Bundesverwaltungsamt

D III 3

SAK-Handreichung

für

Behörden und Kommunen

Version 1.0
Datum 13. Februar 2026

Ansprechpartner/-in:

Herr Lipaczewski, Michael
D III 3
Bundesverwaltungsamt
E-Mail: Michael.Lipaczewski@bva.bund.de

Dokumentinformationen

Speicherdatum:	16.02.2026
Version:	1.0
Zustand:	☐ in Bearbeitung ☐ vorgelegt am: ☒ abgenommen
Verfasser:	NOOTS.Infosec@bva.bund.de
Projektleiter:	NOOTS.Infosec@bva.bund.de
Dokumenten-ID:	SAK-Handreichung

Dokumentenhistorie

Datum	Version	Änderungsgrund	Bearbeiter
13.02.2026	1.0	Abnahme	NOOTS.Infosec@bva.bund.de

Ggf. Verteiler

Empfänger	Gremium	Erhalten am

Inhaltsverzeichnis

1. Geltungsbereich und Vertraulichkeit

1.1. Zielgruppe

Dieses Dokument richtet sich an die NOOTS-Teilnehmer, welche im Zuge ihrer Teilnahme am National-Once-Only-Technical-System (NOOTS) ihren sicheren Anschlussknoten (SAK) selbständig konfigurieren müssen. Für den SAK muss ein Sicherheitskonzept von jedem NOOTS-Teilnehmer selbstständig erstellt werden. Dieses Dokument unterstützt dabei, indem es allgemeine Informationen zum NOOTS, sowie bereits durchgeführte Überlegungen und Umsetzungen darstellt.

1.2. Geltungsbereich

Dieses Dokument ist ausschließlich für den Gebrauch der NOOTS-Teilnehmer bestimmt. Eine Veränderung dieses Dokumentes in elektronischer oder physikalischer Form, bedarf der vorherigen Genehmigung des BVA.

1.3. Einstufung

Dieses Dokument ist als öffentlich eingestuft und darf so den NOOTS-Teilnehmern übergeben werden.

1.4. Zuständigkeit und Revision

Dieses Dokument dient als Handreichung für die NOOTS-Teilnehmer. Die Fortschreibung und Prüfung des Rahmendokuments erfolgen im Rahmen der Behandlung des übergeordneten Sicherheitskonzeptes. Die Zuständigkeit obliegt der/dem Informationssicherheits-verantwortlichen des NOOTS-Teilnehmers. Zur Erstellung und Aktualisierung des Sicherheitskonzeptes ist immer das aktuell gültige Dokument der SAK-Handreichung als Grundlage heranzuziehen. Eine regelmäßige Revision des Sicherheitskonzeptes wird erwartet. Die Empfehlung des BVA ist, das Sicherheitskonzept alle zwei Jahre zu revidieren, die Entscheidung obliegt allerdings dem NOOTS-Teilnehmer.

2. Einleitung

2.1. Aufbau und Zweck des Dokuments

Dieses Dokument dient zur Hilfestellung, damit die NOOTS-Teilnehmer auf Basis der hier bereitgestellten Informationen ein Sicherheitskonzept für den Betrieb ihres SAK erstellen können.

Die Struktur dieses Dokuments orientiert sich am typischen Aufbau eines Sicherheitskonzeptes des BVA. Soweit möglich werden allgemein geltende Informationen aus dem vorliegenden übergeordneten Sicherheitskonzept wiedergegeben. Ansonsten wird erläutert, welche Informationen die NOOTS-Teilnehmer wie erfassen und darstellen müssen.

2.2. Vorgehen

Die methodische Vorgehensweise eines Sicherheitskonzeptes basiert auf dem BSI 200-2 Standard. Dabei wird ein klassischer Sicherheitsprozess durchlaufen.

Typischerweise wird für jeden Prozessabschnitt (Strukturanalyse, Schutzbedarfsfeststellung etc.) eine separate Datei erstellt, welche im Sicherheitskonzept referenziert und als Anlage mit abgelegt wird. Bei Nichtnutzung kann diese Tabelle entfernt werden.

Im Folgenden werden die Arbeitspakete kurz dargestellt, die von den NOOTS-Teilnehmern zu bearbeiten sind.

2.2.1 Einstufung

Die Ersteller eines Sicherheitskonzeptes sind für dessen Einstufung verantwortlich. In der Regel sind die Dokumente zur Sicherheitskonzeption als VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) eingestuft, da diese sensiblen Informationen über die Infrastruktur, Fachverfahren oder IT-Systeme beinhalten. Bei einer solchen Einstufung muss darauf geachtet werden, dass ausschließlich Personen mit entsprechender Freigabe Zugriff darauf haben.

2.2.2 Geltungsbereich

Für ein Sicherheitskonzept muss ein Geltungsbereich definiert werden, der aufzeigt, für welche organisatorische, technische und räumliche Komponenten das Sicherheitskonzept gilt.

Der Geltungsbereich umfasst alle Prozesse, Anwendungen, IT-Systeme, Netze, Räume und Gebäude, die für den Betrieb des SAK relevant sind und in der Verantwortung der Teilnehmer liegen, sowie Schnittstellen zu Komponenten, die zwar ebenfalls erforderlich sind, im Sicherheitskonzept aber nicht betrachtet werden, weil sie nicht in der Verantwortung der Teilnehmer liegen.

Der Geltungsbereich ist von jedem NOOTS-Teilnehmer individuell zu ermitteln.

2.2.3 Strukturanalyse

In der Strukturanalyse werden alle relevanten Komponenten erfasst und dokumentiert mit denen der SAK interagiert und die zu dessen Betrieb erforderlich sind. Komponenten, die mit dem SAK geliefert werden, sind bereits vorausgefüllt und können vom NOOTS-Teilnehmer übernommen werden, da sie zur zentralen NOOTS-Infrastruktur gehören. Netzpläne, Geschäftsprozesse, IT-Systeme, Räume, Gebäude und Standorte, Kommunikationsverbindungen, Lieferanten und Administratoren müssen vom SAK-Betreiber/NOOTS-Teilnehmer selbständig erfasst und dokumentiert werden.

