Stellungnahme

Dezember 2025

Verordnung zur Bestimmung anderer Netze des Bundes zum Datenaustausch über das NOOTS im Anwendungsbereich des Onlinezugangsgesetz

Zusammenfassung

Wir begrüßen die zahlreichen Aktivitäten im Zuge der fortschreitenden Registermodernisierung. Vor diesem Hintergrund bietet das NOOTS-Netz einen Ansatz zur beschleunigten Umsetzung des OZG und zur flexibleren Gestaltung behördlicher IT-Anbindungen über öffentliche Telekommunikationsnetze. Gleichzeitig zeigt sich an einigen Stellen, dass für eine tragfähige und zukunftssichere Nutzung noch Anpassungen und Konkretisierungen notwendig sind.

Rolle und Grenzen intermediärer Komponenten

Die derzeitigen Einschränkungen in den Verwaltungsnetzen ergeben sich wesentlich aus Sicherheitsvorgaben, die aufgrund unzureichend geschützter Fachsysteme erforderlich sind. Intermediäre wie der sichere Anschlussknoten (SAK) sollen diese Defizite überbrücken und eine abgesicherte Kommunikation ermöglichen – auch für Onlineangebote. Diese Architektur ist nachvollziehbar, führt jedoch zu einer erheblichen Ausweitung der Komplexität. Daher sollte sie nicht als Dauerlösung verstanden werden, sondern nur so lange bestehen, bis Fachsysteme ein Sicherheitsniveau erreichen, das direkte und weniger reglementierte Kommunikationswege ermöglicht.

Absehbare Skalierungsgrenzen

Die in der TR-03176 beschriebene Schnittstellenlogik zwischen Registern und Intermediären schafft bereits jetzt eine beträchtliche Komplexität, die zudem von mehreren zentralen Systemen abhängt, deren endgültige Ausgestaltung noch offen ist. Dies wirft Fragen zur späteren Skalierbarkeit auf (weitere Anmerkungen zur

zukünftigen Nutzung des NOOTS-Netz in Abschnitt »Evaluierungsbedarf und langfristige Perspektive«).

Einordnung im Kontext bestehender Netze und Cloud-Strategien

Die im Entwurf beschriebene fehlende Konnektivität dürfte teilweise darauf zurückzuführen sein, dass nicht alle Behörden umfassend an das Verbindungsnetz angebunden sind. Dass das NOOTS-Netz auf öffentlichen Telekommunikationsnetzen aufsetzt und damit Architekturentscheidungen zwischen On-Premise- und Cloud-Komponenten offenlässt, ist grundsätzlich positiv. Allerdings weisen die technischen Richtlinien des BSI hohe Erwartungen an die Verfügbarkeit beteiligter Systeme aus, die durch reine Internetanbindungen – Stichwort »Best Effort« – nicht immer erfüllt werden können. Daher sollte geprüft werden, ob nicht ein zweiter, unabhängiger Übertragungsweg erforderlich ist.

Notwendige Präzisierungen im Verordnungstext

Der Verordnungsentwurf benötigt aus unserer Sicht noch einzelne Präzisierungen, um Interpretationsspielräume zu minimieren:

Die Formulierung, dass »Signale« (§ 3) übertragen werden, sollte durch eine eindeutige Bezugnahme auf Datenübertragung wie den XÖV-Standard ersetzt werden. Ebenso bleibt offen, was konkret unter einer »sachgerechten Einbindung« der technischen Einrichtung zu verstehen ist, da hierfür weder technische noch betriebliche Kriterien genannt werden. Sinnvoll wäre hier die explizite Bezugnahme auf BSI-Vorgaben. Positiv ist hingegen, dass die Verschlüsselung an einschlägigen TRs des BSI ausgerichtet wird, was eine langfristig robuste Kryptografie – einschließlich postquanten-sicherer Verfahren – ermöglicht. Es sollte klargestellt werden, dass sich der Stand der Technik aus diesen Richtlinien ableitet.

Verweis auf IT-Planungsratbeschlüsse

Der in der Verordnung zitierte Beschluss »2022/39« bezieht sich nicht auf die Nutzung intermediärer Plattformen im nationalen Kontext. Vielmehr legt Beschluss 2022/34 fest, dass für das EU-OOTS intermediäre Plattformen verwendet werden sollen. Für das nationale NOOTS wird dies nicht gefordert. Hier bedarf es eventuell einer Korrektur des Verweises, um Missverständnissen vorzubeugen.

Anforderungen an Authentifizierung und Überwachung

Die Verwendung des Begriffs »Multi-Faktor-Authentifizierung« in Abschnitt B »Besonderer Teil«, Unterpunkt »zu §3 Absatz 3« im Zusammenhang mit der Kommunikation zwischen Systemen ist fachlich nicht passend, da klassische Mehrfaktormodelle auf Personen ausgerichtet sind. Außerdem kommt der vorgesehenen Monitoring-Funktion eine zentrale sicherheitsrelevante Rolle zu, da sie bei Auffälligkeiten Berechtigte oder Anschlussknoten temporär isolieren soll. Diese

Bedeutung sollte sich in klaren, verbindlichen Anforderungen widerspiegeln, beispielsweise auf Basis eines IT-Grundschutz-Schutzniveaus »hoch«.

