen laut den Informationsblättern (Factsheets) der Beobachtungsstelle für die nationalen Interoperabilitätsrahmen (NIFO, National Interoperability Framework Observatory) einen hohen Entwicklungsstand aufweist?

Die NIFO-Factsheets finden Sie:

- Alte Factsheets bis 2017
- Aktuelle Factsheets
- Beispiel: Deutschland 2024

EIF Empfehlung 1: *Sicherstellen, dass nationale Interoperabilitätsrahmen und -strategien an den EIF angeglichen sind, und diese im erforderlichen Umfang auf den Kontext und die spezifischen Bedürfnisse des betreffenden Mitgliedstaates hin zuschneiden und erweitern.*

Mit diesem Kriterium wird bewertet, ob die Spezifikationen in die nationalen Spezifikationskataloge der Mitgliedstaaten aufgenommen wurden, die einen hohen Entwicklungsstand in Bezug auf Interoperabilität aufweisen.

In den Factsheets zur digitalen öffentlichen Verwaltung wird der Entwicklungsstand der nationalen Interoperabilitätsrahmen gemessen am EIF anhand von drei Kategorien bewertet.

Die drei Kategorien sind:

1. konzeptionelles Modell für die erbringung integrierter öffentlicher Dienste;
2. Interoperabilitätsschichten
3. Interoperabilitätsgrundsätze.

Berichte über die nationalen Interoperabilitätsrahmen in 2024 finden Sie unter Digital Public Administration factsheets.

Wie wird geprüft?

Suche nach der Spezifikation im nationalen Katalog der Mitgliedstaaten. Für dieses Kriterium werden nur Mitgliedstaaten berücksichtigt, deren Interoperabilitätsrahmen laut NIFO-Factsheet angeglichen ist.

4.2. Zentrale Interoperabilitätsgrundsätze des EIF

Diese Kategorie umfasst Elemente im Zusammenhang mit den zentralen Interoperabilitätsgrundsätzen Offenheit (Grundsatz 2), Transparenz (Grundsatz 3), Weiterverwendbarkeit (Grundsatz 4), Technologieneutralität und Datenportabilität (Grundsatz 5).

4.2.1. EIF-A02: Ermöglicht die Spezifikation die Veröffentlichung von Daten im Internet?

EIF Empfehlung 2: *Veröffentlichen der in eigenem Besitz befindlichen Daten als offene Daten, sofern diese nicht gewissen Beschränkungen unterliegen.*

Bezieht sich darauf, ob es die Spezifikation ermöglicht, Daten als offene Daten zu veröffentlichen oder nicht.

Wie wird geprüft?

Der Nachweis dieses Kriteriums ergibt sich in der Regel aus der Funktion der Spezifikation oder einer konkreten Umsetzung der Spezifikation. Um das Kriterium zu erfüllen, muss die Spezifikation mindestens die erste Stufe des 5-Sterne-Modells von Tim Berners-Lee erreichen.

4.2.2. EIF-A03: Inwieweit können die Interessenträger zur Entwicklung der Spezifikation beitragen?

EIF Empfehlung 3: *Sorge für gleiche Wettbewerbsbedingungen für quelloffene Software und Nachweis einer aktiven und fairen Erwägung einer Nutzung quelloffener Software unter Berücksichtigung der Gesamtbetriebskosten der Lösung.*

Bezieht sich auf die Frage, inwieweit die verschiedenen Interessenträger, denen eine Spezifikation nutzen kann, an den Arbeitsgruppen teilnehmen können, die sich mit der Entwicklung bestimmter Spezifikationen befassen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums findet sich in der Regel auf der Website der Normungsorganisation (*Standards Developing Organisation*, SDO), die die Norm oder Spezifikation entwickelt hat. Die Normungsorganisation muss bestätigen, dass alle Interessenträger zur Entwicklung ihrer Lösungen beitragen können.

4.2.3. EIF-A04: Inwieweit ist eine öffentliche Überprüfung Teil des Versionszyklus?

EIF Empfehlung 3: *Sorge für gleiche Wettbewerbsbedingungen für quelloffene Software und Nachweis einer aktiven und fairen Erwägung einer Nutzung quelloffener Software unter Berücksichtigung der Gesamtbetriebskosten der Lösung.*

Für eine öffentliche Überprüfung muss der Entwurf der Spezifikation öffentlich zugänglich sein, damit die Interessenträger Beiträge zur Verbesserung und Behebung möglicher Fehler liefern können.

Wie wird geprüft?

Der Nachweis dieses Kriteriums findet sich in der Regel auf der Website der Normungsorganisation, die die Norm oder Spezifikation entwickelt hat und/oder diese pflegt. Die Normungsorganisation muss bestätigen, dass eine öffentliche Überprüfung Teil der Entwicklung und Genehmigung der Spezifikation ist.

4.2.4. EIF-A05: Inwieweit gelten Beschränkungen und Lizenzgebühren für die Verwendung der Spezifikation?

Weitere Informationen unter FRAND Licensing Terms

EIF Empfehlung 3: *Sorge für gleiche Wettbewerbsbedingungen für quelloffene Software und Nachweis einer aktiven und fairen Erwägung einer Nutzung quelloffener Software unter Berücksichtigung der Gesamtbetriebskosten der Lösung.*

Neben Open-Source-Software bezieht sich die EIF-Empfehlung auf eine Spezifikation an sich auf jeder Interoperabilitätsebene (rechtlich, organisatorisch, semantisch oder technisch).

Wie wird geprüft?

Der Nachweis dieses Kriteriums findet sich in der Regel auf der Website der Normungsorganisation, die die Norm oder Spezifikation entwickelt und/oder pflegt. FRAND ist im Sinne der Beschreibung in der Mitteilung der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss über den Umgang der EU mit standardessenziellen Patenten zu verstehen.

4.2.5. EIF-A06: Inwieweit ist die Spezifikation für ihre Verwendung bei der Entwicklung digitaler Lösungen/Dienste ausreichend ausgereift?

EIF Empfehlung 4: *Bevorzugen offener Spezifikationen bei angemessener Berücksichtigung der Erfüllung der funktionalen Anforderungen, der Ausgereiftheit, der Marktunterstützung und der Innovation.*

Reife in Bezug auf die Stabilität der Spezifikation bedeutet, dass sie einen ausreichenden Entwicklungsgrad erreicht hat und Mechanismen für ihre Weiterentwicklung vorhanden sind (Verfahren für das Änderungsmanagement, Überwachung usw.)

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, Umsetzungen der Spezifikation vorzuweisen oder Informationen über das Erstellungsdatum und die Aktualisierungen der Spezifikation bereitzustellen.

4.2.6. EIF-A07: Inwieweit hat die Spezifikation für ihre Verwendung bei der Entwicklung digitaler Lösungen/Dienste eine ausreichende Marktakzeptanz erreicht?

EIF Empfehlung 4: *Bevorzugen offener Spezifikationen bei angemessener Berücksichtigung der Erfüllung der funktionalen Anforderungen, der Ausgereiftheit, der Marktunterstützung und der Innovation.*

Reife in Bezug auf die Stabilität der Spezifikation bedeutet, dass sie einen ausreichenden Entwicklungsgrad erreicht hat und Mechanismen für ihre Weiterentwicklung vorhanden sind (Verfahren für das Änderungsmanagement, Überwachung usw.)

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, Umsetzungen der Spezifikation vorzuweisen oder Informationen über das Erstellungsdatum und die Aktualisierungen der Spezifikation bereitzustellen.

4.2.7. EIF-A08: Inwieweit wird die Spezifikation von mindestens einer Gemeinschaft unterstützt?

EIF Empfehlung 3: *Sorge für gleiche Wettbewerbsbedingungen für quelloffene Software und Nachweis einer aktiven und fairen Erwägung einer Nutzung quelloffener Software unter Berücksichtigung der Gesamtbetriebskosten der Lösung.*

Bezieht sich darauf, ob Gemeinschaften rund um die Spezifikation auf rechtlicher, organisatorischer, semantischer oder technischer Ebene zu ihrer Verbesserung und Entwicklung beitragen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu prüfen, ob eine Entwicklergemeinschaft Arbeiten oder Entwicklungen in Bezug auf die Norm oder Spezifikation durchgeführt hat.

4.2.8. EIF-A09: Inwieweit ermöglicht die Spezifikation die Sichtbarkeit von Abläufen, Bestimmungen, Daten und Dienstleistungen der Verwaltung?

EIF Empfehlung 5: *Sorge für interne Sichtbarkeit und Bereitstellung externer Schnittstellen für europäische öffentliche Dienste.*

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, Umsetzungsbeispiele oder Pläne für die Aufnahme der Norm oder Spezifikation in einen Verwaltungsprozess vorzuweisen. Ein gängiger Anwendungsfall ist die Digitalisierung öffentlicher Dienste.

4.2.9. EIF-A10: Inwieweit geht die Spezifikation nachvollziehbar auf Abläufe, Bestimmungen, Daten und Dienstleistungen der Verwaltung ein?

EIF Empfehlung 5: *Sorge für interne Sichtbarkeit und Bereitstellung externer Schnittstellen für europäische öffentliche Dienste.*

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, Umsetzungen oder Pläne für die Aufnahme der Norm oder Spezifikation in einen Verwaltungsprozess vorzuweisen. Ein gängiger Anwendungsfall ist die Digitalisierung öffentlicher Dienste.

4.2.10. EIF-A11: Inwieweit ermöglicht die Spezifikation Schnittstellen für den Zugang zu Dienstleistungen der Verwaltung?