2.2.4 Schutzbedarfsfeststellung

Mit der Schutzbedarfsfeststellung werden die entsprechenden Schutzbedarfe für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit definiert. Die in diesem Dokument vorgeschlagenen Schutzbedarfe können übernommen werden, müssen vom NOOTS-Teilnehmer allerdings nochmal überprüft werden, da je nach Einsatz des SAK auch höhere Schutzbedarfe vorliegen können. Zum Beispiel wenn ein essenzieller Kernprozess/Fachverfahren auf einen SAK angewiesen ist.

2.2.5 Modellierung

In der Modellierung werden die BSI IT-Grundschutzbausteine ermittelt, die für den Informationsverbund relevant sind. Hier werden aus übergeordneter Sicht relevante Bausteine vorgegeben, diese müssen aber von den Teilnehmern überprüft werden, da je nach Art des Einsatzes des SAK ggf. weitere Bausteine relevant sein können.

2.2.6 IT-Grundschutz-Check

Der IT-Grundschutz-Check dient dazu, zu identifizieren, welche Anforderungen der ermittelten Bausteine bereits erfüllt sind und welche noch vom NOOTS-Teilnehmer erfüllt werden müssen (Soll-Ist-Vergleich). Für die im Kapitel Modellierung (siehe Kapitel 6)

vorgegebenen Bausteine wurde der IT-Grundschutz-Check bereits durchgeführt. Einige der Anforderungen sind bereits erfüllt, andere müssen von den NOOTS-Teilnehmern selbständig umgesetzt werden. Diese sind in den Tabellen ersichtlich.

Wurden weitere Bausteine ausgewählt, muss der IT-Grundschutz-Check für diese Bausteine selbstständig durchgeführt werden.

2.2.7 Risikoanalyse

In der Risikoanalyse wurde, gemäß des Standards 200-2 und 200-3 des BSI geprüft, welche Gefährdungen für die SAK relevant sind. Auch hier muss je nach Einsatzort des SAK die durchgeführte Risikoanalyse überprüft und ggf. durch weitere Risiken erweitert werden.

3. Verfahrensbeschreibung

Ein SAK ist eine NOOTS-Komponente, die von jedem NOOTS-Teilnehmer als JAR-Datei über die Registrierungsseite heruntergeladen werden muss. Der SAK erlaubt es so den Teilnehmern, über ein interoperables Anschlussprotokoll einen einfachen und sicheren Anschluss an die NOOTS-Infrastruktur zu gewährleisten. Der SAK-Betrieb erfolgt dezentral, aus diesem Grund sind die Teilnehmer dafür verantwortlich, die Betriebsinfrastruktur und die -prozesse eigenständig zu betrachten. Es wird zwischen zwei NOOTS-Teilnehmern unterschieden. Data Consumer (DC) und Data Provider (DP). Beide kommunizieren ausschließlich über die SAK mit den anderen NOOTS-Teilnehmern. Aufgabe der DC ist es, Nachweise abzurufen, die von DP bereitgestellt werden.

Der SAK-DC nutzt ein Spring Boot-Framework mit einem eingebetteten Tomcat. Im SAK-DP wird das Framework Netty[1] genutzt. Diese Komponenten werden für den Datentransport über die NOOTS-Infrastruktur verwendet. Der SAK-DC (Sichere Anschlussknoten des Data Consumers) stellt eine Nachweis-Anfrage an das NOOTS. Vereinfacht wird anschließend überprüft, ob dieser auch die Berechtigung hat, einen Nachweis anzufragen. Nachdem die Überprüfung abgeschlossen wurde, wird in der Registerdatennavigation (RDN) ermittelt, an welchen DP die Anfrage gesendet werden muss. Die RDN liefert dem DC die zum Verbindungsaufbau benötigten Informationen und es wird eine Verbindung zwischen SAK-DC und SAK-DP hergestellt. Der Nachweis-Antrag kann so über den SAK-DP (sicherer Anschlussknoten des Data Providers) an den DP geschickt werden, der den Antrag anschließend bearbeitet und den Nachweis über den SAK an den DC schickt.

[1] https://de.wikipedia.org/wiki/Netty

An Realisierung und Betrieb sind die folgenden **Dienstleistenden** beteiligt:

Dienstleistender	Beschreibung	Outsourcing [ja/ nein]	Cloud-Nutzung [ja/ nein]
Seitenbau	Implementierung (Softwareentwicklung) der sicheren Anschlussknoten (SAK)	Nein	Nein
Dataport	Containerisierung der SAK	Nein	Nein

Tabelle 1: Liste der Dienstleistenden

3.1. Informationstechnik

Überblick der Netzwerkstruktur:

Das System NOOTS (National-Once-Only-Technical-System) bildet die technische Grundlage für den nationalen Datenaustausch im Rahmen der Registermodernisierung (RegMo). Die zugrunde liegende NOINF-Infrastruktur wird von Dataport betrieben.

Die NOOTS-Plattform ist als containerisierte, hochverfügbare Systemlandschaft in den redundanten Data Centern (Alsterdorf und Norderstedt) von Dataport implementiert.

Die Architektur basiert auf einem Kubernetes-Cluster zur Orchestrierung sowie einem PostgreSQL-Replikationscluster mit automatischem Failover und TLS-gesicherter Datenreplikation.

Zugriffe auf die NOOTS-Plattform haben registrierte DC und DP. Mit einem SAK wird eine sichere Verbindung zu NOOTS hergestellt. Mit dieser Verbindung können die DC und DP die NOOTS-Komponenten ansteuern, welche für die Nachweiserstellung und Bearbeitung verwendet werden.

