Januar 2026

4. Konsultationsrunde zu ausgewählten NOOTS-Architekturdokumenten

Nachfolgend finden Sie die auf OpenCoDE eingereichten Antworten zu den einzelnen Leitfragen.

Dokument	Leitfragen
AD-NOOTS-05 Grobkonzept IAM für Behörden	**Leitfrage 1:** Sind die Gründe für die Einschränkung des Funktionsumfangs gegenüber dem Stand Q3/Q4/2024 durch den Ausschluss der Pflege von NOOTS-Teilnehmern u. dezentralen NOOTS-Komponenten sowie deren Übertragung in ein Pflegesystem (DAMAS) verständlich? **Hintergrund der Frage:** Gegenüber dem Konzeptionsstand 2024 sind umfassende fachliche Funktionen in das Datenmanagementsystem (DAMAS) überführt worden, insbesondere die Pflege von NOOTS-Teilnehmern. **Zweck der Frage:** Verständnis für den Neuentwurf IAMfB etablieren. **Antwort:** Es ist ausreichend dargestellt, dass die Pflege der Informationen jetzt im DAMAS erfolgt.
AD-NOOTS-05 Grobkonzept IAM für Behörden	**Leitfrage 2:** Ist die Rolle des IAMfB innerhalb des Nachweisabrufprozesses nachvollziehbar? **Hintergrund der Frage:** Das IAMfB erfüllt mehrere Funktionen für den Nachweisabrufprozess neben der reinen Autorisierung durch das Zugriffstoken. **Zweck der Frage:** Die Gesamtperspektive sowie übergreifende Zusammenhänge im NOOTS sollen adressiert sein. **Antwort:** Ja, die Rolle ist nachvollziehbar. Es sollte allerdings noch mit Blick auf das Zugriffstoken geklärt werden, ob die Art und Weise der Erzeugung wie beschrieben geeignet ist. Es wird beschrieben, dass das Zugriffstoken nicht an eine spezifische Anfrage gebunden ist, aber nur auf eine spezifische Anfrage mittels eines Anfragetoken ausgestellt wird. In NOOTS-1290 wird beschrieben, dass das Zugriffstoken das Anfragetoken beinhaltet. Das erscheint widersprüchlich, da es hier eine direkte Verbindung zwischen Zugriffstoken und Anfragetoken gibt, obwohl das Zugriffstoken natürlich auch für beliebig viele weitere Nachweisanforderungen während seiner Gültigkeit genutzt werden kann. Hier sollten die Formulierungen und Abhängigkeiten bitte überprüft werden. Auch ein expliziter Verweis auf die im OAuth2-Umfeld bekannten Refreshtoken und das diese hier nicht ausgestellt werden dürfen, inklusive Begründung, ist wünschenswert.