Definition des Standes der Technik

Die Verordnung sollte eindeutig festlegen, dass der Stand der Technik anhand der vom BSI veröffentlichten Normen und der künftig bereitgestellten Stand-der-Technik-Bibliothek zu bestimmen ist. Dies schafft sowohl Rechtssicherheit als auch ein einheitliches technisches Fundament für alle Beteiligten.

Klärungsbedarf zu den berechtigten Stellen nach § 2

Nach § 2 NOOTSNetzV sind alle öffentlichen Stellen nach § 1 OZG zum Datenaustausch berechtigt. Die Gesetzesbegründung (S. 10) sieht jedoch vor, dass der Begriff der Verwaltungsleistung weit auszulegen ist. Dabei wird allerdings nicht weiter erläutert, was dies letztlich bedeutet und was hiervon umfasst ist. Mit Blick auf das OZG dürfte sich die Regelung primär an Onlinedienste und Fachverfahren von öffentlichen Stellen als nachweisabrufende Stellen (Data Consumer) richten, da diese gegenüber den Nutzenden die Verwaltungsleistungen erbringen. Unklar bleibt jedoch, ob auch nachweisliefernde Stellen (Data Provider) von § 2 NOOTSNetzV erfasst werden. Konsequenterweise müssen sich auch diese an das NOOTS anschließen (siehe beispielsweise die Verpflichtungen aus dem Identifikationsnummerngesetzes [IDNrG]). Es wäre kaum nachvollziehbar, wenn sich diese Stellen – im Gegensatz zu den nachweisabrufenden Stellen – weiterhin über das Verbindungsnetz anbinden müssten, anstatt das mit der Verordnung eingeführte NOOTS-Netz zu nutzen. Zumal die Technische Richtlinie ausdrücklich vorsieht, dass auch sie einen sogenannten sicheren Anschlussknoten (SAK) betreiben müssen. Eine Vereinheitlichung der Begriffsdefinitionen über die Dokumente hinweg würde hier bereits für eine größere Klarheit sorgen.

Adressierungsfragen und IPv6

Es sollte konsequent auf IPv6 gesetzt werden, insbesondere bei neu entwickelten Komponenten wie dem sicheren Anschlussknoten.

Evaluierungsbedarf und langfristige Perspektive

Da das NOOTS-Netz eingeführt wird, weil das Verbindungsnetz die Anforderungen derzeit nicht erfüllen kann, besteht die Möglichkeit, dass später erneut Anpassungen an der Netzarchitektur notwendig werden. Um unnötige Umstellungen zukünftig zu vermeiden, sollte daher eine Evaluierungsvorschrift in die Verordnung aufgenommen werden, die eine Bewertung der langfristigen Eignung des NOOTS-Netzes ermöglicht.

Anhang zu den technischen Richtlinien BSI TR-03176 und TR-03190

Zusammenfassung

Die Technischen Richtlinien schaffen eine erste Grundlage für IT-Sicherheit, während systematische Qualitätssicherungsmaßnahmen für den operativen Betrieb noch weitergehender Konkretisierung bedürfen.

Identifizierte Anforderungsbereiche

Die nachfolgende tabellarische Analyse identifiziert sieben kritische Bereiche für die Produktionsreife sowie fünf notwendige Ergänzungsbereiche:

Identifizierte Lücke	Erwartete Auswirkung auf Produktivbetrieb
Fehlerklassifikation und Monitoring Es fehlt eine standardisierte, maschinenlesbare Fehlerklassifikation, die konsistentes Fehlerhandling über alle Systemkomponenten ermöglicht.	Ohne einheitliche Fehlerklassifikation ist ein automatisiertes Monitoring nicht möglich. Dies erschwert die Fehlerdiagnose erheblich und gefährdet die Einhaltung von Service-Level-Vereinbarungen.
Test- und Abnahmestrategie Die Dokumente enthalten keine konkreten Anforderungen an Integrationstests, Performance-Tests oder Sicherheitstests. Ebenso fehlen noch klare Abnahmekriterien für die Produktionsfreigabe.	Es sind unkalkulierbare Ausfälle und Sicherheitslücken im Produktivbetrieb zu erwarten. Die Definition messbarer Abnahmekriterien ist für die Qualitätssicherung daher unerlässlich.
Service Level Objectives Es existieren noch keine messbaren Qualitätsziele für Verfügbarkeit, Performance und Datenintegrität. Dies betrifft sowohl das Monitoring als auch die Reporting-Anforderungen.	Ohne definierte Service Level Objectives sind SLA-Vereinbarungen nicht durchsetzbar und eine objektive Qualitätsmessung nicht möglich. Kapazitätsplanung und kontinuierliche Verbesserung werden so erheblich erschwert.
Incident Management Die Dokumente enthalten keine Vorgaben für Incident-Klassifikation, Eskalationswege, Zeitvorgaben zur Fehlerreaktion oder operative Prozesse für den Störungsfall.	Lange Ausfallzeiten bei Störungen und inkonsistente Fehlerbehandlung sind zu erwarten. Der Aufbau entsprechender strukturierter Prozesse erfordert erheblichen Vorlauf.