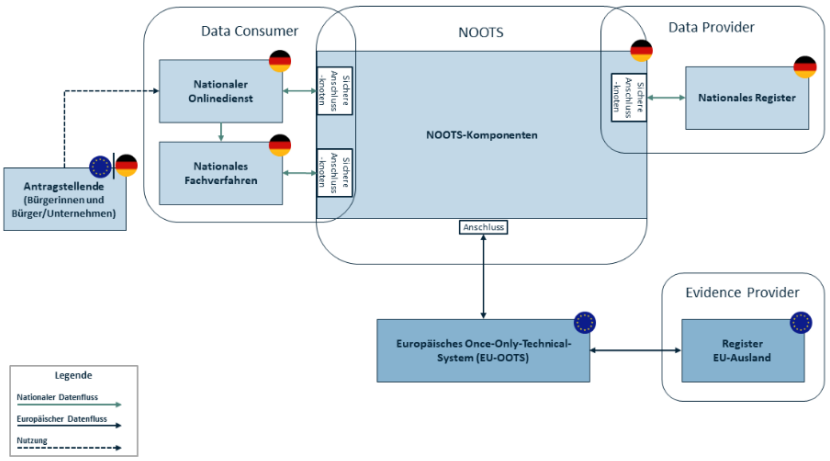

Abbildung 1: Systemübersicht NOOTS

Der SAK-DC wird als JAR-Datei heruntergeladen und muss als selbständige Anwendung mit Anbindung an das Internet laufen und an das NOOTS angebunden werden. Hierfür wird eine Integrationsanleitung [Ref01] bereitgestellt. Nach dem Ausführen der JAR-Datei und nach der Registrierung ist für die entsprechende Behörde ein Eintrag im Identity- and Accessmanagement für Behörden (IAM-B) bekannt und ist somit berechtigt, Nachweis-Anfragen zu senden. Ähnlich verhält es sich mit dem SAK-DP.

3.2. Abgrenzung des Informationsverbunds

Nach dem BSI-Standard 200-2 umfasst ein Informationsverbund „die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen." Demnach bildet sich der Informationsverbund aus dem im Sicherheitskonzept beschriebenen IT-Verfahren und zusätzlicher, in anderen Sicherheitskonzepten beschriebener oder zu beschreibender Komponenten.

Zum Informationsverbund gehören somit der SAK sowie alle Komponenten und Systeme des SAK-Betreibers, welche mit diesem interagieren (siehe Abbildung 2). Nicht zum Informationsverbund gehören sämtliche technische Systeme und Dienste, die innerhalb der von Dataport betriebenen Rechenzentrumsumgebung bereitgestellt und betrieben werden. Dieser Informationsverbund umfasst alle

Bestandteile der NOOTS, die für den Betrieb, die Kommunikation, das Monitoring und die Verwaltung erforderlich sind.

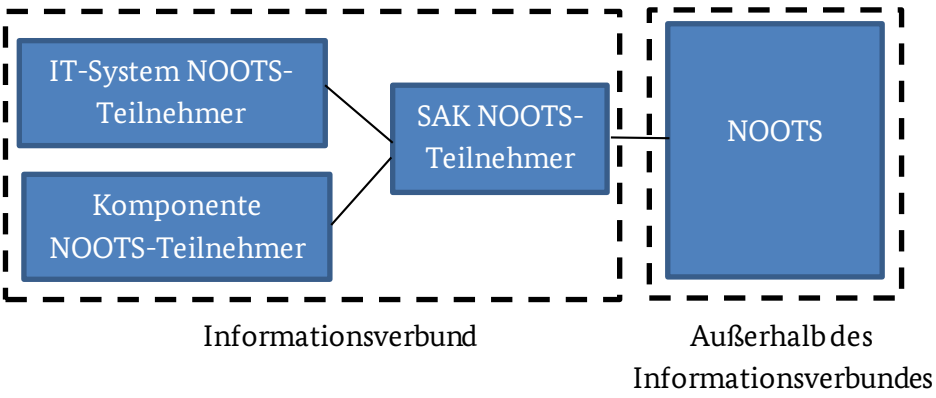

Abbildung 2: Darstellung Informationsverbund

4. Strukturanalyse

Im vorliegenden Dokument werden ausschließlich die im Rahmen der Bereitstellung des SAK betrachteten Komponenten des Informationsverbundes aufgeführt und beschrieben.

Eine vollständige Darstellung aller ermittelten Zielobjekte des Informationsverbundes kann an folgender Stelle gefunden werden.	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Tabelle 2: Angaben zur Strukturanalyse

4.1. Anwendungen

Der SAK wird durch und mit Software realisiert. Folgende Anwendungen liegen vollständig oder teilweise in der Verantwortung des SAK-Betreibers und müssen im Sicherheitskonzept betrachtet werden.

Bezeichnung Anwendung (gemäß Strukturanalyse)	Beschreibung
Hauptanwendung SAK	Lieferung der Anwendung als JAR-Datei, welche auf der Umgebung (VM) des Betreibers installiert wird.
TomCat	Installiert auf: Betriebsumgebung SAK-DC (VM/Host) Laufzeit: Spring Boot mit embedded TomCat
Netty	Installiert auf: Betriebsumgebung SAK-DP (VM/Host) Laufzeit: Spring Boot mit embedded Netty (reactor-netty/WebFlux)
REST-Schnittstelle	Schnittstelle für http-Anfragen

Tabelle 3: Anwendungen aus der Strukturanalyse

4.2. Netzanbindung und Netze

Für die Kommunikation mit NOOTS-MVP müssen die SAK, sowohl SAK-DC als auch SAK-DP über das Internet kommunizieren.