EIF Empfehlung 5: *Sorge für interne Sichtbarkeit und Bereitstellung externer Schnittstellen für europäische öffentliche Dienste.*

Bezieht sich darauf, dass die Verfügbarkeit von Schnittstellen zu internen Informationssystemen sichergestellt werden soll. Dies wird in der EIF-Umsetzungsstrategie wie folgt beschrieben: *Öffentliche Verwaltungen betreiben zur Abwicklung ihrer internen Abläufe oftmals eine Vielzahl an verschiedenartigen Informationssystemen. Für Interoperabilität muss sichergestellt sein, dass zu diesen Systemen und den von diesen verarbeiteten Daten Schnittstellen zur Verfügung stehen. Im Gegenzug erleichtert Interoperabilität die Weiterverwendung von Systemen und Daten und ermöglicht deren Integration in größere Systeme.*

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, Dienste vorzuweisen, die die Spezifikation umgesetzt haben, um Informationen effizienter auszutauschen und zu nutzen und Interoperabilitätshürden zu überwinden.

4.2.11. EIF-A12: Inwieweit kann die Spezifikation auch in einem anderen als dem ursprünglich angedachten Kontext verwendet, d. h. bereichsübergreifend genutzt und umgesetzt werden?

EIF Empfehlung 6: *Mit- und Weiterverwenden bestehender Lösungen sowie Zusammenarbeit bei der Entwicklung gemeinsamer Lösungen bei der Einführung europäischer öffentlicher Dienste.*

Bezieht sich auf die Verwendung der Spezifikation über einen bestimmten Bereich hinaus. Beispiel: Eine im Bereich der elektronischen Gesundheitsdienste (eHealth) entwickelte Spezifikation, die in anderen Bereichen verwendet werden kann.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, Beispiele für die Verwendung der Norm oder der technischen Spezifikationen in anderen Bereichen als dem Bereich vorzulegen, für den sie ursprünglich entwickelt wurde. So beschreibt beispielsweise die DCAT-AP-Spezifikation, die für

einen bestimmten Zweck und Bereich entwickelt wurde, Datensätze des öffentlichen Sektors für Open-Data-Portale. Sie wurde neben europäischen Datenportalen jedoch auch häufig für die Erstellung anderer Spezifikationen und Lösungen weiterverwendet.

4.2.12. EIF-A13: Ist die Spezifikation technologieunabhängig?

EIF Empfehlung 8: *Bürgern und Unternehmen und anderen Verwaltungseinrichtungen sollten keine technischen Lösungen aufgezwungen werden, die eine bestimmte Technik vorschreiben oder in keinem Verhältnis zu ihren tatsächlichen Bedürfnissen stehen.*

Technologieneutralität bedeutet, dass keine Abhängigkeit von anderen („verwandten“) Spezifikationen besteht; Plattformneutralität bedeutet, dass keine Abhängigkeit von einer bestimmten Umgebung, einer bestimmten Internetplattform oder einem bestimmten Betriebssystem besteht.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu prüfen, dass die Umsetzung der Norm oder Spezifikation nicht von einer anderen Norm oder Spezifikation abhängt, insbesondere von proprietären Technologien oder Anbietern. Es sollte jedoch geprüft werden, ob die Spezifikation von anderen Spezifikationen abhängt, auch wenn diese quelloffen sind. Dies bedeutet, dass die Spezifikation andere Spezifikationen/Plattformen erfordert, um zu funktionieren.

4.2.13. EIF-A14: Ist die Spezifikation plattformunabhängig?

EIF Empfehlung 8: *Bürgern und Unternehmen und anderen Verwaltungseinrichtungen sollten keine technischen Lösungen aufgezwungen werden, die eine bestimmte Technik vorschreiben oder in keinem Verhältnis zu ihren tatsächlichen Bedürfnissen stehen.*

Technologieneutralität bedeutet, dass keine Abhängigkeit von anderen („verwandten“) Spezifikationen besteht; Plattformneutralität bedeutet, dass keine Abhängigkeit von einer bestimmten Umgebung, einer bestimmten Internetplattform oder einem bestimmten Betriebssystem besteht.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu prüfen, dass die Umsetzung der Norm oder Spezifikation nicht von einer anderen Norm oder Spezifikation abhängt, insbesondere von proprietären Technologien oder Anbietern. Es sollte jedoch geprüft werden, ob die Spezifikation von anderen Spezifikationen abhängt, auch wenn diese quelloffen sind. Dies bedeutet, dass die Spezifikation andere Spezifikationen/Plattformen erfordert, um zu funktionieren.

4.2.14. EIF-A15: Inwieweit erlaubt die Spezifikation Teilumsetzungen?

EIF Empfehlung 8: *Bürgern und Unternehmen und anderen Verwaltungseinrichtungen sollten keine technischen Lösungen aufgezwungen werden, die eine bestimmte Technik vorschreiben oder in keinem Verhältnis zu ihren tatsächlichen Bedürfnissen stehen.*

Teilumsetzungen beziehen sich auf die Anwendung von Spezifikationen, nicht in ihrer Gesamtheit, sondern eines Teils der in der Dokumentation festgelegten Anforderungen oder Merkmale.

Darunter kann auch eine Umsetzung unterschiedlicher Profile verstanden werden, die sich je nach Kontext der Umsetzung auch auf bestimmte Anforderungen bezieht.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu prüfen, ob die Dokumentation der Spezifikation Überlegungen zu Teilumsetzungen enthält.

4.2.15. EIF-A16: Kann die Spezifikation angepasst werden?

EIF Empfehlung 8: *Bürgern und Unternehmen und anderen Verwaltungseinrichtungen sollten keine technischen Lösungen aufgezwungen werden, die eine bestimmte Technik vorschreiben oder in keinem Verhältnis zu ihren tatsächlichen Bedürfnissen stehen.*

Ein gutes Beispiel für Anpassungen sind die *Core Vocabularies*, in denen eine Reihe allgemeiner Anforderungen festgelegt sind, die in jedem Kontext passen könnten und bei der Umsetzung eine Anpassung an bereichsspezifische Anforderungen ermöglichen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu prüfen, ob die Dokumentation der Spezifikation Teilumsetzungen unterstützt.

4.2.16. EIF-A17: Kann die Spezifikation erweitert werden?

EIF Empfehlung 8: *Bürgern und Unternehmen und anderen Verwaltungseinrichtungen sollten keine technischen Lösungen aufgezwungen werden, die eine bestimmte Technik vorschreiben oder in keinem Verhältnis zu ihren tatsächlichen Bedürfnissen stehen.*

Ein gutes Beispiel für Erweiterungen sind die *Core Vocabularies*, bei denen es sich um eine Reihe allgemeiner Anforderungen handelt, die in unterschiedlichen Kontexten passen und sich in einer Art Erweiterungsverfahren ergänzen können, um bei jeder Umsetzung bereichsspezifische Anforderungen zu erfüllen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu prüfen, ob die Dokumentation der Spezifikation die Erweiterung der Spezifikation ermöglicht.

4.2.17. EIF-A18: Inwieweit ermöglicht die Spezifikation die Datenportabilität zwischen Systemen/Anwendungen, um die Umsetzung oder Weiterentwicklung europäischer öffentlicher Dienste unterstützen?

EIF Empfehlung 9: *Sorge für die Datenportabilität, insbesondere damit Daten sich mühelos zwischen Systemen und Anwendungen, auf denen die Einführung und Weiterentwicklung europäischer öffentlicher Dienste beruht, ohne ungerechtfertigte Einschränkungen übertragen lassen, insoweit dies rechtlich zulässig ist.*

Wie wird geprüft?

Der Nachweis dieses Kriteriums bestehen in der Regel in einer Dokumentation der Merkmale der Spezifikation, die belegt, dass sie sich positiv auf die Interoperabilität auswirkt.

4.3. EIF Grundsätze mit Bezug auf allgemeine nutzerseitige Bedürfnisse und Erwartungen

Diese Kategorie umfasst alle EIF-Grundsätze, die mit den Nutzerbedürfnissen zusammenhängen. Hierzu zählen die Grundsätze Nutzerorientierung (Grundsatz 6), Inklusion und Barrierefreiheit (Grundsatz 7), Sicherheit und Privatsphäre (Grundsatz 8) und Mehrsprachigkeit (Grundsatz 9).

4.3.1. EIF-A19: Inwieweit erlaubt die Spezifikation, relevante Informationen bei Bedarf weiterzuverwenden?

EIF Empfehlung 13: *Soweit nach geltender Rechtslage möglich, sollten von den Nutzern europäischer öffentlicher Dienste lediglich die zwingend benötigten Angaben und diese nur einmal verlangt werden.*

Der Grundsatz der einmaligen Erfassung soll Vorgänge oder Transaktionen zwischen Verwaltungen und Interessenträgern effizienter machen. Dies bedeutet, dass bestimmte Daten oder Informationen nicht doppelt oder mehrfach bereitgestellt werden müssen, wenn sie öffentlichen Verwaltungen bereits vorliegen.

Der erste europäische Datenraum: das Once-Only Technical System (OOTS).

Wie wird geprüft?

Dieses Kriterium ist im Zusammenhang mit europäischen Lösungen zu verstehen, die zur Umsetzung des Grundsatzes der einmaligen Erfassung (*Once-Only Principle*, OOP) beitragen (d. h. CEF, *Connecting Europe Facility*). Aus diesem Grund besteht der Nachweis dieses Kriteriums in der Regel aus Umsetzungen oder Erwähnungen der Spezifikation in diesen Lösungen.

4.3.2. EIF-A20: Inwieweit ermöglicht die Spezifikation einen barrierefreien Zugang?

Ein Beispiel für eine solche Spezifikation sind die Web Content Accessibility Guidelines (WCAG)

EIF Empfehlung 14: *Sorge dafür, dass alle europäischen öffentlichen Dienste allen Bürgern zur Verfügung stehen, auch solchen mit Behinderungen, älteren Menschen und sonstigen benachteiligten Gruppen. Bei digitalen öffentlichen Diensten sollten öffentliche Verwaltungen den auf europäischer und internationaler Ebene weithin anerkannten Spezifikationen für einen barrierefreien Zugang entsprechen.*

Ein Beispiel einer Spezifikation für den barrierefreien Zugang ist WAI-ARIA, enthalten in der Übersicht zu den Web Content Accessibility Guidelines (WCAG).