Dokument	Leitfragen
AD-NOOTS-05 Grobkonzept IAM für Behörden	**Leitfrage 3:** Sind die Maßnahmen, die das IAMfB im Fall eines Sicherheitsvorfalls ergreift, verständlich und nachvollziehbar? **Hintergrund der Frage:** Das IAMfB erfüllt als Policy Enforcement Point (PEP) eine wichtige Sollbruchstelle. **Zweck der Frage:** Bedeutung des Einsatzes als PEP. **Antwort:** Die Gründe für eine Sperre sind zu wenig detailliert dargestellt. Es ist unklar, wie eine Sperre ausgeführt wird, v.a. ist nicht ersichtlich, wie der Sperrmechanismus vor missbräuchlichen Gebrauch geschützt ist. Des Weiteren fehlen Erläuterungen ob und ggf. wie weitere Maßnahmen folgen, z.B. die Information von Betroffenen und Recoverystrategien. Zudem ist nur die Sperrung der SAK-DC thematisiert. Es stellt sich jedoch die Frage, ob auch andere Komponenten (SAK-DP, oder sogar Vergabestellen) gesperrt werden können. Hier bedarf es einer Ausführung bzgl. der Entscheidungen für oder gegen die Möglichkeit der Sperrung der NOOTS Komponenten und NOOTS-Teilnehmer. Des Weiteren liest es sich, als ob FPE-005 immer dann auftreten kann, wenn ein Data Consumer im DAMAS gepflegt wurde, aber das IAMfB die aktuellen Daten noch nicht vom DAMAS abgerufen hat. Die Frage ist aus unserer Sicht noch offen, wie dem vorgebeugt wird.
AD-NOOTS-08 Grobkonzept Vermittlungsstelle	**Leitfrage 1:** Sind der Architekturansatz und die Motivation bzw. Rahmenbedingungen verständlich, nachvollziehbar und vollständig beschrieben? **Hintergrund der Frage:** Die generelle Verständlichkeit und Vollständigkeit des Konzepts sind wichtig. **Zweck der Frage:** Falls erforderlich können Ergänzungen oder weitere Erklärungen aufgenommen werden. **Antwort:** Die Verständlichkeit ist grundsätzlich gegeben, die abstrakte Berechtigungsprüfung sollte einmal zusammenhängend definiert und beschrieben werden, damit das Prinzip klar verständlich wird.
AD-NOOTS-08 Grobkonzept Vermittlungsstelle	**Leitfrage 2:** Ist die Einbindung der Vermittlungsstelle in den Nachweisabrufprozess sowie das Zusammenwirken mit anderen Systemen verständlich, nachvollziehbar und vollständig beschrieben? **Hintergrund der Frage:** Die Vermittlungsstelle spielt im Nachweisabrufprozess eine wesentliche Rolle. Zusammenhänge mit anderen Systemen sind für die Vermittlungsstelle und für andere Systeme relevant.

Dokument	Leitfragen
	Zweck der Frage: Die Gesamtperspektive sowie übergreifende Zusammenhänge im NOOTS sollen adressiert sein. **Antwort:** Es ist nicht ersichtlich, warum nicht geprüft wird, ob der DC eine Berechtigung zum Abruf der Daten der jeweiligen betroffenen Person erhalten hat. Dies widerspricht den in 2.2 aufgeführten Zielen.
AD-NOOTS-08 Grobkonzept Vermittlungsstelle	**Leitfrage 3:** Ist die Beschreibung der Durchführung der Berechtigungsprüfung verständlich, nachvollziehbar und vollständig? **Hintergrund der Frage:** Wesentliches Ziel der Vermittlungsstelle ist die Durchführung der Berechtigungsprüfung. Dies soll im Konzept nachvollziehbar beschrieben sein. **Zweck der Frage:** Transparenz und Verständlichkeit der Umsetzung der (insbes. gesetzlich vorgeschriebenen) abstrakten Berechtigungsprüfung sollen erreicht werden. **Antwort:** Wie wird sichergestellt, dass ein kompromittierter oder missbräuchlicher DC nicht den Anlass falsch angibt, um sich eine positive Berechtigungsprüfung zu «erschleichen"? Und in welchem Zyklus werden die Inhalte aus dem DAMAS gespiegelt?
AD-NOOTS-08 Grobkonzept Vermittlungsstelle	**Leitfrage 4**: Gibt es weitere Inhalte, Aspekte oder Ergänzungen, die Sie beschrieben wünschen? **Hintergrund der Frage:** Das Konzept soll den Lesern alle erforderlichen Informationen liefern und keine Unklarheiten oder Lücken aufweisen. **Zweck der Frage**: Lesern, auch mit verschiedenen Hintergründen, soll ein bestmögliches Verständnis ermöglicht werden. **Antwort:** NOOTS-1008: Die Vermittlungsstelle MUSS Änderungen an den Abrufberechtigungen protokollieren. Unserem Verständnis nach sollte das im DAMAS passieren.
AD-NOOTS-06 Grobkonzept Intermediäre Plattform	**Leitfrage 1:** Ist die Darstellung der Ziele der IP – unter Berücksichtigung ihrer Rollen als Data Consumer und Data Provider im grenzüberschreitenden Nachweisabruf – klar, verständlich und eindeutig? **Hintergrund der Frage:** Die grundlegenden Ziele und Rollen der IP müssen für die Leserinnen und Leser klar und verständlich beschrieben sein. **Zweck der Frage:** Die Frage hilft, gezieltes Feedback zu Verständlichkeit und Klarheit der Ziele und Rollen der IP zu erhalten.