Bezeichnung Netz	Beschreibung
Internet	Der Zugriff über das Internet ist möglich.

Tabelle 4: Netze aus der Strukturanalyse

4.3. Strukturanalyse NOOTS-Teilnehmer

Der NOOTS-Teilnehmer muss für folgende Punkte eine Strukturanalyse durchführen:

- Geschäftsprozesse
- IT-Systeme
- Räume
- IT-Komponenten
- Kommunikationsverbindungen

Eine Strukturanalyse wird häufig in einer Excel-Datei erstellt und die wesentlichen Ergebnisse finden Einzug in das Sicherheitskonzept. Ebenfalls zur Strukturanalyse gehört ein Netzplan. Dieser zeigt alle IT-Systeme und Kommunikationsverbindungen auf, welche für den Betrieb des SAK benötigt werden.

5. Schutzbedarfsfeststellung

Eine Initiale Schutzbedarfsfeststellung wurde hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit durchgeführt. Der Schutzbedarf kann Tabelle 6 entnommen werden.

Die Feststellung des Schutzbedarfs ist an folgender Stelle/an folgenden Stellen dokumentiert:	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Tabelle 5: Angaben zur Schutzbedarfsfeststellung

Der Schutzbedarf ist durch jeden NOOTS-Teilnehmer auf Basis der verarbeiteten Daten selber zu ermitteln und festzulegen. Im Falle eines höheren Schutzbedarfes müssen ggf. ergänzende Sicherheitsmaßnahmen durch den Teilnehmer umgesetzt werden.

Die Schutzbedarfe für die Vertraulichkeit, Integrität und Verfügbarkeit ergeben sich dadurch, dass der SAK als eine wichtige Komponente der NOOTS-Infrastruktur verstanden wird, da nur dadurch Nachweisanfragen und -Antworten auf diese, gesendet werden können. Somit ergibt sich, dass ggf. personenbezogene Daten, welche vertraulich verarbeitet werden müssen, gesendet und empfangen werden können, dass diese Daten richtig sind und nicht verändert wurden. Je nach Einsatzgebiet des SAK ist auch davon auszugehen, dass eine hohe Verfügbarkeit benötigt wird, um innerbetriebliche Prozesse durchführen zu können.

Schutzziel	Beschreibung	Schutzbedarf
Vertraulichkeit	Die Informationen können von keiner unberechtigten Partei gesichtet werden.	Hoch
Integrität	Die Informationen können von keiner unberechtigten Partei geändert werden.	Hoch

Schutzziel	Beschreibung	Schutzbedarf
Verfügbarkeit	Die Informationen stehen berechtigten Parteien zur Verfügung, wenn diese sie brauchen.	Hoch

Tabelle 6: Schutzbedarfe der SAK

6. Modellierung

In der Modellierung wird der Informationsverbund mithilfe der in der Strukturanalyse ermittelten Zielobjekte und Anforderungen aus Bausteinen des IT-Grundschutzes und anderen Quellen nachgebildet. Das Ergebnis ist ein IT-Grundschutz-Modell des Informationsverbunds, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen besteht und die durch die Verwendung der Bausteine die sicherheitsrelevanten Aspekte des Informationsverbunds beinhaltet.

Es wurden bereits sieben Bausteine identifiziert, welche für den Betrieb der SAK benötigt werden. Einige der Anforderungen der Bausteine müssen vom SAK-Betreiber umgesetzt werden. Eine Liste der Anforderungen kann in Kapitel 7 betrachtet werden.

Neben den bereits identifizierten Bausteinen muss vom SAK-Betreiber geprüft werden, ob weitere Bausteine in die Modellierung des Informationsverbundes einfließen. Wenn ja, dann müssen diese ebenfalls Einzug finden.

6.1. IT-Grundschutz-Modell

In der folgenden Tabelle ist das IT-Grundschutz-Modell der in diesem Sicherheitskonzept betrachteten Zielobjekte dargestellt. Dieses Modell enthält neben den Bausteinen des IT-Grundschutz-Kompendiums (Ref02) relevante, **benutzerdefinierte Bausteine (vgl. Kapitel** Fehler! Verweisquelle konnte nicht gefunden werden.**1).** Nach dem BSI 200-2 Standard sind die Bausteine mit einer entsprechenden ID zu kennzeichnen. Die IDs (SAK-00x) sind Vorschläge und können angepasst oder verändert werden.

Zielobjekt (gemäß Strukturanalyse)	**Baustein**
SAK-001	APP.3.1 Webanwendung und Webservices
SAK-002	APP.3.2 Webserver
SAK-003	APP.6 Allgemeine Software
SAK-004	APP.7 Entwicklung und Individualsoftware
SAK-005	CON.8 Software-Entwicklung
SAK-006	CON.10 Entwicklung von Webanwendungen
SAK-007	APP.BDB.WAS Web-Anwendungs-Server

Tabelle 7: IT-Grundschutz-Modell

7. IT-Grundschutz-Check

Der IT-Grundschutz-Check stellt einen Soll-Ist-Vergleich dar, in welchem identifiziert wird, welche Anforderungen des IT-Grundschutzes bereits erfüllt sind und welche nicht. Im Rahmen dieses Dokumentes wird geschaut, welche Anforderungen von NOOTS-Teilnehmern (SAK-Betreibern) umzusetzen sind bzw. welche teilweise durch Dataport erfüllt wurden.

7.1. Zusammenfassung der Ergebnisse

Die folgende Tabelle zeigt, welche BSI IT-Grundschutzbaustein-Anforderungen vom NOOTS-Teilnehmer umzusetzen sind. Diese Bausteine sind eine Empfehlung. Es muss allerdings geprüft werden, ob weitere Bausteine herangezogen werden, da vom jeweiligen Einsatzort des SAK Abweichungen des IT-Grundschutz-Checks vorkommen können.