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in Dokumentation, die belegt, dass die Norm oder Spezifikation einen barrierefreien Zugang fördert. Darüber hinaus kann das Kriterium erfüllt werden, wenn die Spezifikation an einer Stelle auf Barrierefreiheit eingeht. Die Spezifikation soll die Schaffung digitaler Dienste fördern, die allen Bürgern zur Verfügung stehen, auch solchen mit Behinderung, älteren Menschen und sonstigen benachteiligten Gruppen.

4.3.3. EIF-A21: Inwieweit gewährleistet die Spezifikation den Schutz personenbezogener Daten, die von öffentlichen Verwaltungen verarbeitet werden?

EIF Empfehlung 15: *Festlegen eines gemeinsamen Rahmens für Sicherheit und Datenschutz und Festlegen von Verfahren, nach denen öffentliche Dienste einen gesicherten und vertrauenswürdigen Datenaustausch zwischen öffentlichen Verwaltungen und bei Interaktionen mit Bürgern und Unternehmen gewährleisten.*

Bezieht sich auf die Maßnahmen der öffentlichen Verwaltungen in Bezug auf sensible Informationen für die ordnungsgemäße Erbringung öffentlicher Dienste. Die verschiedenen Maßnahmen umfassen den Empfang, die Einstufung und den Austausch solcher Informationen.

Sicherung des Rechts auf Schutz personenbezogener Daten durch die Einhaltung des geltenden rechtlichen Rahmens für die großen Mengen an personenbezogenen Daten von Bürgern, die sich im Besitz öffentlicher Verwaltungen befinden und von diesen verwaltet werden.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in der Unterstützung der Datenverwaltung gemäß den Datenschutzrichtlinien.

4.3.4. EIF-A22: Sieht die Spezifikation Mittel zur Beschränkung des Zugangs zu Informationen/Daten vor?

EIF Empfehlung 15: *Festlegen eines gemeinsamen Rahmens für Sicherheit und Datenschutz und Festlegen von Verfahren, nach denen öffentliche Dienste einen gesicherten und vertrauenswürdigen Datenaustausch zwischen öffentlichen Verwaltungen und bei Interaktionen mit Bürgern und Unternehmen gewährleisten.*

Der Grundsatz der Vertraulichkeit besagt, dass nur der Absender und der (die) vorgesehene(n) Empfänger den Inhalt einer Nachricht erstellen können dürfen. Die Vertraulichkeit ist beeinträchtigt, wenn eine unbefugte Person in der Lage ist, eine Nachricht zu erstellen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu belegen, dass die Spezifikation einige Bestimmungen für die Beschränkung des Zugangs zu Informationen/Daten enthält. Darüber hinaus sollten auch Fälle berücksichtigt werden, in denen Erweiterungen der Spezifikation oder die Spezifikation selbst mittels einer anderen Spezifikation eine korrekte Datenverarbeitung ermöglichen.

4.3.5. EIF-A23: Ist die Spezifikation Teil eines europäischen oder nationalen Vorhabens zu Datenschutzaspekten?

EIF Empfehlung 15: *Festlegen eines gemeinsamen Rahmens für Sicherheit und Datenschutz und Festlegen von Verfahren, nach denen öffentliche Dienste einen gesicherten und vertrauenswürdigen Datenaustausch zwischen öffentlichen Verwaltungen und bei Interaktionen mit Bürgern und Unternehmen gewährleisten.*

Sicherung des Rechts auf Schutz personenbezogener Daten durch die Einhaltung des geltenden rechtlichen Rahmens für die großen Mengen an personenbezogenen Daten von Bürgern, die sich im Besitz öffentlicher Verwaltungen befinden und von diesen verwaltet werden.

Bezieht sich auf die Maßnahmen der öffentlichen Verwaltungen in Bezug auf sensible Informationen für die ordnungsgemäße Erbringung öffentlicher Dienste. Die verschiedenen Maßnahmen umfassen den Empfang, die Einstufung und den Austausch solcher Informationen.

Beispielsweise sind die Spezifikationen des Europäischen Instituts für Telekommunikationsnormen (ETSI) zu elektronischen Signaturen und Infrastrukturen (ESI) Teil der Vertrauensbildung der eDelivery-Lösung, weil damit sichergestellt wird, dass bei der Umsetzung der Lösung Sicherheit und Privatsphäre gewährleistet sind.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin festzustellen, ob die Spezifikation als Grundlage für die Konzeption und Umsetzung eines Vorhabens (nach Möglichkeit eines digitalen öffentlichen Dienstes) verwendet oder bereits in einem Vorhaben verwendet wird.

4.4. Datenaustausch und -verarbeitung

4.4.1. EIF-A24: Inwieweit ermöglicht die Spezifikation einen sicheren Datenaustausch?

EIF Empfehlung 15: *Festlegen eines gemeinsamen Rahmens für Sicherheit und Datenschutz und Festlegen von Verfahren, nach denen öffentliche Dienste einen gesicherten und vertrauenswürdigen Datenaustausch zwischen öffentlichen Verwaltungen und bei Interaktionen mit Bürgern und Unternehmen gewährleisten.*

Dies bezieht sich auf die Maßnahmen der öffentlichen Verwaltungen in Bezug auf sensible Informationen für die ordnungsgemäße Erbringung öffentlicher Dienste. Die verschiedenen Maßnahmen umfassen den Empfang, die Einstufung und den Austausch solcher Informationen.

Wie wird geprüft?

Für den Nachweis dieses Kriteriums kann Datenaustausch verstanden werden als die Veröffentlichung von Daten durch die Verwaltung, damit sie später von Bürgern genutzt werden können. Die Spezifikation muss sicherstellen, dass der Datenaustausch vollständig sicher ist und dass die Daten nicht verändert wurden.

4.4.2. EIF-A25: Inwieweit ermöglicht die Spezifikation eine sichere Datenverarbeitung?

EIF Empfehlung 15: *Festlegen eines gemeinsamen Rahmens für Sicherheit und Datenschutz und Festlegen von Verfahren, nach denen öffentliche Dienste einen gesicherten und vertrauenswürdigen Datenaustausch zwischen öffentlichen Verwaltungen und bei Interaktionen mit Bürgern und Unternehmen gewährleisten.*

Bezieht sich auf die Maßnahmen der öffentlichen Verwaltungen in Bezug auf sensible Informationen für die ordnungsgemäße Erbringung öffentlicher Dienste. Die verschiedenen Maßnahmen umfassen den Empfang, die Einstufung und den Austausch solcher Informationen.

Verarbeitung umfasst ein breites Spektrum von Vorgängen im Zusammenhang mit personenbezogenen Daten, einschließlich manueller oder automatisierter Verfahren. Dazu gehören das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten oder eine andere Form der Bereitstellung, das Abgleichen oder Verknüpfen sowie das Einschränken, Löschen oder Vernichten von personenbezogenen Daten.

Wie wird geprüft?

Für den Nachweis dieses Kriteriums kann Datenaustausch verstanden werden als die Veröffentlichung von Daten durch die Verwaltung, damit sie später von Bürgern genutzt werden können. Die Spezifikation muss gewährleisten, dass die Datenverarbeitung vollständig sicher ist und dass die Daten nicht verändert wurden.

4.4.3. EIF-A26: Inwieweit gewährleistet die Spezifikation die Authentizität und Authentifizierung der an einem Datenaustausch beteiligten Akteure?

EIF Empfehlung 15: *Festlegen eines gemeinsamen Rahmens für Sicherheit und Datenschutz und Festlegen von Verfahren, nach denen öffentliche Dienste einen gesicherten und vertrauenswürdigen Datenaustausch zwischen öffentlichen Verwaltungen und bei Interaktionen mit Bürgern und Unternehmen gewährleisten.*

Authentifizierung bedeutet, dass die Nutzer diejenigen sind, die sie behaupten zu sein. Verfügbarkeit bedeutet, dass Ressourcen für berechtigte Nutzer verfügbar sind; „Denial of Service“-Angriffe, von denen zuweilen in nationalen Nachrichten berichtet wird, sind Angriffe auf die Verfügbarkeit. Experten für Informationssicherheit befassen sich mit Zugriffskontrolle und Nichtabstreitbarkeit. Autorisierung bedeutet die Möglichkeit, zwischen berechtigten und unberechtigten Nutzern zu unterscheiden sowie den Grad der Berechtigung festzulegen. Authentizität bedeutet die ständige Kontrolle am System, um sicherzustellen, dass sensible Orte geschützt sind und einwandfrei funktionieren.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, dass die Dokumentation zur Spezifikation die Authentizität und Authentifizierung der an einem Datenaustausch beteiligten Akteure belegt. Darüber hinaus sollten auch Fälle berücksichtigt werden, in denen Erweiterungen der Spezifikation oder die Spezifikation selbst mittels einer anderen Spezifikation eine korrekte Datenverarbeitung ermöglichen.

4.4.4. EIF-A27: Inwieweit werden Informationen vor unbefugten Änderungen geschützt?

EIF Empfehlung 15: *Festlegen eines gemeinsamen Rahmens für Sicherheit und Datenschutz und Festlegen von Verfahren, nach denen öffentliche Dienste einen gesicherten und vertrauenswürdigen Datenaustausch zwischen öffentlichen Verwaltungen und bei Interaktionen mit Bürgern und Unternehmen gewährleisten.*

Integrität bedeutet, dass Informationen vor unbefugten Änderungen geschützt sind, die für berechtigte Nutzer nicht wahrnehmbar wären; einige Hacking-Angriffe gefährden die Integrität von Datenbanken und verschiedenen anderen Ressourcen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, dass die Dokumentation zur Spezifikation Verfahren zur Sicherstellung der Integrität belegt. Darüber hinaus sollten auch Fälle berücksichtigt werden, in denen Erweiterungen der Spezifikation oder die Spezifikation selbst mittels einer anderen Spezifikation eine korrekte Datenverarbeitung ermöglichen.

