

Bewertung von IT-Standards durch das Föderale Standardisierungsboard

Fassung vom 1. 12. 2025

Bewertung von IT-Standards durch das Föderale Standardisierungsboard

Fassung vom 1. 12. 2025

Die Bewertung von IT-Standards vor einer verbindlichen Vorgabe ist eine der Hauptaufgaben des Föderalen Standardisierungsboards des IT-Planungsrats. CAMSS ist ein Rahmenwerk der europäischen 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* bzw. *Szenarien*. Die EU Kommission stellt zwei Profile für europäische Kommunikationsszenarien zur Verfügung. In diesem Dokument werden zwei weitere Profile für den nationalen Kontext festgelegt. So soll erreicht werden, dass nationale Gremien Beschlüsse zu IT-Standards auf der Basis einer neutralen und objektiven Bewertung treffen können. Das Föderale Standardisierungsboard hat dieses Dokument im September 2025 als Grundlage seiner Prüfung und Bewertung von IT-Standards beschlossen.

Datum der Erstellung dieses Dokuments: 24.4.2026. Für das Föderale Standardisierungsboard des IT-Planungsrats (FIT.SB) erstellt durch Conny Diebel (FITKO), Lutz Rabe (KoSIT), Tobias Schuh (FITKO) und Frank Steimke (KoSIT). Zur Kontaktaufnahme nutzen Sie bitte die E-Mail it-standards@fitko.de.

Dieser Inhalt steht unter der Lizenz **CC BY 4.0**. Den Lizenztext finden Sie unter: creativecommons.org/licenses/by/4.0/deed.de. Bei der Verwendung des Werkes ist das "Föderale Standardisierungsboard des IT-Planungsrats" als Urheber zu nennen.

Inhaltsverzeichnis

1. Einführung.	1
2. Die Prozesse der Standardisierungsagenda.	2
2.1. Übergreifende Prozesse und Aufgaben.	2
2.2. Lebenszyklusprozess.	3
3. Profil für fachunabhängige und fachübergreifende IT-Standards.	6
3.1. Subsidiarität und Verhältnismäßigkeit.	8
3.2. Offenheit.	9
3.3. Transparenz.	10
3.4. Wiederverwendung.	10
3.5. Technologieneutralität.	11
3.6. Sicherheit und Privatsphäre.	11
3.7. Mehrsprachigkeit.	12
3.8. Verwaltungsvereinfachung.	13
3.9. Informationsbewahrung.	13
3.10. Qualität, Effektivität und Effizienz.	13
3.11. Digitale Souveränität.	14
3.12. Marktakzeptanz.	15
4. Profil zur Feststellung der XÖV-Konformität.	16
4.1. Bereitstellungspflichten.	20
4.2. Auskunftspflichten der entwickelnden und betreibenden Stellen.	22
4.3. Wiederverwendung.	22
4.4. Technische Kriterien.	23
4.5. Prüfung der XÖV-Konformität.	25
Abkürzungsverzeichnis und Glossar.	28
Bibliografie.	30

Kapitel 1. 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 "CAMSS" Ansatz [IE CAMSS]. Er 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" bzw. "Szenarien". Die EU-Kommission legt Profile fest, die zur Bewertung auf der Grundlage *europäischer Anforderungen zur Interoperabilität* geeignet sind. Dazu gehören [CAMSS EIF] und [CAMSS MSP]. Für das Föderale Standardisierungsboard ist insbesondere das "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 Praxis-einsatz 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 2 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 1.1. Prozessmodell der Standardisierungsagenda



Die Entscheidung des Föderalen 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:

- Wenn die Interoperabilität zu europäischen Verfahren im Vordergrund steht, soll das [CAMSS EIF] Szenario der Europäischen Kommission genutzt werden.
- Sofern in Ausschreibungen die Konformität zu Normen oder Standards der EU-Kommission gefordert werden soll, ist das [CAMSS MSP] Szenario der Europäischen Kommission einschlägig.
- Für einen auf der Grundlage des XÖV-Standardisierungsrahmens entwickelten IT-Standard soll das Profil zur Feststellung der XÖV-Konformität gemäß Kapitel 4 (die XÖV-Zertifizierung) angewandt werden.
- 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 gemäß Kapitel 3 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 Entwicklungs- und Betriebskosten

Kapitel 2. Die Prozesse der Standardisierungsagenda

Im Folgenden wird das in Abbildung 1.1 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.

2.1. 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 Standardisierungsradsars.

2.1.1. 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 Standardisierungsradsars wird ein Konzept erarbeitet und mit dem Standardisierungsboard abgestimmt. Eine Orientierung geben bereits existierende Technologieradare.

2.1.2. 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-detail](#)The European Interoperability Framework in detail

2.2. 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

2.2.1. 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.