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A1 Sichere Konfiguration eines Webservers		
Beschreibung		**(TA1)** Nachdem der IT-Betrieb einen Webserver installiert hat, MUSS er eine sichere Grundkonfiguration vornehmen. **(TA2)** Dazu MUSS er insbesondere den Webserver-Prozess einem Konto mit minimalen Rechten zuweisen. **(TA3)** Der Webserver MUSS in einer gekapselten Umgebung ausgeführt werden, sofern dies vom Betriebssystem unterstützt wird. **(TA4)** Ist dies nicht möglich, SOLLTE jeder Webserver auf einem eigenen physischen oder virtuellen Server ausgeführt werden. **(TA5)** Dem Webserver-Dienst MÜSSEN alle nicht notwendige Schreibberechtigungen entzogen werden. **(TA6)** Nicht benötigte Module und Funktionen des Webservers MÜSSEN deaktiviert werden.
Status		Muss von SAK-Betreiber umgesetzt werden.
Umsetzungs-kommentar		TomCat und Netty, sowie der SAK müssen sicher konfiguriert werden.

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A2 Schutz der Webserver-Dateien		
Beschreibung		**(TA1)** Der IT-Betrieb MUSS alle Dateien auf dem Webserver, insbesondere Skripte und Konfigurationsdateien, so schützen, dass sie nicht unbefugt gelesen und geändert werden können. **(TA2)** Es MUSS sichergestellt werden, dass Webanwendungen nur auf einen definierten Verzeichnisbaum zugreifen können (WWW-Wurzelverzeichnis). **(TA3)** Der Webserver MUSS so konfiguriert sein, dass er nur Dateien ausliefert, die sich innerhalb des WWW-Wurzelverzeichnisses befinden. **(TA4)** Der IT-Betrieb MUSS alle nicht benötigten Funktionen, die Verzeichnisse auflisten, deaktivieren. Vertrauliche Daten MÜSSEN vor unberechtigtem Zugriff geschützt werden. **(TA5)** Insbesondere MUSS der IT-Betrieb sicherstellen, dass vertrauliche Dateien nicht in öffentlichen Verzeichnissen des Webservers liegen. **(TA6)** Der IT-Betrieb MUSS regelmäßig überprüfen, ob vertrauliche Dateien in öffentlichen Verzeichnissen gespeichert wurden.
Status		Muss von SAK-Betreiber umgesetzt werden.
Umsetzungs-kommentar		TA1 muss vom SAK-Betreiber umgesetzt werden TA5 und TA6 müssen teilweise vom SAK-Betreiber umgesetzt werden

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A4 Protokollierung von Ereignissen		
Beschreibung	**(TA1)** Der Webserver MUSS mindestens folgende Ereignisse protokollieren: - erfolgreiche Zugriffe auf Ressourcen, - fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressourcen und Server-Fehlern sowie - allgemeine Fehlermeldungen. **(TA2)** Die Protokollierungsdaten SOLLTEN regelmäßig ausgewertet werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	Der SAK bietet die Protokollierungsschnittstelle über STDOUT. Die Umsetzung der Anforderung obliegt der jeweiligen betreibenden Institution.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A8 Planung des Einsatzes eines Webservers		
Beschreibung	**(TA1)** Es SOLLTE geplant und dokumentiert werden, für welchen Zweck der Webserver eingesetzt und welche Inhalte er bereitstellen soll. **(TA2)** In der Dokumentation SOLLTEN auch die Informationen oder Dienstleistungen des Webangebots und die jeweiligen Zielgruppen beschrieben werden. **(TA3)** Für den technischen Betrieb und die Webinhalte SOLLTEN geeignete Zuständige festgelegt werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA3 ist vom SAK-Betreiber umzusetzen	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A8 Planung des Einsatzes eines Webservers		
Beschreibung	**(TA1)** Es SOLLTE geplant und dokumentiert werden, für welchen Zweck der Webserver eingesetzt und welche Inhalte er bereitstellen soll. **(TA2)** In der Dokumentation SOLLTEN auch die Informationen oder Dienstleistungen des Webangebots und die jeweiligen Zielgruppen beschrieben werden. **(TA3)** Für den technischen Betrieb und die Webinhalte SOLLTEN geeignete Zuständige festgelegt werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA3 ist vom SAK-Betreiber umzusetzen	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A9 Festlegung einer Sicherheitsrichtlinie für den Webserver		
Beschreibung	**(TA1)** Es SOLLTE eine Sicherheitsrichtlinie erstellt werden, in der die erforderlichen Maßnahmen und Zuständigkeiten benannt sind. **(TA2)** Weiterhin SOLLTE geregelt werden, wie Informationen zu aktuellen Sicherheitslücken besorgt werden. **(TA3)** Auch SOLLTE geregelt werden, wie Sicherheitsmaßnahmen umgesetzt werden und wie vorgegangen werden soll, wenn Sicherheitsvorfälle eintreten.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA3 müssen vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A10 Auswahl eines geeigneten Webhosters		
Beschreibung		**(TA1)** Betreibt die Institution den Webserver nicht selbst, sondern nutzt Angebote externer Unternehmen im Rahmen von Webhosting, SOLLTE die Institution bei der Auswahl eines geeigneten Webhosters auf folgende Punkte achten: - **(TA2)** Es SOLLTE vertraglich geregelt werden, wie die Dienste zu erbringen sind. **(TA3)** Dabei SOLLTEN Sicherheitsaspekte innerhalb des Vertrags schriftlich in einem Service Level Agreement (SLA) festgehalten werden. - **(TA4)** Die eingesetzten IT-Systeme SOLLTEN vom Webhoster regelmäßig kontrolliert und gewartet werden. **(TA5)** Der Webhoster SOLLTE dazu verpflichtet werden, bei technischen Problemen oder einer Kompromittierung von Kundschaftssystemen zeitnah zu reagieren. - **(TA6)** Der Webhoster SOLLTE grundlegende technische und organisatorische Maßnahmen umsetzen, um seinen Informationsverbund zu schützen.
Status		Muss von SAK-Betreiber umgesetzt werden.
Umsetzungs-kommentar		TA1 – TA6 müssen vom SAK-Betreiber umgesetzt werden.