4.4.5. EIF-A28: Inwieweit gewährleistet und ermöglicht die Spezifikation eine korrekte Datenverarbeitung?

EIF Empfehlung 15: *Festlegen eines gemeinsamen Rahmens für Sicherheit und Datenschutz und Festlegen von Verfahren, nach denen öffentliche Dienste einen gesicherten und vertrauenswürdigen Datenaustausch zwischen öffentlichen Verwaltungen und bei Interaktionen mit Bürgern und Unternehmen gewährleisten.*

Die Genauigkeit und Vollständigkeit der Informationssysteme und der in diesen Systemen enthaltenen Daten sollte ein Anliegen der Verwaltung sein. Ein unbefugtes Ändern oder Löschen von Daten (durch Externe oder Beschäftigte) kann sich auf die Organisation auswirken. Jede Organisation sollte Kontrollen durchführen, um sicherzustellen, dass die in ihre automatisierten Dateien und Datenbanken eingegebenen und dort gespeicherten Daten vollständig und korrekt sind und dass die Genauigkeit der verbreiteten Daten gewährleistet ist.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in Dokumentation, die belegt, dass die Spezifikation Datenverarbeitung ermöglicht. Darüber hinaus sollten auch Fälle berücksichtigt werden, in denen Erweiterungen der Spezifikation oder die Spezifikation selbst mittels einer anderen Spezifikation eine korrekte Datenverarbeitung ermöglichen.

4.4.6. EIF-A29: Inwieweit ist in der Spezifikation ein Verfahren zur Zugriffskontrolle vorgesehen?

EIF Empfehlung 15: *Festlegen eines gemeinsamen Rahmens für Sicherheit und Datenschutz und Festlegen von Verfahren, nach denen öffentliche Dienste einen gesicherten und vertrauenswürdigen Datenaustausch zwischen öffentlichen Verwaltungen und bei Interaktionen mit Bürgern und Unternehmen gewährleisten.*

Mit der Zugriffskontrolle wird bestimmt, wer worauf Zugriff haben muss. Beispielsweise muss festgelegt werden können, dass Nutzer A die Daten in einer Datenbank einsehen, sie aber nicht neu laden darf. Nutzer A könnte auch die Berechtigung für Aktualisierungen erhalten. Dafür kann ein Verfahren zur Zugangskontrolle eingerichtet werden. Die Zugriffskontrolle ist in zwei Bereiche untergliedert: Rollenverwaltung und Rechteverwaltung. Die Rollenverwaltung betrifft die Nutzer, die Rechteverwaltung die Ressourcen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in der Dokumentation eines in der Spezifikation vorgesehenen Verfahrens oder einer Erweiterung, um die Zugriffskontrolle zu gewährleisten. Darüber hinaus können auch Spezifikationen genannt werden, die in Verbindung mit der zu bewertenden Spezifikation verwendet werden können, um Verfahren zur Zugriffskontrolle bereitzustellen.

4.4.7. EIF-A30: Inwieweit könnte die Spezifikation in einem mehrsprachigen Kontext verwendet werden?

EIF Empfehlung 16: *Verwenden von Informationssystemen und technischen Architekturen, die Mehrsprachigkeit beim Aufbau europäischer öffentlicher Dienste zulassen. Entscheiden über den Grad an Unterstützung von Mehrsprachigkeit auf Grundlage der Bedürfnisse der voraussichtlichen Nutzer.*

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in Dokumentation, die belegt, dass die Norm oder Spezifikation die mehrsprachige öffentliche Dienste fördert. Darüber hinaus kann die Spezifikation einen Beitrag zum europäischen öffentlichen Dienst leisten, indem sie eine Entwicklung in verschiedenen Sprachen ermöglicht, z. B. kann HTML so konfiguriert werden, dass eine Website in vielen Sprachen bereitgestellt wird.

4.5. EIF Grundsätze für die Zusammenarbeit zwischen öffentlichen Verwaltungen

Diese Kategorie umfasst die Kriterien zur Bewertung der Grundsätze der Zusammenarbeit zwischen öffentlichen Einrichtungen, Unternehmen und Bürgern. Dazu zählen die Grundsätze der Verwaltungsvereinfachung (Grundsatz 10), der Informationsbewahrung (Grundsatz 11) und der Bewertung von Effektivität und Effizienz (Grundsatz 12).

4.5.1. EIF-A31: Erleichtert die Spezifikation die Erbringung europäischer öffentlicher Dienste?

EIF Empfehlung 17: *Vereinfachen von Prozessen und Nutzen digitaler Kanäle für die Bereitstellung europäischer öffentlicher Dienste im gebotenen Umfang, um unverzüglich und in hochwertiger Form auf Anfragen von Nutzern zu reagieren und den Verwaltungsaufwand für die öffentlichen Verwaltungen, Unternehmen und Bürger zu vermindern.*

Dieses Kriterium würde jede Spezifikation erfüllen, die die Digitalisierung erleichtert und die Verwaltung vereinfacht, indem z. B. einem Identifizierungsdienst Zugang zu einem digitalen Bestand mit Bürgerinformationen ermöglicht wird.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in Dokumentation, die belegt, dass die Norm oder Spezifikation Verwaltungsprozesse strafft. Spezifikationen zur Erleichterung und Förderung des digitalen Austauschs bei gleichzeitiger Vermeidung des analogen Informationsaustauschs können als Beitrag zur Verringerung des Verwaltungsaufwands betrachtet werden. So fördert beispielsweise die Nutzung von HTML im Rahmen des Informationsaustauschs die Schaffung digitaler Dienste, die den digitalen Austausch und die digitale Nutzung von Daten ermöglichen, während gleichzeitig analoge Prozesse vermieden werden.

4.5.2. EIF-A32: Ermöglicht die Spezifikation Kanäle für die Erbringung digitaler Dienste?

EIF Empfehlung 17: *Vereinfachen von Prozessen und Nutzen digitaler Kanäle für die Bereitstellung europäischer öffentlicher Dienste im gebotenen Umfang, um unverzüglich und in hochwertiger Form auf Anfragen von Nutzern zu reagieren und den Verwaltungsaufwand für die öffentlichen Verwaltungen, Unternehmen und Bürger zu vermindern.*

Dieses Kriterium wäre unter anderem erfüllt, wenn eine Spezifikation die Erbringung öffentlicher Dienste erleichtert oder bessere Mittel bietet, um die Digitalisierung und Verwaltungsvereinfachung zu fördern. Zum Beispiel wäre das eine Spezifikation, die sich unmittelbar auf die API-Leistung bezieht, um die Erbringung eines digitalen öffentlichen Dienstes über eine API zu erleichtern und zu verbessern.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in Dokumentation, die belegt, dass die Norm oder Spezifikation Verwaltungsprozesse strafft. Spezifikationen zur Erleichterung und Förderung des digitalen Austauschs bei gleichzeitiger Vermeidung des analogen Informationsaustauschs können als Beitrag zur Verringerung des Verwaltungsaufwands betrachtet werden. So fördert beispielsweise die Nutzung von HTML im Rahmen des Informationsaustauschs die Schaffung digitaler Dienste, die den digitalen Austausch und die digitale Nutzung von Daten ermöglichen, während gleichzeitig analoge Prozesse vermieden werden.

4.5.3. EIF-A33: Inwieweit ermöglicht die Spezifikation die langfristige Bewahrung von Daten/Informationen/Wissen (einschließlich elektronischer Aufzeichnungen)?

EIF Empfehlung 18: *Formulieren einer langfristigen Bewahrungspolitik für Informationen in Bezug auf europäische öffentliche Dienste und insbesondere für Informationen, die grenzüberschreitend ausgetauscht werden.*

Bezieht sich auf die Fähigkeit der Spezifikation, zur langfristigen Bewahrung von Informationen beizutragen.

Wie wird geprüft?

Als Nachweis dieses Kriteriums muss in der Dokumentation der Spezifikation der Schwerpunkt auf die langfristige Bewahrung von Informationen gelegt und diese sichergestellt werden.

4.5.4. EIF-A34: Inwieweit werden Bewertungen der Effektivität der Spezifikation vorgenommen?

EIF Empfehlung 19: *Bewerten der Effektivität und Effizienz unterschiedlicher Interoperabilitätslösungen und technischer Optionen unter Berücksichtigung der Nutzerbedürfnisse, der Verhältnismäßigkeit und des Kosten-Nutzen-Verhältnisses.*

Bezieht sich auf das Maß, in dem die Spezifikation bei ihrer Verwendung effektiv ist. Es gibt indirekte Methoden, mit denen festgestellt werden kann, dass die Spezifikation effektiv ist, z. B. wenn eine Lösung effektiv ist und für den gewünschten Dienst die Spezifikation nutzt.

Effektivität: Das Maß, in dem die Spezifikationen das Ziel erreichen, die angestrebte Maßnahme ihrem Zweck entsprechend umzusetzen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in bereits durchgeführten Bewertungen der Norm oder technischen Spezifikation unter Berücksichtigung ihrer Effektivität. Dies können Studien sein, in denen die Effektivität mit anderen Spezifikationen verglichen wird. Ein Beispiel für Studien oder Dokumentation könnten Artikel in Forschungsjournalen (z. B. auf Researchgate) oder Beiträge in Fachforen sein.

4.5.5. EIF-A35: Inwieweit werden Bewertungen der Effizienz der Spezifikation vorgenommen?

EIF Empfehlung 19: *Bewerten der Effektivität und Effizienz unterschiedlicher Interoperabilitätslösungen und technischer Optionen unter Berücksichtigung der Nutzerbedürfnisse, der Verhältnismäßigkeit und des Kosten-Nutzen-Verhältnisses.*

Bezieht sich auf die sinnvolle Nutzung von Zeit und Ressourcen, die durch die Verwendung einer Spezifikation nicht unnötig verschwendet werden. Es gibt indirekte Methoden, mit denen festgestellt werden kann, dass die Spezifikation effizient ist, z. B. wenn eine Lösung für einen Dienst die Spezifikation nutzt und effizient ist.