2.2.2. 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-Planungsrats entscheidet das Standardisierungsboard über die Umsetzung eines Standardisierungsbedarfs.

2.2.3. 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.

2.2.4. 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.

2.2.5. 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.

2.2.6. 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.

2.2.7. 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 3. 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 wesentlich 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).

Subsidiarität und Verhältnismäßigkeit	
KKN-01	Es handelt sich um einen fachunabhängigen oder fachübergreifenden IT-Standard
KKN-02	Es gibt in der öffentlichen Verwaltung keinen anderen, bereits beschlossenen IT-Standard mit gleichem oder ähnlichem Standardisierungsgegenstand
KKN-03	Der Bedarf an einem IT-Standard ist nachgewiesen
KKN-04	Der Bedarf an der verbindlichen Vorgabe eines IT-Standardisierungsbedarfs ist nachgewiesen
KKN-05	Die Möglichkeit der Vorgabe eines Marktstandards im Sinne des § 2 Abs 1 Satz 2 [IT-Staatsvertrag] wurde geprüft
Offenheit	
KKN-06	Alle Interessensträger können sich diskriminierungsfrei an der Entwicklung und Weiterentwicklung des IT-Standards beteiligen
KKN-07	Eine öffentliche Überprüfung ist Teil des Releasezyklus
KKN-08	Die Lizenzierung der geistigen Eigentumsrechte an dem IT-Standard erfolgt zu FRAND -Bedingungen
KKN-09	Der IT-Standard unterstützt die Bereitstellung offener Verwaltungsdaten
Transparenz	

KKN-10	Inwieweit geht der IT-Standard nachvollziehbar auf Abläufe, Bestimmungen, Daten und Dienstleistungen der Verwaltung ein?
Wiederverwendung	
KKN-11	Werden verbindlich beschlossene Kerndatenmodelle angemessen berücksichtigt?
KKN-12	Werden bewährte Datenobjekte, Codelisten und Prozessmuster in angemessenem Umfang wiederverwendet?
Technologieneutralität	
KKN-13	Ist der IT-Standard technologieneutral?
Sicherheit und Privatsphäre	
KKN-14	Inwieweit ermöglicht der IT-Standard einen sicheren Datenaustausch?
KKN-15	Inwieweit gewährleistet der IT-Standard die Authentizität und Authentifizierung der an einem Datenaustausch beteiligten Akteure?
Mehrsprachigkeit	
KKN-16	Wird die DIN 91379 für die Schreibweise von Namen angemessen berücksichtigt?
Verwaltungsvereinfachung	
KKN-17	Trägt der IT-Standard zur Umsetzung des Once Only Prinzips bei?
Informationsbewahrung	
KKN-18	Inwieweit ermöglicht der IT-Standard die langfristige Bewahrung von Daten/Informationen/Wissen?
Qualität, Effektivität und Effizienz	
KKN-19	Ist der IT-Standard geeignet, den gemeldeten Bedarf zu decken?
KKN-20	Ist der IT-Standard detailliert genug, konsistent und vollständig für die Verwendung und Entwicklung von Produkten und Dienstleistungen?
KKN-21	Basiert der IT-Standard auf Normen oder Marktstandards im Sinne des § 2 Abs. 1 Satz 2 [IT-Staatsvertrag]?
KKN-22	Basiert der IT-Standard auf einem Fachmodell, welches etablierte Modellierungsmethoden nutzt?
KKN-23	Hat der IT-Standard die notwendige Reife?
Digitale Souveränität	
KKN-24	Die öffentliche Verwaltung muss die Entwicklung und Weiterentwicklung des IT-Standards ausreichend kontrollieren und steuern können.
KKN-25	Ist der dauerhafte Betrieb des IT-Standards gewährleistet?

KKN-26	Entspricht der IT-Standard den einschlägigen Vorgaben der föderalen Architekturrichtlinie?
Marktakzeptanz	
KKN-27	Wird der IT-Standard von verschiedenen Anbietern/Lieferanten für unterschiedliche Implementierungen verwendet?

3.1. Subsidiarität und Verhältnismäßigkeit

KKN-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).

KKN-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	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	Prüft das Deutsche Informationszentrum für technische Regeln (DITR).
KoSIT	Prüft das XRepository hinsichtlich XÖV-Standards und Standardisierungsiniciativen.

KKN-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.

KKN-04: Der Bedarf an der verbindlichen Vorgabe eines IT-Standardisierungsbedarfs ist nachgewiesen

Ggfs. ist eine Empfehlung ausreichend.

Zuständigkeiten im Rahmen der Prüfung	
Föderales Standardisierungsboard	Prüft, ob es zur Erreichung der Ziele zwingend einer verbindlichen Vorgabe des IT-Planungsrats auf der Grundlage des § 2 [IT-Staatsvertrag] bedarf.