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A14 Integritätsprüfungen und Schutz vor Schadsoftware		
Beschreibung		**(TA1)** Der IT-Betrieb SOLLTE regelmäßig prüfen, ob die Konfigurationen des Webservers und die von ihm bereitgestellten Dateien noch integer sind und nicht durch Angriffe verändert wurden. **(TA2)** Die zur Veröffentlichung vorgesehenen Dateien SOLLTEN regelmäßig auf Schadsoftware geprüft werden.
Status		Muss von SAK-Betreiber umgesetzt werden.
Umsetzungs-kommentar		TA2 muss vom SAK-Betreiber umgesetzt werden.

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A15 Redundanz		
Beschreibung		**(TA1)** Webserver SOLLTEN redundant ausgelegt werden. **(TA2)** Auch die Internetanbindung des Webservers und weiterer IT-Systeme, wie etwa der Webanwendungsserver, SOLLTEN redundant ausgelegt sein.
Status		Muss von SAK-Betreiber umgesetzt werden.
Umsetzungs-kommentar		TA1 und TA2 muss vom SAK-Betreiber umgesetzt werden.

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A16 Penetrationstest und Revision		
Beschreibung		**(TA1)** Webserver SOLLTEN regelmäßig auf Sicherheitsprobleme hin überprüft werden. **(TA2)** Auch SOLLTEN regelmäßig Revisionen durchgeführt werden. **(TA3)** Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert, ausreichend geschützt und vertraulich behandelt werden. **(TA4)** Abweichungen SOLLTE nachgegangen werden. **(TA5)** Die Ergebnisse SOLLTEN dem ISB vorgelegt werden.
Status		Muss von SAK-Betreiber umgesetzt werden.

Umsetzungs-kommentar	TA1 – TA5 muss vom SAK-Betreiber umgesetzt werden.