Effizienz: Zeit und Mittel, die erforderlich sind, um die Ergebnisse unter Verwendung der Spezifikation zu erzielen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in bereits durchgeführten Bewertungen der Norm oder technischen Spezifikation unter Berücksichtigung ihrer Effizienz. Dies können Studien sein, in denen die Effizienz mit anderen Spezifikationen verglichen wird. Ein Beispiel für Studien oder

Dokumentation könnten Artikel in Forschungsjournalen (z. B. auf Researchgate) oder Beiträge in Fachforen sein.

4.6. EIF Interoperabilitätsschichten

Diese Kategorie steht im Einklang mit den entsprechenden Interoperabilitätsmodellen, die im EIF beschrieben werden und für alle öffentlichen Dienste gelten. Sie umfasst sechs Schichten: Interoperabilitätsgovernance, Governance integrierter öffentlicher Dienste, rechtliche Interoperabilität, organisatorische Interoperabilität, semantische Interoperabilität und technische Interoperabilität, die unter die Kriterien A2 bis A10 in der Kategorie „Offenheit“ fallen.

4.6.1. EIF-A36: Nimmt die Spezifikation Bezug auf die Europäische Interoperabilitäts-Referenzarchitektur (EIRA) oder wäre dies möglich?

EIF Empfehlung 20: *Sorge für eine verwaltungsebenen- und sektorübergreifende ganzheitliche Governance von Interoperabilitätsmaßnahmen.*

Die EIRA definiert die zur Förderung der Interoperabilität erforderlichen Fähigkeiten als eine Reihe von Architekturbausteinen. Ein Bezug der Spezifikationen zu diesen Bausteinen bedeutet die Fähigkeit, rechtliche, organisatorische, semantische oder technische Aspekte zu ermöglichen, die für die Entwicklung interoperabler öffentlicher Dienste erforderlich sind. Dieser Bezug kann der EIRA-Bibliothek für Interoperabilitätsspezifikationen (*EIRA Library of Interoperability Specifications*, ELIS) entnommen, aber auch ad hoc hergestellt werden.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, einen möglichen Bezug der Norm oder Spezifikation zu einem EIRA-Architekturbaustein (*Architecture Building Block*, ABB) zu erläutern.

4.6.2. EIF-A37: Inwieweit kann bewertet werden, ob die Umsetzungen der Spezifikation die Vorgaben einhalten?

EIF Empfehlung 21: *Einrichten von Prozessen für die Auswahl der maßgeblichen Normen und Spezifikationen, ihre Bewertung, die Überwachung ihrer Umsetzung, die Kontrolle der Einhaltung und die Überprüfung ihrer Interoperabilität.*

Bezieht sich darauf, dass die Umsetzung der Spezifikation den in der Spezifikation festgelegten Anforderungen entspricht. Es gibt unterschiedliche Methoden, um sicherzustellen, dass eine Umsetzung die Anforderungen einer Spezifikation einhält: manuell prüfen, ob die Umsetzung den Anforderungen der Spezifikation (falls vorhanden) entspricht, zusätzliche für diesen Zweck vorhandene Methoden oder Ressourcen verwenden oder spezifische Instrumente der Normungsorganisation verwenden, die die Spezifikation entwickelt.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel aus kostenlosen Prüfinstrumenten oder Zertifizierungen, mit denen die Norm oder Spezifikation bewertet wird.

4.6.3. EIF-A38: Wird die Spezifikation von einem europäischen Mitgliedstaat empfohlen?

EIF Empfehlung 23: *Heranziehen der maßgeblichen Kataloge für Normen, Spezifikationen und Leitlinien auf einzelstaatlicher und auf EU-Ebene im Einklang mit dem NIF und den betreffenden DIF bei der Beschaffung und Entwicklung von IKT-Lösungen.*

Empfohlene Spezifikationen sind diejenigen Spezifikationen, die die Mitgliedstaaten als Beispiele für die Einführung bestimmter digitaler öffentlicher Dienste oder für deren Nutzung bei der Beschaffung dieser digitalen öffentlichen Dienste oder Lösungen nennen.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in einer Empfehlung eines Mitgliedstaats einer Umsetzung der Norm oder Spezifikation. Diese Empfehlung kann von der Verwaltung des Mitgliedstaats oder von der für die Normung in dem betreffenden Mitgliedstaat zuständigen Stelle stammen (z. B. Difi in Norwegen mit folgender Bewertung von Normen und Spezifikationen für den sicheren Datenaustausch unter Standarder for sikker informasjonsutveksling på Internett oder dieser Katalog empfohlener Spezifikationen:Arkivstandarder).

4.6.4. EIF-A39: Ist die Spezifikation für ein grenzüberschreitendes europäisches Projekt/eine grenzüberschreitende europäische Initiative ausgewählt worden?

EIF Empfehlung 23: *Heranziehen der maßgeblichen Kataloge für Normen, Spezifikationen und Leitlinien auf einzelstaatlicher und auf EU-Ebene im Einklang mit dem NIF und den betreffenden DIF bei der Beschaffung und Entwicklung von IKT-Lösungen.*

Die Europäische Kommission hat ein Verfahren zur Ermittlung und Bewertung von Spezifikationen für die Entwicklung bzw. Beschaffung von IT-Lösungen eingerichtet. Die Durchführungsbeschlüsse mit den von der Europäischen Kommission ermittelten Spezifikationen können abgerufen werden unter ICT technical specifications.

Es ist jedoch auch möglich, dass eine Spezifikation außerhalb des oben genannten Kontextes für europäische Projekte oder Initiativen ausgewählt wird. Diese Spezifikationen können positiv bewertet werden.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in der Dokumentation einer Umsetzung der Norm oder Spezifikation im Zusammenhang mit einem grenzüberschreitenden Projekt oder einer grenzüberschreitenden Initiative (siehe z. B. CEF Digital, CEF-Bausteine, TESTA usw.).

4.6.5. EIF-A40: Ist die Spezifikation in einem offenen nationalen Normenverzeichnis/-katalog enthalten?

EIF Empfehlung 23: *Heranziehen der maßgeblichen Kataloge für Normen, Spezifikationen und Leitlinien auf einzelstaatlicher und auf EU-Ebene im Einklang mit dem NIF und den betreffenden DIF bei der Beschaffung und Entwicklung von IKT-Lösungen.*

EIF Empfehlung 6: *Mit- und Weiterverwenden bestehender Lösungen sowie Zusammenarbeit bei der Entwicklung gemeinsamer Lösungen bei der Einführung europäischer öffentlicher Dienste.*

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, dass die Norm oder Spezifikation in einen nationalen Normenkatalog aufgenommen wurde. Dies kann in der CAMSS-Normenliste überprüft werden:

4.6.6. EIF-A41: Ist die Spezifikation in einem offenen europäischen Normenverzeichnis/-katalog enthalten?

EIF Empfehlung 23: *Heranziehen der maßgeblichen Kataloge für Normen, Spezifikationen und Leitlinien auf einzelstaatlicher und auf EU-Ebene im Einklang mit dem NIF und den betreffenden DIF bei der Beschaffung und Entwicklung von IKT-Lösungen.*

EIF Empfehlung 6: *Mit- und Weiterverwenden bestehender Lösungen sowie Zusammenarbeit bei der Entwicklung gemeinsamer Lösungen bei der Einführung europäischer öffentlicher Dienste.*

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin, dass die Norm oder Spezifikation in einen supranationalen Normenkatalog aufgenommen wurde. Die Spezifikation kann auf europäischen Plattformen, z. B. CEN, CENELEC oder ETSI, gefunden werden.

4.6.7. EIF-A42: Ist die Spezifikation eine europäische Norm?

EIF Empfehlung 27: *Sorge dafür, dass die Rechtsvorschriften anhand eines „Interoperabilitäts-Checks" auf vorhandene Hindernisse für die Interoperabilität durchleuchtet werden. Bemühen darum, bei der Ausarbeitung von Rechtsvorschriften zur Schaffung eines europäischen öffentlichen Dienstes diese mit der maßgeblichen Gesetzgebung in Einklang zu bringen, Durchführung eines „digitalen Checks" und Berücksichtigung datenschutzrechtlicher Anforderungen.*

Europäische Normen sind jene Normen, die von einschlägigen Organisationen entwickelt wurden. CEN, CENELEC und ETSI sind dabei die wichtigsten Organisationen und entwickeln ihre Normen auf der Grundlage der in der europäischen Normungsverordnung festgelegten Anforderungen. Website des CEN und CENELEC: https://www.cencenelec.eu/

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel in einer Bewertung der Norm oder Spezifikation im Hinblick auf die Verordnung (EU) Nr. 1025/2012.

4.6.8. EIF-A43: Ermöglicht die Spezifikation eine Geschäftsprozessmodellierung?

EIF Empfehlung 28: *Dokumentieren der Geschäftsprozesse unter Verwendung allseits anerkannter Modellierungstechniken und Herstellen von Einvernehmen darüber, wie diese Prozesse zur Bereitstellung eines europäischen öffentlichen Dienstes aneinander angeglichen werden sollten.*

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu belegen, dass die Norm oder Spezifikation ein einheitliches Vorgehen bei der Geschäftsprozessmodellierung unterstützt, d. h. dass die Spezifikation bei der Gestaltung von Flussdiagrammen usw. herangezogen oder allgemein dafür genutzt wird. Ein Beispiel hierfür könnten UML oder ITIL sein, also Spezifikationen für die Festlegung verschiedener Schritte oder Punkte der Geschäftsentwicklung.

4.6.9. EIF-A44: Inwieweit ermöglicht die Spezifikation Vereinbarungen über organisatorische Interoperabilität?

EIF Empfehlung 29: *Klären und Formalisieren der organisatorischen Beziehungen für die Einrichtung und den Betrieb europäischer öffentlicher Dienste.*

Bezieht sich auf die Fähigkeit der Spezifikationen, das Erstellen und Formalisieren von Interoperabilitätsvereinbarungen zu unterstützen und zu erleichtern. Beispiele sind Absichtserklärungen (*Memorandum of Unterstanding*, MoU) und Dienstleistungsvereinbarungen (*Service Level Agreement*, SLA).

