DATABUND
Bundesverband der mittelständischen IT- Dienstleister und Softwarehersteller für den öffentlichen Sektor e. V.

Seeburger Str. 25
13581 Berlin

Tel.: +49 30 220 661 600
Fax: +49 30 220 661 609
E-Mail: info@databund.de

DATABUND-Stellungnahme zum Referentenentwurf

NOOTS-Netz-Verordnung

Verbunden mit der Bestimmung des NOOTS-Kommunikationsverbunds als ein "weiteres Netz des Bundes" stellt dieser Verordnungsentwurf mit den TRs deutlich heraus, dass es in Deutschland einer Bund- und Länderübergreifenden Governance des Datenaustauschs innerhalb der Verwaltung und mit der Verwaltung bedarf, die bisher nicht definiert worden ist. Leider bleiben der Entwurf und auch die TRs hinter dieser Erwartung zurück und bedürfen deutlicher Präzisierungen und Schärfungen, damit beteiligte Stellen nicht alleine ohne Hilfestellungen und Austauschmöglichkeiten vor schier unlösbaren Aufgaben stehen.

Innerhalb des NOOTS-Kommunikationsverbunds wird nicht auf eine deutliche Trennung zwischen Inhaltsdaten auf der Verfahrensebene und dem davon zu trennenden sicheren Transport der Daten unterschieden. Zusätzlich wird der NOOTS Kommunikationsverbund künstlich mit dem Verbindungsnetz gleichgesetzt, um den Anforderungen des ID-Nr-Gesetzes zu genügen. Denn dort ist festgelegt, dass nur ein Netz des Bundes und der Länder im Sinne des Verbindungsnetzes zum Austausch der ID-Nr und mit ihr verbundenen Nachweisdaten genutzt werden darf. Die Komponenten (SAK, RDN ,VS, IAM für Behörden) der NOOTS-Kommunikationsinfrastruktur sind nicht auf der Ebene des Verbindungsnetzes, sondern auf der Anwendungsebene angesiedelt. Deshalb ist die Definition in §3 (1) des Entwurfs zur NOOTSNetzV keine passende Definition des NOOTS-Kommunikationsverbunds, sondern eher abzielend auf ein physisches IT-Netz. Auch die Betrachtung der Alternativen vergleicht das anwendungsunabhängige Verbindungsnetz von Bund und Ländern mit den Anforderungen einer gesicherten Datenübertragung auf Anwendungsebene. Diese Begründung geht deshalb auch nicht auf etablierte Kommunikationsstrukturen der öffentlichen Verwaltung, wie OSCI-Transport in Verbindung mit dem DVDV und optional XTA2, ein, obwohl ein Großteil der Anforderungen, die in der NOOTS-Kommunikationsinfrastruktur gefordert werden, direkt

mittels OSCI-Transport in Verbindung mit DVDV und optional XTA2 erfüllt werden könnten. Zudem wird auch der internationale Standard ebMS 3.0/AS4 nicht betrachtet, der innerhalb der EU als eDelivery Building Block zur sicheren Datenübertragung empfohlen und für sehr unterschiedliche Geschäftsprozesse mit der öffentlichen Verwaltung eingesetzt wird.

Bei E.3 Erfüllungsaufwand der Verwaltung wird davon ausgegangen, dass alle im Kontext des OZG an das NOOTS anzuschließenden öffentlichen Stellen schon über einen Telekommunikationsanschluss verfügen, der den noch unbekannten Verfügbarkeits- und Lastanforderungen genügt. Insbesondere in den TR-Entwürfen wird davon ausgegangen, dass die fachverantwortlichen und betriebsverantwortlichen Stellen für die Sicheren Anschlussknoten (SAK) in ihrer Verantwortung ermitteln können, wie die Lastverteilung aussieht, um die entsprechende Skalierung ihrer Systeme zu planen. Hier wird also voraussichtlich ein Mehraufwand auf Seiten der öffentlichen Verwaltung in den dezentralen Strukturen entstehen, der in der Verordnung außer Acht gelassen wird.