Dokument	Leitfragen
	Antwort: Es wird klar, was die Kernaufgabe der IP ist und wie der Nachweisaustausch funktionieren soll. Da der eigentliche Abruf des Nachweises für den DC nicht so relevant ist, wäre es nützlich zusätzlich die Unterschiede beim Abruf des Nachweises über die IP darzustellen, falls die Komplexität nicht durch die IP gebündelt und reduziert wird.
AD-NOOTS-06 Grobkonzept Intermediäre Plattform	**Leitfrage 2:** Ist der Ablauf der Abrufe nationaler Nachweise aus dem europäischen Ausland sowie europäischer Nachweise aus Deutschland verständlich und nachvollziehbar dargestellt? **Hintergrund der Frage:** Die Beschreibungen des grenzüberschreitenden Nachweisabrufs wurden seit der letzten Veröffentlichung überarbeitet. **Zweck der Frage:** Die Frage hilft sicherzustellen, dass der grenzüberschreitende Nachweisabrufprozess verständlich ist und alle relevanten Schritte berücksichtigt wurden. **Antwort:** s.o.
AD-NOOTS-06 Grobkonzept Intermediäre Plattform	**Leitfrage 3:** Deckt die Darstellung der funktionalen und nicht-funktionalen Anforderungen an die IP aus Ihrer Sicht alle für das Grobkonzept relevanten Aspekte korrekt und vollständig ab? **Hintergrund der Frage:** Die Anforderungen wurden seit der letzten Veröffentlichung konsolidiert. **Zweck der Frage:** Die Frage hilft zu verifizieren, dass alle Anforderungen vollständig erfasst sind. Ggf. sollen mögliche Lücken identifiziert werden. **Antwort:** s.o.
AD-NOOTS-06 Grobkonzept Intermediäre Plattform	**Leitfrage 4:** Ist die Darstellung der Fehlerbehandlung und der Fehlerszenarien in der IP – unter Berücksichtigung von Anhang A: Fehlermapping – nachvollziehbar und verständlich ausgeführt? **Hintergrund der Frage:** Der Anhang wurde seit der letzten Veröffentlichung im Dokument ergänzt. **Zweck der Frage:** Die Frage hilft sicherzustellen, dass die neue Darstellung verständlich ist und Verbesserungspotenziale zu erkennen. **Antwort:** s.o.

Dokument	Leitfragen
AD-NOOTS-06 Grobkonzept Intermediäre Plattform	**Leitfrage 5:** Gibt es weitere Inhalte, Aspekte oder Ergänzungen, zu denen Sie sich eine Beschreibung wünschen? **Hintergrund der Frage:** Das Konzept soll den Leserinnen und Lesern alle erforderlichen Informationen liefern und keine Unklarheiten oder Lücken aufweisen. **Zweck der Frage:** Die Frage hilft sicherzustellen, dass keine wesentliche Aspekte unberücksichtigt sind. **Antwort:** s.o.
BD-NOOTS-05 White Paper Reifegradunabhängiger Nachweisabruf	**Leitfrage 1:** Sind die grundlegenden fachlichen Festlegungen, insbesondere die Definition eines Nachweistyps als Baumstruktur von Datenfeldern, klar, verständlich und eindeutig? **Hintergrund der Frage:** Die fachlichen Festlegungen bilden die Basis für alle darauffolgenden Überlegungen und sollten daher klar und verständlich beschrieben sein. **Zweck der Frage:** Die Frage hilft zu verstehen, ob die fachlichen Festlegungen verständlich sowie zielführend sind. **Antwort:** Es ist klar wie der Nachweistyp definiert wird. Unklar ist jedoch noch der Umgang mit dem Attribut »Abrufberechtigung«. Auch gibt es keine Vergleiche und Bezüge zu aktuell existierenden Standards (FIM mit XDatenfelder, XÖV). Eine Nachnutzung mittels FIM wäre wünschenswert. Uns beschäftigt die Frage, warum diese nicht aufgeführt sind. Hinweis: Hier würden doppelte Strukturen aufgebaut, die dann wieder gemappt werden müssen. Eine Nachnutzung mittels FIM würde den Entwicklungsprozess verschlanken da FIM-Bausteine direkt nachgenutzt würden.
BD-NOOTS-05 White Paper Reifegradunabhängiger Nachweisabruf	**Leitfrage 2:** Ist die Konfigurationssicht, d.h. insbesondere die Beschreibung der Pflegeprozesse, verständlich, nachvollziehbar und vollständig? **Hintergrund der Frage:** Die Konfigurationssicht erfolgt vorgelagert und ist die Grundlage für die Laufzeitsicht und sollte daher verständlich, nachvollziehbar und vollständig beschrieben sein. **Zweck der Frage:** Die Frage hilft zu verstehen, ob hierzu noch weitere Ausführungen notwendig sind. **Antwort:** Wie erfolgt das Mapping zwischen Registerdaten und Nachweisdatenfeldern? Wie wird sichergestellt, dass alle Register den Nachweis umsetzen, wer prüft eigentlich die Nachweise bzw. wie wird sichergestellt, dass nur berechtigte Nachweise abgerufen werden?