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu prüfen, ob sich die Spezifikation positiv auf das Erstellen oder Schließen von Vereinbarungen über organisatorische Interoperabilität auswirkt.

4.6.10. EIF-A45: Ermuntert die Spezifikation zur Gründung von Gemeinschaften und zum Austausch ihrer Daten und Ergebnisse auf nationalen und/oder europäischen Plattformen?

EIF Empfehlung 32: *Unterstützen des Aufbaus sektorspezifischer und sektorübergreifender Gemeinschaften, deren Ziel darin besteht, Spezifikationen für offene Informationen zu schaffen, und Ermuntern der betreffenden Gemeinschaften zur Weitergabe ihrer Ergebnisse auf nationalen und europäischen Plattformen.*

Bezieht sich auf Spezifikationen, die eng mit den ausgetauschten Daten/Informationen, ihrem Format und ihrer Struktur zusammenhängen. Dies würde eine gemeinsame Methode/ein gemeinsames Verfahren ermöglichen, um die Weiterverwendung und den Austausch zu verbessern und mögliche Einschränkungen zu beseitigen. Ein Beispiel hierfür könnte RDF sein, das zur Beschreibung von Informationen und ihren Metadaten mittels spezifischer Syntax und Serialisierung verwendet wird.

Wie wird geprüft?

Der Nachweis dieses Kriteriums besteht in der Regel darin zu prüfen, ob die Spezifikation die Einrichtung europäischer Plattformen/Gemeinschaften unterstützt, um die Erkenntnisse und Ergebnisse aus der Erweiterung und Umsetzung digitaler Lösungen/Dienste auszutauschen und einzubeziehen.

Kapitel 5. Profil für die Multi-Stakeholder Platform

Anwendungsbereich

Dieses CAMSS-Szenario befasst sich mit der Bewertung formaler Spezifikationen im Rahmen der öffentlichen Auftragsvergabe (“ …assessment of formal specifications in the context of public procurement”). Die verwendeten Kriterien sind in Anhang II der Normungsverordnung [EU 1025/2012] als Anforderungen für die Identifizierung technischer IKT-Spezifikationen für deren Verwendung im Beschaffungswesen festgelegt.

Automatisierte Übersetzung

Der gesamte Abschnitt ist mit Google Translate automatisiert übersetzt worden. Es gab noch keine Qualitätssicherung.

Eine informelle Übersetzung durch den Sprachendienst des BMI wäre wünschenswert.

Die verschiedenen Kriterien des MSP-Szenarios sind gemäß der europäischen Normungsverordnung 1025/2012 in Kategorien unterteilt.

MSP-A01	Die technische Spezifikation oder der Standard wurde von verschiedenen Anbietern/Lieferanten für unterschiedliche Implementierungen verwendet.
MSP-A02	Die Implementierung der technischen Spezifikation oder des Standards beeinträchtigt nicht die Interoperabilität mit Implementierungen, die derzeit auf bestehenden europäischen oder internationalen Standards basieren.
MSP-A03	Es liegen öffentliche Verweise (insbesondere in Richtlinien oder bei der Auftragsvergabe) auf die jeweiligen Spezifikationen der öffentlichen Behörden vor.
MSP-A04	Deckt die technische Spezifikation oder Norm andere Bereiche ab als die technischen Spezifikationen, die als europäische Norm in Erwägung gezogen werden? (d. h. technische Spezifikationen, die von einer nicht formalen Normungsorganisation, also nicht CEN, CENELEC oder ETSI, bereitgestellt werden, können als europäische Norm oder alternativ als identifizierte technische Spezifikation in Erwägung gezogen werden.)
MSP-A05a	Ist die Annahme neuer europäischer Normen, die dieselben Bereiche abdecken wie die vorgeschlagene Spezifikation (oder Norm), innerhalb eines angemessenen Zeitrahmens vorgesehen?
MSP-A05b	Gibt es bereits bestehende europäische Normen mit Marktakzeptanz, die dieselben Bereiche abdecken wie die vorgeschlagene Spezifikation (oder Norm), die bewertet wird?
MSP-A05c	Wenn ja, werden die bestehenden Standards obsolet?

MSP-A06	Ist die Organisation, die Standards entwickelt, eine gemeinnützige Organisation?
MSP-A07	Steht die Teilnahme am Erstellungsprozess der Spezifikation allen interessierten Parteien (z. B. Organisationen, Unternehmen und Einzelpersonen) offen?
MSP-A08	Werden die Spezifikationen in einem auf Konsens ausgerichteten Entscheidungsprozess verabschiedet?
MSP-A09	Ist die relevante Dokumentation des Entwicklungs- und Genehmigungsprozesses der Spezifikation archiviert und gekennzeichnet?
MSP-A10	Werden Informationen über (neue) Standardisierungsaktivitäten durch geeignete und zugängliche Mittel weithin bekannt gemacht?
MSP-A11	Alle relevanten Beteiligten können gegen die Entwicklung und Genehmigung von Spezifikationen formal Einspruch einlegen oder Einwände erheben?
MSP-A12	Verfügt die Spezifikation über einen definierten Wartungs- und Supportprozess?
MSP-A13	Ist die Spezifikation öffentlich verfügbar, um sie zu angemessenen Bedingungen zu implementieren und zu verwenden?
MSP-A14a	Ist die Spezifikation auf (F)RAND-Basis lizenziert?
MSP-A14b	Ist die Spezifikation lizenzfrei lizenziert?
MSP-A15a	Befasst sich die Spezifikation mit der Interoperabilität zwischen öffentlichen Verwaltungen und erleichtert diese?
MSP-A15b	Gibt es Belege dafür, dass sich die Einführung der Spezifikation positiv auf einen oder mehrere der folgenden Bereiche auswirkt: organisatorische Prozesse, das Umfeld, den Verwaltungsaufwand, die Unterstützung von Menschen mit Behinderungen, grenzüberschreitende Dienste, politische Ziele, gesellschaftliche Bedürfnisse?
MSP-A16a	Ist die Spezifikation weitgehend unabhängig von bestimmten Herstellerprodukten?
MSP-A16b	Ist die Spezifikation weitgehend unabhängig von bestimmten Plattformen oder Technologien?
MSP-A17	Ist die Spezifikation detailliert genug, konsistent und vollständig für die Verwendung und Entwicklung von Produkten und Dienstleistungen?

5.1. Marktakzeptanz

In dieser Kategorie wird geprüft, ob technische Spezifikationen Marktakzeptanz finden und ihre Implementierungen die Interoperabilität mit bestehenden europäischen oder internationalen Standards nicht beeinträchtigen. Die Marktakzeptanz kann durch praktische Beispiele konformer Implementierungen verschiedener Anbieter nachgewiesen werden.

5.1.1. MSP-A01: Die technische Spezifikation oder der Standard wurde von verschiedenen Anbietern/Lieferanten für unterschiedliche Implementierungen verwendet.

Wie wird geprüft?

Die Begründung für dieses Kriterium besteht aus einer Sammlung verschiedener Produkte oder Projekte, die Implementierungen der bewerteten Spezifikation enthalten und von verschiedenen Anbietern/Lieferanten entwickelt oder durchgeführt werden.

5.1.2. MSP-A02: Die Implementierung der technischen Spezifikation oder des Standards beeinträchtigt nicht die Interoperabilität mit Implementierungen, die derzeit auf bestehenden europäischen oder internationalen Standards basieren.

Wie wird geprüft?

Um dieses Kriterium zu erfüllen, sollten die folgenden Schritte befolgt werden.

- Prüfen Sie, ob in der Dokumentation der bewerteten Spezifikation angegeben ist, dass zwischen dieser Spezifikation und einer europäischen oder internationalen Spezifikation ein Interoperabilitätsproblem besteht.
- Wenn kein Problem besteht, stellen Sie fest, welche bestehenden europäischen oder internationalen Spezifikationen auf der bewerteten Spezifikation basieren oder von dieser verwendet werden können und ob sie bereits vom MSP identifiziert wurden.
- Sobald die Liste erstellt ist, prüfen Sie die Marktakzeptanz der aufgeführten Spezifikationen. Bei allgemein akzeptierten Spezifikationen gehen wir davon aus, dass sie die Interoperabilität mit anderen Spezifikationen nicht beeinträchtigen.
- Überprüfen Sie abschließend, ob zwischen den Spezifikationen daraus und den bewerteten Spezifikationen ein Interoperabilitätsproblem besteht.
- In Ermangelung europäischer oder internationaler Spezifikationen, deren Umsetzung mit einer der bewerteten Spezifikationen in Zusammenhang stehen könnte, lautet die Begründung für dieses Kriterium „N/A“, da nicht mit einem gewissen Grad an Sicherheit angegeben werden kann, ob die Umsetzung der bewerteten Spezifikation die Interoperabilität mit der Umsetzung bestehender europäischer oder internationaler Spezifikationen behindert.

5.1.3. MSP-A03: Es liegen öffentliche Verweise (insbesondere in Richtlinien oder bei der Auftragsvergabe) auf die jeweiligen Spezifikationen der öffentlichen Behörden vor.

Wie wird geprüft?

Um dieses Kriterium zu untermauern, wird untersucht, ob in öffentlichen Dokumenten von Behörden, insbesondere im Hinblick auf Richtlinien und Beschaffungen, auf die bewertete Spezifikation verwiesen wird.

5.2. Kohärenzprinzip

Diese Kategorie dient dazu, zu prüfen, ob technische Spezifikationen kohärent sind, d. h., sie decken Bereiche ab, in denen die Einführung neuer europäischer Normen nicht innerhalb eines angemessenen Zeitraums vorgesehen ist, in denen bestehende Normen keine Marktakzeptanz gefunden haben oder obsolet geworden sind und in denen die Umsetzung der technischen Spezifikationen in europäische Normungsprodukte nicht innerhalb eines angemessenen Zeitraums vorgesehen ist.