Identifizierte Lücke	Erwartete Auswirkung auf Produktivbetrieb
Datenqualität und Nachvollziehbarkeit Während sicherheitsorientierte Protokollierung und Schema-Validierung vorhanden sind, fehlen Anforderungen an umfassende Datenqualitätsprüfung und qualitätsorientiertes Monitoring.	Dies birgt erhebliche DSGVO-Risiken. Insbesondere die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO erfordert vollständige Nachvollziehbarkeit aller Datenverarbeitungsvorgänge.
Kapazitäts- und Skalierungsplanung Die Dokumente enthalten keine Angaben zu erwarteten Lastszenarien, Skalierungsgrenzen oder erforderlichen Kapazitätsreserven.	Performance-Degradation unter Last und Systemausfälle bei unerwartetem Nutzerwachstum gefährden die Akzeptanz des Systems. Eine fundierte Dimensionierung ist komplex und zeitaufwendig.
Disaster Recovery und Business Continuity Backup und Recovery werden nur oberflächlich erwähnt. Es fehlen konkrete Angaben zu Recovery-Zielen, Backup-Strategien, Failover-Prozessen und Test-Verfahren.	Das Risiko großer Datenverluste und tagelanger Systemausfälle besteht. Die Entwicklung einer robusten Disaster-Recovery-Strategie erfordert eine umfassende Planung.

Ergänzende Anforderungsbereiche

Anforderungsbereich	Erläuterung
Interoperabilität und Konformität	Die Dokumente enthalten keine Anforderungen für Konformitätstests oder Zertifizierungsverfahren.
Security Operations	Über die definierten Sicherheitsanforderungen hinaus fehlen Vorgaben zur kontinuierlichen Überwachung und Reaktion auf Sicherheitsvorfälle. Der Aufbau entsprechender Security-Operations-Capabilities ist zeitintensiv.
Governance und Change Management	Es fehlen klare Definitionen von Entscheidungsgremien und Change-

Anforderungsbereich	Erläuterung
	Management-Prozessen. Insbesondere Vorgaben zur Rückwärtskompatibilität und Versionskontrolle sind für die Marktreife relevant. Dies betrifft sowohl das Monitoring als auch den Reporting-Anforderungen.
Dokumentation und Schulung	Neben den technischen Spezifikationen fehlen Anforderungen an operative Dokumentation wie Betriebshandbücher und Troubleshooting-Guides. Die Erstellung qualitativ hochwertiger Dokumentationen ist aufwendig.
Compliance und Auditing	Es fehlen explizite Anforderungen für regelmäßige Compliance-Audits, Datenschutz-Folgenabschätzungen und IT-Grundschutz-Zertifizierung. Die Umsetzung regulatorischer Anforderungen erfordert spezialisiertes Know-how.

Risikobewertung und Schlussfolgerung

Die BSI-Richtlinien TR-03176 und TR-03190 schaffen eine Grundlage für die IT-Sicherheit des NOOTS. Die identifizierten sieben kritischen Lücken erfordern jedoch detaillierte Spezifikation vor dem Produktivbetrieb, denn sie bringen eine Reihe von Risiken mit sich. So ist ohne klar definierte Betriebsprozesse damit zu rechnen, dass Störungen zu längeren Ausfallzeiten führen. Zudem kann eine unzureichende Nachvollziehbarkeit bei der Verarbeitung personenbezogener Daten erhebliche Compliance-Probleme bis hin zu Verstößen gegen die DSGVO nach sich ziehen. Auch die Leistungsfähigkeit der Systeme ist gefährdet, da ohne eine systematische Kapazitätsplanung die Stabilität unter Produktionslast nicht gewährleistet werden kann. Darüber hinaus steigt das Risiko von Datenverlusten, wenn keine umfassende Strategie für Desaster-Recovery und Wiederanlaufkonzepte vorliegt. Fehlende Standards für die Interoperabilität bergen außerdem die Gefahr einer zunehmenden Fragmentierung. Zusammengenommen haben die identifizierten Risiken das Potential, die Erfolgsaussichten einer reibungslosen und nachhaltigen Implementierung der Registermodernisierung zu schmälern.

nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Esther Steverding | Bereichsleiterin Public Sector
T +49 30 27576-216 | e.steverding@bitkom.org

Verantwortliches Bitkom-Gremium

AK Digitale Verwaltung