Dokument	Leitfragen
BD-NOOTS-05 White Paper Reifegradunabhängiger Nachweisabruf	**Leitfrage 3:** Ist die Laufzeitsicht, d.h. insbesondere der Ablauf eines reifegradunabhängigen Nachweisabrufs im NOOTS inklusive der Rollen der einzelnen NOOTS-Komponenten und der NOOTS-Teilnehmer, verständlich, nachvollziehbar und vollständig beschrieben? **Hintergrund der Frage:** Das Whitepaper ist die Basis für zukünftige Anpassungen in den AD-NOOTS. Daher sollte insbesondere der (um Reifegradunabhängigkeit erweiterte) Nachweisabrufprozess klar beschrieben sein. **Zweck der Frage:** Die Frage hilft dabei, die zukünftigen Anpassungen der AD-NOOTS auf ein stabiles Fundament zu stellen. **Antwort:** Die Darstellung als Laufzeitdiagramm wäre wünschenswert. Wie wird der Reifegrad des Nachweises übergeben?
BD-NOOTS-05 White Paper Reifegradunabhängiger Nachweisabruf	**Leitfrage 4:** Gibt es weitere Inhalte, Aspekte oder Ergänzungen, zu denen Sie sich eine Beschreibung wünschen? **Hintergrund der Frage:** Das Konzept soll den Leserinnen und Lesern alle erforderlichen Informationen liefern und keine Unklarheiten oder Lücken aufweisen. **Zweck der Frage:** Die Frage hilft sicherzustellen, dass keine wesentliche Aspekte unberücksichtigt sind. **Antwort:** Umgang mit den Unterschiedlichen Reifegraden: Ist es erlaubt die Nachweise mit Reifegrad B mittels KI in den Reifegrad C zu bringen? Wie wird mit dem Thema Barrierefreiheit umgegangen, v.a. Reifegrad B? Wie wird mit einem Nachweis im Reifegrad B umgegangen, wenn es keinen Standard für den Reifegrad C gibt, da hier dann die Struktur der gelieferten Daten fehlt? Es werden Begrifflichkeiten wie Registertypenverantwortliche und fachlich Verantwortliche mit Vollzugszuständigkeiten genannt. Handelt es sich dabei um Einzelpersonen, Behörden, Abteilungen, Unternehmen, etc.? Und wie wird entschieden, wer diese Verantwortlichkeiten erhält? Eine Aufstellung und Beschreibung wären zur Klärung hilfreich.
BD-NOOTS-01 White Paper Zero Trust im NOOTS	**Leitfrage 1:** Sind das im Dokument dargestellte Paradigma Zero Trust sowie die daraus abgeleiteten Designprinzipien insgesamt verständlich und nachvollziehbar? **Hintergrund der Frage:** Das White Paper stellt ein Grundlagenkonzept auf einer abstrakten Ebene mit neuen Aspekten für NOOTS vor, das für einen weiteren Leserkreis gedacht ist. Die allgemeine Verständlichkeit ist eine Basisanforderung an das Dokument. **Zweck der Frage:** Beschreibung verbessern/vereinfachen/ergänzen