5.2.1. MSP-A04: Deckt die technische Spezifikation oder Norm andere Bereiche ab als die technischen Spezifikationen, die als europäische Norm in Erwägung gezogen werden? (d. h. technische Spezifikationen, die von einer nicht formalen Normungsorganisation, also nicht CEN, CENELEC oder ETSI, bereitgestellt werden, können als europäische Norm oder alternativ als identifizierte technische Spezifikation in Erwägung gezogen werden.)

Wie wird geprüft?

Um dieses Kriterium zu begründen, soll die Untersuchung in mehreren Schritten durchgeführt werden.

- Zunächst müssen die Bereiche ermittelt werden, die von der bewerteten Spezifikation abgedeckt werden, sowie die Anzahl der damit verbundenen SDOs und technischen Ausschüsse.
- Anschließend wird die Dokumentation dieser SDOs und technischen Ausschüsse überprüft, um herauszufinden, ob darin eine Spezifikation erwähnt wird, die als europäische Norm vorgeschlagen wird und einen der Bereiche abdecken könnte, die von der bewerteten Spezifikation abgedeckt werden.
- Anschließend wird die von CEN, CENELEC, ETSI und anderen relevanten europäischen Institutionen herausgegebene Dokumentation analysiert, um festzustellen, ob eine andere Spezifikation, die denselben Bereich wie die bewertete Spezifikation abdeckt, als europäische Norm vorgeschlagen wurde.
    - https://www.cenelec.eu/
    - https://www.cen.eu/Pages/default.aspx
    - http://www.etsi.org/standards
- Sobald die Untersuchung durchgeführt und ihre Ergebnisse analysiert wurden, wird eine Begründung mit der Anzahl der Übereinstimmungen vorgelegt, die zwischen der bewerteten Spezifikation und allen anderen Spezifikationen festgestellt wurden, die als europäische Norm vorgeschlagen werden.

5.2.2. MSP-A05a: Ist die Annahme neuer europäischer Normen, die dieselben Bereiche abdecken wie die vorgeschlagene Spezifikation (oder Norm), innerhalb eines angemessenen Zeitrahmens vorgesehen?

Wie wird geprüft?

Zur Begründung dieses Kriteriums werden die Ergebnisse der für Kriterium A8 durchgeführten Untersuchung analysiert, um festzustellen, ob es eine Spezifikation gibt, die dieselben Bereiche wie die bewertete Spezifikation abdeckt und als europäische Norm vorgeschlagen wird. Unter „angemessenem Zeitrahmen“ ist lediglich zu verstehen, dass die Spezifikation bereits in den Unterlagen einer zuständigen europäischen Institution als für die Entwicklung als europäische Norm vorgeschlagene Spezifikation veröffentlicht wurde.

5.2.3. MSP-A05b: Gibt es bereits bestehende europäische Normen mit Marktakzeptanz, die dieselben Bereiche abdecken wie die vorgeschlagene Spezifikation (oder Norm), die bewertet wird?

Wie wird geprüft?

Zur Begründung dieses Kriteriums ist in den Datenbanken von ETSI/CEN/CENELEC oder anderen relevanten europäischen Institutionen zu recherchieren, ob es eine europäische Norm gibt, die dieselben Bereiche wie die bewertete Spezifikation abdeckt. Bei Übereinstimmung ist/sind die Spezifikation(en) zu analysieren, um festzustellen, ob sie marktüblich ist/sind.

https://www.cenelec.eu/ https://www.cen.eu/Pages/default.aspx http://www.etsi.org/standards

5.2.4. MSP-A05c: Wenn ja, werden die bestehenden Standards obsolet?

Wie wird geprüft?

Zur Begründung dieses Kriteriums werden die aus der Forschung zu Kriterium A9b gewonnenen Spezifikationen den Ergebnissen neuer Forschungen in den einzelnen von diesen Spezifikationen abgedeckten Bereichen gegenübergestellt, um neue Spezifikationen zu ermitteln. Eine Spezifikation aus der Liste gilt als veraltet, wenn eine neuere Spezifikation existiert, die denselben/dieselben technischen Bereich/Bereiche abdeckt und bereits implementiert ist.

5.3. Eigenschaften

In dieser Kategorie wird bewertet, ob die Spezifikation von einer gemeinnützigen Organisation entwickelt wurde, d. h. von einem Berufsverband, einer Industrie, einem Branchenverband oder einer anderen Mitgliederorganisation, die in ihrem Fachgebiet technische IKT-Spezifikationen entwickelt und keine europäische, nationale oder internationale Normungsorganisation ist . Zusätzlich wird bewertet, ob die Spezifikation durch Prozesse entwickelt wurde, die die folgenden Kriterien erfüllen.

5.3.1. MSP-A06: Ist die Organisation, die Standards entwickelt, eine gemeinnützige Organisation?

Wie wird geprüft?

Um dieses Kriterium zu begründen, muss die SDO, die Eigentümerin der vorgeschlagenen Spezifikation ist, untersucht werden, um festzustellen, ob es sich um eine gemeinnützige Organisation handelt. Beispiele für gemeinnützige Organisationen, die Standards und Spezifikationen entwickeln, sind das World Wide Web Consortium und die Internet Engineering Task Force (IETF). Siehe W3C https://www.w3.org/ und IETF https://www.ietf.org/ .

5.3.2. MSP-A07: Steht die Teilnahme am Erstellungsprozess der Spezifikation allen interessierten Parteien (z. B. Organisationen, Unternehmen und Einzelpersonen) offen?

Wie wird geprüft?

Zur Begründung dieses Kriteriums muss der Entwicklungsprozess der bewerteten Spezifikation untersucht werden, um festzustellen, ob es sich um einen offenen Prozess für alle Beteiligten handelt (sofern es Ausnahmen im Prozess gibt, sind diese zu analysieren). Die Begründung besteht aus einer begründeten Aussage (JA/NEIN) und einer kurzen Beschreibung des Prozesses. Sie ist in der Regel in der Spezifikationsdokumentation oder auf der Website der SDO zu finden.

5.3.3. MSP-A08: Werden die Spezifikationen in einem auf Konsens ausgerichteten Entscheidungsprozess verabschiedet?

Wie wird geprüft?

Um dieses Kriterium zu begründen, muss der Entwicklungsprozess der bewerteten Spezifikation untersucht werden. Ziel dieser Untersuchung ist es festzustellen, ob und in welchem Ausmaß das Prozessziel – und damit die Genehmigungsmethodik – allgemein anerkannt ist. Die Begründung besteht aus einer begründeten Stellungnahme (JA/NEIN) und einer kurzen Beschreibung des Prozesses. Sie ist in der Regel in der Spezifikationsdokumentation oder auf der Website der SDO zu finden.

5.3.4. Transparenz

5.3.4.1. MSP-A09: Ist die relevante Dokumentation des Entwicklungs- und Genehmigungsprozesses der Spezifikation archiviert und gekennzeichnet?

Wie wird geprüft?

Um dieses Kriterium zu begründen, müssen die Repositorien der SDO, die Eigentümerin der Spezifikation ist, untersucht werden, um festzustellen, ob der Entwicklungs- und Genehmigungsprozess der Spezifikation dokumentiert ist. Diese Dokumentation ist in der Regel in der Spezifikationsdokumentation oder auf der Website der SDO zu finden.

5.3.4.2. MSP-A10: Werden Informationen über (neue) Standardisierungsaktivitäten durch geeignete und zugängliche Mittel weithin bekannt gemacht?

Wie wird geprüft?

Zur Begründung dieses Kriteriums muss eine Untersuchung zum Veröffentlichungsprozess der (neuen) Normungsaktivitäten durchgeführt werden, um festzustellen, ob diese Informationen durch geeignete und zugängliche Mittel weithin bekannt gemacht werden.

Zu diesem Zweck ist Folgendes zu berücksichtigen.

- Weithin angekündigt: Die offene, wiederholte und diskriminierungsfreie Verbreitung von Informationen gilt als weithin angekündigt.
- Geeignete Mittel: Als geeignet gelten alle Fachmittel wie Untersuchungsberichte, Fachzeitschriften und Bulletins öffentlicher Organisationen mit Fachkompetenz.
- Zugänglich: Alle Mittel, die der Öffentlichkeit ohne jegliche Diskriminierung der Benutzer zugänglich sind, gelten als zugänglich.

Diese Informationen finden Sie in der Spezifikationsdokumentation oder auf der Website des SDO.

5.3.4.3. MSP-A11: Alle relevanten Beteiligten können gegen die Entwicklung und Genehmigung von Spezifikationen formal Einspruch einlegen oder Einwände erheben?

Wie wird geprüft?

Um dieses Kriterium zu begründen, muss der Entwicklungsprozess der bewerteten Spezifikation untersucht werden, um festzustellen, ob alle relevanten Stakeholder formal Einspruch erheben können.

oder Einwände gegen die Entwicklung und Genehmigung von Spezifikationen erheben. Die Begründung für dieses Kriterium besteht aus Beispielen von Leitlinien des Entwicklungsprozesses oder aus Dokumentationen, die formelle Einwände relevanter Interessengruppen enthalten.

Zu diesem Zweck werden diejenigen Stakeholder als relevant betrachtet, deren Input einen direkten Einfluss auf den Entwicklungsprozess der Spezifikation haben könnte, oder diejenigen anderen Stakeholder, deren Input einen direkten Einfluss auf den Entwicklungsprozess der Spezifikation haben könnte.

Diese Informationen finden Sie in der Spezifikationsdokumentation oder auf der Website des SDO.

5.4. Anforderungen

In dieser Kategorie orientieren sich die Kriterien an den in der europäischen Normungsverordnung festgelegten Anforderungen.

5.4.1. MSP-A12: Verfügt die Spezifikation über einen definierten Wartungs- und Supportprozess?

Wie wird geprüft?