Insbesondere wird der Verantwortungsbereich des Empfängers von fachlichen Inhaltsdaten bis in die Internet-Zone (dort ist der SAK verortet) ausgedehnt, um die durchgehende Verschlüsselung der Fachdaten schon am SAK aufzuheben. Es erfolgt also keine Ende-zu-Ende-Verschlüsselung zwischen den fachlich verantwortlichen Systemen, sondern nur eine Punkt-zu-Punkt-Verschlüsselung auf einzelnen Transportstrecken. Dies bietet das Risiko, dass an dezentralen Punkten des NOOTS-Kommunikationsverbunds unerwünschte Profilbildungen ermöglicht werden, wenn die SAK bspw. mandantenfähig für Online-Dienste aus unterschiedlichen fachlichen Ressorts eingesetzt werden.

Der Begriff Multi-Faktor-Authentifizierung in der Begründung zu § 3 Absatz 3 ist für die Absicherung einer Maschine-zu-Maschine-Kommunikation nicht passend, weil dieser für gewöhnlich für die Authentifizierung von Menschen an Computer-Systemen verwendet wird. Hier sollte mindestens ein passenderer Begriff für die Zusicherung von Eigenschaften über Token gewählt werden.

Innerhalb der Entwürfe der technischen Richtlinien werden einige Aspekte benannt, die deutlich ausführlicher und präziser beschrieben werden müssen, um zu wirksamen Sicherheitsanforderungen beizutragen:

- Im NOOTS soll ein zentrales Monitoring aufgebaut werden, das nicht nur Protokolldaten sammelt, sondern auch auswertet und automatisiert teilnehmende Stellen aus dem NOOTS ausschließen kann. Dies geht weit über die übliche Definition des Monitorings hinaus. Außerdem ist nicht ersichtlich, welche Fehlerklassen es für Störungen gibt und wo spezifiziert werden soll, was in den Protokolldaten enthalten ist.
- Die betriebsverantwortlichen Stellen müssen einen SAK betreiben und sich auf dessen sichere Implementierung verlassen, ohne diese prüfen zu können. Es ist lediglich vorgeschrieben, eine Code-Signatur zu prüfen. Im Kontext einer Cloud-Anwendung muss sonst aber auch jedes bereitgestellte Binary auf Schwachstellen und Schadsoftware geprüft werden, bevor es eingesetzt werden darf.
- Es gibt keine Aussagen dazu, ob vor dem produktiven Anschluss an das NOOTS erst ein Testsystem oder Staging-System in einer NOOTS-Testumgebung in Betrieb genommen werden muss. Bei so einem großen Vorhaben sollte dies ein Standard-Vorgehen sein.
- Bzgl. Business Continuity und Umgang mit Sicherheitsvorfällen wird nicht definiert, welche Recovery-Ziele und Backup-Strategien und Failover-Prozesse einzuhalten sind. Es besteht also das Risiko, dass die OZG-Antragsverfahren tagelang von Störungen betroffen sind, weil diese Prozesse nicht ausreichend definiert werden.
- Weder die Verordnung noch die TR-Entwürfe machen Aussagen zur Governance und Entscheidungsstrukturen. Es werden keine Vorgaben gemacht, wie mit Rückwärtskompatibilität und Versionskontrolle umgegangen werden soll. Es finden sich auch keine Aussagen zu Release-Zyklen und Test- sowie Freigabe-Prozessen. Ein Betriebskonzept für die beteiligten XÖV-Standards und die SAK-Software sind essentiell für die Betriebsplanung der fachverantwortlichen und betriebsverantwortlichen Stellen.

Für Rückfragen und weitere Informationen stehen wir gerne zur Verfügung.

Berlin, den 13.12.2025

Der DATABUND-Vorstand