Dokument	Leitfragen
	Antwort: Laufzeitdiagramm: In Kapitel 1.3 wird der Ablauf eines Nachweisabrufs schrittweise erläutert. Die Abfrage des Zugrifftokens bei der Vermittlungsstelle wird laut dem Dokument «AD-NOOTS-08 Grobkonzept Vermittlungsstelle" allerdings im Rahmen des Nachweisabrufs durch den SAK-DC getriggert. Der Prozess, wie er hier im Dokument «D-NOOTS-01 White Paper Zero Trust im NOOTS" beschrieben ist, sieht vor, dass der Zugriffstoken von der Vermittlungsstelle geholt wird, dann der Nutzer zur Re-Authentifizierung geleitet wird und dann erst der Nachweisabruf an den DP geschickt wird. Hier stellt sich die Frage, wie das funktionieren soll ?
BD-NOOTS-01 White Paper Zero Trust im NOOTS	**Leitfrage 2:** Widersprechen die im Dokument genannten Sicherheitsziele des NOOTS den Ihnen bekannten Sicherheitszielen im Kontext von NOOTS? **Hintergrund der Frage:** Die im Dokument beschriebenen Ziele sind weitestgehend von den Zielen der NOOTS-Teilnehmer und -Komponenten abgeleitet und sollten über alle Elemente konsistent sein. **Zweck der Frage:** Frühzeitige Erkennung von grundlegenden Konflikten. **Antwort:** Das Prinzip der minimalen Privilegien wird derzeit nicht eingehalten, da der DC grundsätzlich alle Nachweise abrufen kann – auch solche, die für das jeweilige Antragsverfahren gar nicht erforderlich sind. Besonders bei umfangreichen Onlinediensten ist das kritisch, weil diese häufig eine Abrufberechtigung für eine große Anzahl an Nachweisen besitzen. Zudem sieht das Konzept keine Möglichkeit vor, dass der DP die Nutzerzustimmung zum Nachweisabruf verifizieren kann. Aus unserer Sicht muss im Rahmen der Re-Authentifizierung des Nutzers nicht nur die Identität, sondern auch die Zustimmung zum Abruf der konkret angeforderten Nachweise eingeholt werden. Diese Zustimmung sollte im Token mitgespeichert werden, sodass der Token ausschließlich für den Abruf genau dieser Nachweise genutzt werden kann und der DP die erteilte Zustimmung prüfen kann. Ohne eine solche Absicherung besteht das Risiko, dass ein fehlerhaft arbeitender oder kompromittierter DC Nachweise abruft, für die der Nutzer keine Zustimmung erteilt hat.
BD-NOOTS-01 White Paper Zero Trust im NOOTS	**Leitfrage 3:** Gibt es Themen aus dem Cluster IT-Sicherheit, die Ihrer Meinung nach in der Sicherheitsdokumentation, -konzeption und -architektur zusätzlich berücksichtigt werden sollten?

Dokument	Leitfragen
	Hintergrund der Frage: Das Whitepaper ist ein zusätzliches Dokument und kein klassisches Konzept, das 1:1 umgesetzt wird. Neben dem Whitepaper entsteht ein Konzept zur Sicherheitsarchitektur und Sicherheitskonzepte nach BSI-Standard. **Zweck der Frage:** Sicherstellung Vollständigkeit. **Antwort:** Eine Beschreibung zur Einbindung eines SIEM und die Nutzung damit zusammenhängender Automatismen könnten in einem zusätzlichen Whitepaper dargestellt werden. Zudem wäre eine Übersicht / Inventarisierung aller Komponenten und NOOTS Teilnehmer im Sinne der Übersichtlichkeit im Whitepaper hilfreich.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Esther Steverding | Bereichsleiterin Public Sector
e.steverding@bitkom.org

Verantwortliches Bitkom-Gremium
AK Digitale Verwaltung