KKN-05: Die Möglichkeit der Vorgabe eines Marktstandards im Sinne des § 2 Abs 1 Satz 2 [IT-Staatsvertrag] wurde geprüft

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

Zuständigkeiten im Rahmen der Prüfung	
DIN	Prüft, ob der Standardisierungsbedarf mit einer Norm gedeckt werden kann.
FITKO	Prüft, ob der Standardisierungsbedarf mit einem Marktstandard gedeckt werden kann.

3.2. Offenheit

KKN-06: Alle Interessensträger können sich diskriminierungsfrei an der Entwicklung und Weiterentwicklung des IT-Standards beteiligen

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

KKN-07: Eine öffentliche Überprüfung ist Teil des Releasezyklus

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

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

KKN-08: 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

KKN-09: 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.

3.3. Transparenz

KKN-10: Inwieweit geht der IT-Standard nachvollziehbar auf Abläufe, Bestimmungen, Daten und Dienstleistungen der Verwaltung ein?

Zuständigkeiten im Rahmen der Prüfung	
Föderales 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.

3.4. Wiederverwendung

KKN-11: Werden verbindlich beschlossene Kerndatenmodelle angemessen berücksichtigt?

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

- Kerndatenmodell XUnternehmen;
- 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.

KKN-12: 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 Föderalen Standardisierungsboards – 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 die SEMIC Core Vocabularies und Terminologien berücksichtigt werden.

3.5. Technologieneutralität

KKN-13: 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 Föderalen Standardisierungsboards – die funktionale Beschreibung und das zugrunde liegende Fachmodell des IT-Standards daraufhin, ob der IT-Standard technologieneutral ist.

3.6. Sicherheit und Privatsphäre

KKN-14: 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 Föderalen Standardisierungsboards 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.

KKN-15: 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 Föderalen Standardisierungsboards 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.

3.7. Mehrsprachigkeit

KKN-16: 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 Föderalen Standardisierungsboards – die Selbstauskunft der Betreiber des IT-Standards und 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.

3.8. Verwaltungsvereinfachung

KKN-17: 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 Föderalen Standardisierungsboards – 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.

3.9. Informationsbewahrung

KKN-18: 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.

3.10. Qualität, Effektivität und Effizienz

KKN-19: Ist der IT-Standard geeignet, den gemeldeten Bedarf zu decken?

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

KKN-20: 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 Föderalen Standardisierungsboards – 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.

KKN-21: 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. Marktstandards

(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 Föderalen Standardisierungsboards – 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.

KKN-22: 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 Föderalen Standardisierungsboards – 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.

KKN-23: 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 Föderalen Standardisierungsboards – die Selbstauskunft der Betreiber des IT-Standards und die aktuelle Releasehistorie daraufhin, ob die notwendige Stabilität und Reife des Standards erreicht ist.

3.11. Digitale Souveränität

KKN-24: 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	
Föderales Standardisierungsboard	Prüft das Betriebskonzept 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].

KKN-25: 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	
Föderales Standardisierungsboard	Prüft das Betriebskonzept des IT-Standards daraufhin, ob der dauerhafte oder zumindest sehr langfristige Betrieb gewährleistet ist.

KKN-26: Entspricht der IT-Standard den einschlägigen Vorgaben der föderalen Architekturrichtlinie?

Zuständigkeiten im Rahmen der Prüfung	
Föderales Architekturboard	Prüft – ggfs. zusammen mit Mitgliedern des Föderalen Standardisierungsboards – die Selbstauskunft der Betreiber des IT-Standards und ggfs. die funktionale Beschreibung daraufhin, ob der IT-Standard den einschlägigen Vorgaben der föderalen Architekturrichtlinie entspricht.

3.12. Marktakzeptanz

KKN-27: 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 Föderalen Standardisierungsboards – die Selbstauskunft der Betreiber des IT-Standards und Erkenntnisse des Standardisierungsradars, ob der IT-Standard von verschiedenen Anbietern/Lieferanten für unterschiedliche Implementierungen verwendet wird.

Kapitel 4. 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 IT-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 Marktstandard 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

vorgegeben. 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, dass 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, sowie
- technische Kriterien.

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

- **MUSS:** Kriterien dieser Verbindlichkeitsstufe müssen durch ein XÖV-Vorhaben und seinen IT-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-Profiles 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.