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.3.2.A18 Schutz vor Denial-of-Service-Angriffen		
Beschreibung	**(TA1)** Der Webserver SOLLTE ständig überwacht werden. **(TA2)** Des Weiteren SOLLTEN Maßnahmen definiert und umgesetzt werden, die DDoS-Angriffe verhindern oder zumindest abschwächen.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 und TA2 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.6.A4 Regelung für die Installation und Konfiguration von Software		
Beschreibung	**(TA1)** Die Installation und Konfiguration der Software MUSS durch den IT- Betrieb so geregelt werden, dass – die Software nur mit dem geringsten notwendigen Funktionsumfang installiert und ausgeführt wird, - die Software mit den geringsten möglichen Berechtigungen ausgeführt wird, - die datensparsamsten Einstellungen (in Bezug auf die Verarbeitung von personenbezogenen Daten) konfiguriert werden sowie - alle relevanten Sicherheitsupdates und -patches installiert sind, bevor die Software produktiv eingesetzt wird. **(TA2)** Hierbei MÜSSEN auch abhängige Komponenten (unter anderem Laufzeitumgebungen, Bibliotheken, Schnittstellen sowie weitere Programme) mitbetrachtet werden. **(TA3)** Der IT-Betrieb MUSS in Abstimmung mit den Fachverantwortlichen festlegen, wer die Software wie installieren darf. **(TA4)** Idealerweise SOLLTE Software immer zentral durch den IT-Betrieb installiert werden. **(TA5)** Ist es erforderlich, dass die Software (teilweise) manuell installiert wird, **(TA6)** dann MUSS der IT-Betrieb eine Installationsanweisung erstellen, in der klar geregelt wird, welche Zwischenschritte zur Installation durchzuführen und welche Konfigurationen vorzunehmen sind. **(TA7)** Darüber hinaus MUSS der IT- Betrieb regeln, wie die Integrität der Installationsdateien überprüft wird. **(TA8)** Falls zu einem Installationspaket digitale Signaturen oder Prüfsummen verfügbar sind, **(TA9)** MÜSSEN mit diesen die Integrität überprüft werden. **(TA10)** Sofern erforderlich, SOLLTE der IT-Betrieb eine sichere Standardkonfiguration der Software festlegen, mit der die Software konfiguriert wird. **(TA11)** Die Standardkonfiguration SOLLTE dokumentiert werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	*TA3, TA6, TA7, TA8, TA9 sind Mitwirkungspflichten, die durch den Betreiber des SAK umgesetzt werden müssen.* *TA10, TA11: Der SAK Betreiber muss durch die Prüfung der Signatur verifizieren, dass die Integrität der Installationsdatei gewahrt ist.*	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.6.A5 Sichere Installation von Software		
Beschreibung	**(TA1)** Software MUSS entsprechend der Regelung für die Installation auf den IT-Systemen installiert werden. **(TA2)** Dabei MÜSSEN ausschließlich unveränderte Versionen der freigegebenen Software verwendet werden. **(TA3)** Wird von diesen Anweisungen abgewichen, MUSS dies durch Vorgesetzte und den IT-Betrieb genehmigt werden und entsprechend dokumentiert werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA3 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.6.A8 Regelung zur Verfügbarkeit der Installationsdateien		
Beschreibung	**(TA1)** Der IT-Betrieb SOLLTE die Verfügbarkeit der Installationsdateien sicherstellen, um die Installation reproduzieren zu können. **(TA2)** Hierzu SOLLTE der IT-Betrieb - die Installationsdateien geeignet sichern oder - die Verfügbarkeit der Installationsdateien durch die Bezugsquelle (z. B. App- Store) sicherstellen. **(TA3)** Zusätzlich SOLLTE sichergestellt werden, dass Software reproduzierbar konfiguriert werden kann. **(TA4)** Hierzu SOLLTEN die Konfigurationsdateien gesichert werden. **(TA5)** Alternativ SOLLTE geeignet dokumentiert werden, wie die Software konfiguriert wird. **(TA6)** Diese Regelung SOLLTE in das Datensicherungskonzept der Institution integriert werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA6 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.6.A9 Inventarisierung von Software		
Beschreibung	**(TA1)** Software SOLLTE inventarisiert werden. **(TA2)** In einem Bestandsverzeichnis SOLLTE dokumentiert werden, auf welchen Systemen die Software unter welcher Lizenz eingesetzt wird. **(TA3)** Bei Bedarf SOLLTEN zusätzlich die sicherheitsrelevanten Einstellungen miterfasst werden. **(TA4)** Software SOLLTE nur mit Lizenzen eingesetzt werden, die dem Einsatzzweck und den vertraglichen Bestimmungen entsprechen. **(TA5)** Die Lizenz SOLLTE den gesamten vorgesehenen Benutzungszeitraum der Software abdecken. **(TA6)** Wird von einer Standardkonfiguration abgewichen, SOLLTE dies dokumentiert werden. **(TA7)** Das Bestandsverzeichnis SOLLTE anlassbezogen durch den IT-Betrieb aktualisiert werden, insbesondere wenn Software installiert wird. **(TA8)** Das Bestandsverzeichnis SOLLTE so aufgebaut sein, dass bei Sicherheitsvorfällen eine schnelle Gesamtübersicht mit den notwendigen Details ermöglicht wird.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA8 muss vom SAK-Betreiber umgesetzt werden. TA5: Integrationsleitfaden für SAK DC/DP werden von Seitenbau mitgeliefert, sodass Standardkonfigurationen angepasst werden können.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.6.A10 Erstellung einer Sicherheitsrichtlinie für den Einsatz der Software		
Beschreibung	**(TA1)** Die Institution SOLLTE die Regelungen, die festlegen, wie die Software eingesetzt und betrieben wird, in einer Sicherheitsrichtlinie zusammenfassen. **(TA2)** Die Richtlinie SOLLTE allen relevanten Verantwortlichen, Zuständigen und Mitarbeitenden der Institution bekannt sein und die Grundlage für ihre Arbeit und ihr Handeln bilden. **(TA3)** Inhaltlich SOLLTE die Richtlinie auch ein Benutzenden-Handbuch umfassen, dass erläutert, wie die Software zu benutzen und zu administrieren ist. **(TA4)** Es SOLLTE regelmäßig und stichprobenartig überprüft werden, ob die Mitarbeitenden sich an die Richtlinie halten. **(TA5)** Die Richtlinie SOLLTE regelmäßig aktualisiert werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA5 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.6.A12 Geregelte Außerbetriebnahme von Software		
Beschreibung	**(TA1)** Wenn Software außer Betrieb genommen wird, SOLLTE der IT-Betrieb mit den Fachverantwortlichen regeln, wie dies im Detail durchzuführen ist. **(TA2)** Ebenfalls SOLLTE geregelt werden, wie die Benutzenden hierüber zu informieren sind. **(TA3)** Hierbei SOLLTE geklärt werden, ob die funktionalen Anforderungen fortbestehen (z. B. zur Bearbeitung von Fachaufgaben). **(TA4)** Ist dies der Fall, dann SOLLTE geregelt werden, wie die benötigten Funktionen der betroffenen Software weiter verfügbar sein werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA4 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.6.A13 Deinstallation von Software		
Beschreibung	**(TA1)** Wird Software deinstalliert, SOLLTEN alle angelegten und nicht mehr benötigten Dateien entfernt werden. **(TA2)** Alle Einträge in Systemdateien, die für das Produkt vorgenommen wurden und nicht länger benötigt werden, SOLLTEN rückgängig gemacht werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 und TA2 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.6.A14 Nutzung zertifizierter Software		
Beschreibung	**(TA1)** Bei der Beschaffung von Software SOLLTE festgelegt werden, ob Zusicherungen des herstellenden oder anbietenden Unternehmens über implementierte Sicherheitsfunktionen als ausreichend vertrauenswürdig anerkannt werden können. **(TA2)** Ist dies nicht der Fall, SOLLTE eine Zertifizierung der Anwendung z. B. nach Common Criteria als Entscheidungskriterium herangezogen werden. **(TA3)** Stehen mehrere Produkte zur Auswahl, SOLLTEN insbesondere dann Sicherheitszertifikate berücksichtigt werden, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfasst und die Mechanismenstärke dem Schutzbedarf entspricht.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1, TA2: Die SAK betreibende Stelle muss festlegen, ob sie dem BVA (als Hersteller und Anbieter des SAK) in ausreichendem Maße vertraut. TA3 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA1 Restriktive Rechtevergabe des Web-Anwendungs-Servers		
Beschreibung	**(TA1)** Die Berechtigungen auf dem Web-Anwendungs-Server MUSS ausreichend restriktiv gesetzt werden (Minimalprinzip bei der Rechtevergabe). **(TA2)** Der Web-Anwendungs-Server DARF NICHT als privilegierter Benutzer betrieben werden. **(TA3)** Es SOLLTE ein eigener Nutzer und ggf. eine eigene Gruppe angelegt werden, die NUR mit eingeschränkten Rechten ausgestattet werden DARF. **(TA4)** Es SOLLTE nicht möglich sein, sich mit dem privilegierten Benutzer remote einzuloggen. Die Dateiberechtigungen SOLLTEN restriktiv gesetzt werden.	

Status	Muss von SAK-Betreiber umgesetzt werden.
Umsetzungs-kommentar	TA1 – TA4 muss vom SAK-Betreiber umgesetzt werden.