Um dieses Kriterium zu begründen, muss die SDO, die die bewertete Spezifikation besitzt, analysiert werden, um festzustellen, ob sie einen definierten Wartungs- und Supportprozess eingerichtet hat. Diese Informationen finden Sie in der Spezifikationsdokumentation oder auf der Website der SDO.

5.4.2. MSP-A13: Ist die Spezifikation öffentlich verfügbar, um sie zu angemessenen Bedingungen zu implementieren und zu verwenden?

Wie wird geprüft?

Um dieses Kriterium zu rechtfertigen, muss die SDO, die Eigentümerin der bewerteten Spezifikation ist, analysiert werden, um festzustellen, ob sie die Spezifikation für ihre Umsetzung durch die Öffentlichkeit zu angemessenen Bedingungen bereitstellt, wobei als angemessene Bedingungen alle Bedingungen gelten, die nicht restriktiver sind als die durchschnittlichen Bedingungen anderer SDOs oder Organisationen, die zum spezifischen Anwendungsbereich der bewerteten Spezifikation gehören.

5.4.3. MSP-A14a: Ist die Spezifikation auf (F)RAND-Basis lizenziert?

Wie wird geprüft?

Um dieses Kriterium zu begründen, muss die Lizenz, unter der die bewertete Spezifikation veröffentlicht wird, analysiert werden, um festzustellen, ob sie den (F)RAND-Lizenzbedingungen entspricht. Diese Informationen finden Sie in der Spezifikationsdokumentation oder auf der Website der SDO.

5.4.4. MSP-A14b: Ist die Spezifikation lizenzfrei lizenziert?

Wie wird geprüft?

Um dieses Kriterium zu begründen, muss die Lizenz, unter der die bewertete Spezifikation veröffentlicht wird, analysiert werden, um festzustellen, ob sie lizenzfrei ist. Diese Informationen finden Sie in der Spezifikationsdokumentation oder auf der Website der SDO.

5.4.5. MSP-A15a: Befasst sich die Spezifikation mit der Interoperabilität zwischen öffentlichen Verwaltungen und erleichtert diese?

Wie wird geprüft?

Um dieses Kriterium zu untermauern, muss untersucht werden, ob es bereits von einer öffentlichen Verwaltung veröffentlichte Dokumente gibt, aus denen hervorgeht, dass die bewertete Spezifikation die Interoperabilität zwischen anderen öffentlichen Verwaltungen und der für die Veröffentlichung verantwortlichen Stelle erleichtert.

5.4.6. MSP-A15b: Gibt es Belege dafür, dass sich die Einführung der Spezifikation positiv auf einen oder mehrere der folgenden Bereiche auswirkt: organisatorische

Prozesse, das Umfeld, den Verwaltungsaufwand, die Unterstützung von Menschen mit Behinderungen, grenzüberschreitende Dienste, politische Ziele, gesellschaftliche Bedürfnisse?

Wie wird geprüft?

Um dieses Kriterium zu begründen, muss untersucht werden, ob es bereits von einer öffentlichen Verwaltung veröffentlichte Dokumente gibt, aus denen hervorgeht, dass sich die bewertete Spezifikation positiv auf einen oder mehrere der folgenden Punkte auswirkt:

- Organisatorische Prozesse
- Die Umwelt
- Der Verwaltungsaufwand
- Die Behinderung unterstützt
- Grenzüberschreitende Dienstleistungen
- Politische Ziele und gesellschaftliche Bedürfnisse

Die Begründung für dieses Kriterium ist positiv, wenn sich nachweisen lässt, dass es sich positiv auf einen der oben genannten Bereiche auswirkt.

5.4.7. Neutralität und Stabilität

5.4.7.1. MSP-A16a: Ist die Spezifikation weitgehend unabhängig von bestimmten Herstellerprodukten?

Wie wird geprüft?

Um dieses Kriterium zu begründen, muss die bewertete Spezifikation daraufhin untersucht werden, ob sie unabhängig von bestimmten Anbietern/Produkten ist. Eine mögliche Begründung kann durch die Analyse der Implementierungen der bewerteten Spezifikation erfolgen, um festzustellen, ob diese von verschiedenen Anbietern/Lieferanten durchgeführt wurden.

5.4.7.2. MSP-A16b: Ist die Spezifikation weitgehend unabhängig von bestimmten Plattformen oder Technologien?

Wie wird geprüft?

Um dieses Kriterium zu begründen, muss die bewertete Spezifikation untersucht werden, um festzustellen, ob sie unabhängig von bestimmten Plattformen/Technologien ist. Eine mögliche Begründung kann durch die Analyse der Implementierungen der bewerteten Spezifikation erfolgen, um festzustellen, ob diese mit unterschiedlichen Plattformen/Technologien durchgeführt wurden.

5.4.8. Qualität

5.4.8.1. MSP-A17: Ist die Spezifikation detailliert genug, konsistent und vollständig für die Verwendung und Entwicklung von Produkten und Dienstleistungen?

Wie wird geprüft?

Zur Begründung dieses Kriteriums sind die Informationen über die Implementierungen einschließlich der bewerteten Spezifikation aus den Kriterien A42a und A42b erneut zu verwenden, um nachzuweisen, dass die bewertete Spezifikation bereits für die Implementierung verwendet wurde. Falls die Recherche zur Begründung der Kriterien A42a und A42b nicht durchgeführt wurde, ist sie nun durchzuführen.

Anhang A. Verzeichnis der Abkürzungen

In der folgenden Tabelle werden die in diesem Dokument verwendeten Akronyme erläutert.

Akronym	Bedeutung
ABB	*Architecture Building Blocks* Architekturbausteine
CAMSS	*Common Assessment Method for Standards and Specifications* Gemeinsames Bewertungsverfahren für Normen und Spezifikationen
CAV	Core Assessment Vocabulary
CCCEV	Core Criterion and Core Evidence Vocabulary
CEN	*European Committee for Standardization* Europäisches Komitee für Normung
CENELEC	*European Committee for Electrotechnical Standardization* Europäisches Komitee für elektrotechnische Normung
CSSV	Core Standards and Specifications Vocabulary
DIF	*Domain-specific Interoperability Framework* Bereichsspezifischer Interoperabilitätsrahmen
DITR	Deutsche Informationszentrum für Technische Regeln
EIF	*European Interoperability Framework* Europäischer Interoperabilitätsrahmen
EIRA	*European Interoperability Reference Architecture* Europäische Interoperabilitäts-Referenzarchitektur
ETSI	*European Telecommunications Standards Institute* Europäisches Institut für Telekommunikationsnormen
EU	Europäische Union
FIT.SB	Föderales Standardisierungsboard
FRAND	*Fair, Reasonable And Non-Discriminatory* fair, angemessen und diskriminierungsfrei
KoSIT	Koordinierungsstelle für IT Standards
MSP	Multi Stakeholder Platform
NIF	*National Interoperability Framework*

	Nationaler Interoperabilitätsrahmen
NIFO	*National Interoperability Framework Observatory* Beobachtungsstelle für die nationalen Interoperabilitätsrahmen
NOOTS	Nationales Once Only technical system
OOP	*Once-Only Principle* Grundsatz der einmaligen Erfassung
SAK	Sicherer Anschlussknoten
SDO	*Standards Developing Organisation* Normungsorganisation
XÖV	Rahmenwerk XML in der öffentlichen Verwaltung

Glossar

Interoperabilität

die Fähigkeit öffentlicher Stellen, im Interesse der Verfolgung von Zielen von beiderseitigem Nutzen zusammenzuwirken; dies schließt den Austausch von Informationen und Wissen zwischen den beteiligten Organisationen durch von ihnen unterstützte Geschäftsprozesse mittels Datenaustausch zwischen ihren IKT-Systemen ein.

IT-Standard

Im Sinne dieses Dokuments eine *Norm* oder eine *Spezifikation* im Bereich der Informations- und Kommunikationstechnologien, die den Austausch von Daten zwischen dem Bund und den Ländern oder zwischen öffentlichen Stellen und Bürgerinnen, Bürgern oder Unternehmen festlegt.

Eine verbindliche Festlegung von IT-Standards kann unter anderem gemäß § 2 IT-Staatsvertrag durch Beschluss des IT-Planungsrat erfolgen.

Norm

Eine von einer anerkannten Normungsorganisation angenommene technische Spezifikation zur wiederholten oder ständigen Anwendung, die von einer Normungsorganisation (ISO, CEN, CENELEC oder DIN) angenommen worde, oder eine europäische Norm, die auf der Grundlage eines Auftrags der Kommission zur Durchführung von Harmonisierungsrechtsvorschriften der Union angenommen wurde.

Spezifikation

Ein Schriftstück, in dem die technischen Anforderungen dargelegt sind, die ein Produkt, ein Verfahren, eine Dienstleistung oder ein System zu erfüllen hat, wie Qualitätsstufen, Leistung, Interoperabilität oder Sicherheit, einschließlich der Anforderungen an die Terminologie, Prüfungen und Prüfverfahren sowie die Konformitätsbewertungsverfahren.

Standardisierungsradar

Die FITKO betreibt und pflegt (ggf. mit Hilfe Dritter) ein öffentlich zugängliches Standardisierungsradar, das technologische Entwicklungen und Trends der Standardisierung möglichst frühzeitig und proaktiv aufgreift und öffentlich zugänglich präsentiert. Von Seiten des Bundes werden dazu ergänzend erkennbare Trends auf europäischer Ebene eingebracht, bei denen eine Auswirkung auf Standardisierungsbedarfe in Deutschland zu erwarten ist.

Bibliografie

[EIF 2017] *Europäischer Interoperabilitätsrahmen – Umsetzungsstrategie*, Mitteilung der Kommission vom 23.3.2017.

[EU 1025/2012] *Verordnung (EU) Nr. 1025/2012 des europäischen Parlaments und des Rates zur europäischen Normung* (Normenverordnung) vom 25. Oktober 2012