Bereitstellungspflichten	
XÖEV-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.
XÖEV-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.
XÖEV-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.
XÖEV-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.
Auskunftspflichten der entwickelnden und betreibenden Stellen	
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.
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.
Wiederverwendung	
XOEV-10 (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.
XOEV-16 (muss)	Bei fachlicher Eignung sollen XÖV-Standards die mit der XÖV-Bibliothek herausgegebenen Bausteine anstelle eigener Entwicklungen nutzen. Hierzu ist die im XÖV-Handbuch dargelegte Methodik anzuwenden.
Technische Kriterien	
XOEV-11 (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.
XOEV-12 (muss)	Die Modellierung der Datenstrukturen des XÖV-Standards muss in einem XÖV-Fachmodell unter Verwendung der XÖV-Modellierungssprache in der Notation <i>XÖV classic</i> oder <i>XÖV lite</i> erfolgen.
XOEV-13 (muss)	XÖV-Namens- und Entwurfsregeln müssen entsprechend ihrer Verbindlichkeit bei der Spezifikation eines 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.
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.

[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:

4.1. Bereitstellungspflichten

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

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.

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.

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 liegen das XÖV-Fachmodell, die XSD-Schemata und das Spezifikationsdokument des Standards vollständig und konsistent vor. Das XÖV-Fachmodell muss in der Notation <i>XÖV classic</i> (XMI-Format und proprietäres Format des genutzten UML-Modellierungswerkzeugs) oder <i>XÖV lite</i> (Format XML) vorliegen. Prüfinhalt: XÖV-Fachmodell, Spezifikationsdokument und zugehörige XSD-Schemata des Standards.

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.

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.

4.2. 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.

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.

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.

4.3. Wiederverwendung

Die Nutzung der mit der XÖV-Bibliothek bereitgestellten Bausteine und über das XRepository bereitgestellter Codelisten in XÖV-Standards unterstützt die standardübergreifende Interoperabilität und stellt damit einen zentralen Aspekt der XÖV-Konformität dar.

XOEV-10: 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 und Dokument "Zertifizierungsrelevante Begründungen". Prüfinhalt:Codelisten nutzende Datenstrukturen des Standards; Begründung eventueller Abweichungen.

XOEV-16: Bei fachlicher Eignung sollen XÖV-Standards die mit der XÖV-Bibliothek herausgegebenen Bausteine anstelle eigener Entwicklungen nutzen. Hierzu ist die im XÖV-Handbuch dargelegte Methodik anzuwenden.

Begründung: Die gemeinschaftliche Nutzung von Bausteinen verbessert die Interoperabilität und erleichtert die Implementierung.

Zuständigkeiten im Rahmen der Prüfung	
KoSIT	Prüfgrundlage:Im XRepository bereitgestelltes XÖV-Fachmodell und Dokument "Zertifizierungsrelevante Begründungen". Prüfinhalt:Bausteine und weitere Datenstrukturen des Standards; Begründung eventueller Abweichungen.

4.4. 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.

XOEV-11: 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.

XOEV-12: 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. Prüfinhalt: Fehlerfreie Verarbeitung des XÖV-Fachmodells durch den XGenerator und die XÖV-Produktionsumgebung. 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.

XOEV-13: XÖV-Namens- und Entwurfsregeln müssen entsprechend ihrer Verbindlichkeit bei der Spezifikation eines 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.

Begründung: Die Interoperabilität von XÖV-Standards soll bereits auf der Modellebene unterstützt werden. Die Anwendung der XÖV-Namens- und Entwurfsregeln leistet auf der einen Seite einen Beitrag zur korrekten Anwendung der XÖV-Modellierungssprache und stellt auf der anderen Seite die konkrete Umsetzung grundlegender 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.

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.

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

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

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 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 Verwaltungsdienstverzeichnis 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.

4.5. Prüfung der XÖV-Konformität

Die Abschnitt 4.5, „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.

Abkürzungsverzeichnis und Glossar

Verzeichnis der Akronyme und Abkürzungen	
BVA	Bundesverwaltungsamt
CAMSS	Common Assessment Method for Standards and Specifications
DITR	Deutsches Informationszentrum für technische Regeln
FITKO	Föderale IT-Kooperation
FRAND	Fair, Reasonable and Non-Discriminatory
KoSIT	Koordinierungsstelle für IT-Standards
MSP	Multi stakeholder Platform
NOOTS	Nationales Once Only technical System
SAK	Sicherer Anschlussknoten
XÖV	XML in der öffentlichen Verwaltung

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 wurde, 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

[CAMSS EIF] [CAMSS Assessment EIF Scenario](#) im Rahmen des "Interoperable Europe" Portals der Europäischen Kommission.

[CAMSS MSP] [CAMSS Assessment Multi-Stakeholder Platform \(MSP\) Scenario](#) im Rahmen des "Interoperable Europe" Portals der Europäischen Kommission.

[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

[IE CAMSS] [Common Assessment Method for Standards and Specifications](#) im Rahmen des "Interoperable Europe" Portals der Europäischen Kommission.

[IT-Staatsvertrag] [Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Länder](#)

[ITPLR 2024/05] [Beschluss 2024/05](#) des IT-Planungsrats zur Einrichtung des Föderalen IT-Standardisierungsboards.