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA3 Protokollierung sicherheitsrelevanter Ereignisse auf dem Web-Anwendungs-Server		
Beschreibung	**(TA1)** Es MUSS sichergestellt werden, dass sicherheitsrelevante Ereignisse auf einem Web-Anwendungs-Server mit den erforderlichen Merkmalen nachvollziehbar protokolliert werden. **(TA2)** Die sicherheitsrelevanten Protokollierungsdaten MÜSSEN regelmäßig durch den IT-Betrieb ausgewertet werden. **(TA3)** Bei der Auswertung der Protokollierungsdaten MUSS sichergestellt werden, dass Schadcode in Protokoll-Einträgen vom Auswertungsprogramm nicht interpretiert wird.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA3 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA4 Planung des Einsatzes und der Installation des Web-Anwendungs-Servers		
Beschreibung	**(TA1)** Ausgehend vom Fachkonzept für das jeweilige Fachverfahren SOLLTE der Einsatz und die Installation des Web-Anwendungs-Servers geplant werden. **(TA2)** Die benötigten Funktionen und Schnittstellen SOLLTEN definiert sein. **(TA3)** Falls ein Connector genutzt wird SOLLTE dessen Konfiguration geplant werden. **(TA4)** Es SOLLTE geplant werden, ob Load-Balancing eingesetzt werden soll und welche Parameter für den Connector zu setzen sind. **(TA5)** Die Netzeinbindung des Web-Anwendungs-Servers SOLLTE geplant werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA5 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA7 Shutdown-Schutz		
Beschreibung	**(TA1)** Der Web-Anwendungs-Server SOLLTE vor einem unautorisiertem Shutdown geschützt werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA8 Sicherer Betrieb eines Web-Anwendungs-Servers		
Beschreibung	**(TA1)** Der sichere Betrieb eines Web-Anwendungs-Servers SOLLTE in einer Betriebsdokumentation (z.B. Betriebshandbuch) definiert werden. **(TA2)** Hierbei SOLLTEN die folgenden Aspekte berücksichtigt werden:	

	- Dokumentation von Änderungen am Web-Anwendungs-Server - Einspielen von Sicherheitsupdates und Patches - Dokumentation verwendeter Ports - Dokumentation der Installationsanleitung (oder Verweis) - Protokollierung von Systemereignissen und regelmäßige Auswertung der Protokolle - Art der Datensicherung, Vorgehensweise bei einem Restore - Vorgehensweise bei einem Notfall **(TA3)** Es SOLLTE einen Überblick über die im Betrieb befindlichen Web-Anwendungs-Server Instanzen geben. **(TA4)** Die Konfiguration des Web-Anwendungs-Servers SOLLTEN regelmäßig auf Konformität geprüft werden.
Status	Muss von SAK-Betreiber umgesetzt werden.
Umsetzungs-kommentar	TA1 – TA4 muss vom SAK-Betreiber umgesetzt werden.

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA10 Aktualisierungen der Laufzeit-Umgebung		
Beschreibung	**(TA1)** Die benötigte Laufzeitumgebung MUSS regelmäßig aktualisiert werden. **(TA2)** Dabei MUSS berücksichtigt werden, ob das Update innerhalb einer Hauptversion erfolgen soll oder ob eine neue Hauptversion verwendet werden soll. **(TA3)** Es MUSS sichergestellt werden, dass die Web-Anwendung die neue Version der Umgebung unterstützt.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA3 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA11 Notfallvorsorge für einen Web-Anwendungs-Server		
Beschreibung	**(TA1)** Im Rahmen der Notfallvorsorge für einen Web-Anwendungs-Server SOLLTE betrachtet werden, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA12 Absicherung der Administrations-Schnittstellen		
Beschreibung	**(TA1)** Stellt der Server Administrations-Schnittstellen zur Verfügung, SOLLTEN die folgenden Sicherheitseinstellungen umgesetzt werden: • Zugriff beschränken: Der Zugriff auf das Tool sollte auf die erforderlichen Personen beschränkt werden. • Der Zugriff auf das Tool sollte auf ausgewählte IP-Adressen beschränkt werden. • Zur Authentisierung sind starke und komplexe Passwörter einzusetzen. • Rechte sollten granular vergeben werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 muss vom SAK-Betreiber umgesetzt werden.	

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA12 Absicherung der Administrations-Schnittstellen		
Beschreibung	**(TA1)** Abhängig vom Schutzbedarf des Verfahrens, der Positionierung innerhalb des Netzes und mögliche Anbindungen an öffentliche Netze SOLLTE geprüft werden, die Serverdienste durch jeweils separate ITSysteme voneinander zu trennen. **(TA2)** Dabei SOLLTE ein mehrschichtiger Ansatz (Multi-Tier-Architektur) mit den Sicherheitszonen Webschicht, Anwendungsschicht und Datenschicht erfüllt werden. **(TA3)** Es SOLLTE geprüft werden, ob Webserver, Web-Anwendungs-Server und Datenbanken auf getrennten IT-Systemen zu betreiben sind. **(TA4)** Auch SOLLTEN jeweils eigene Benutzerkonten für die unterschiedlichen Serverprozesse der Systemkomponenten verwendet werden. **(TA5)** Dabei SOLLTEN die Rechte dieser Dienstkonten auf Betriebssystemebene soweit eingeschränkt werden, dass nur auf die erforderlichen Ressourcen und Dateien des Betriebssystems zugegriffen werden kann.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 – TA5 muss vom SAK-Betreiber umgesetzt werden.	

8. Risikoanalyse

Bei der Risikoanalyse wird ermittelt, welche Gefährdungen die Schutzziele beeinträchtigen können. Für den Informationsverbund des SAK wurde bereits eine Risikoanalyse durchgeführt. Je nach Einsatzort des SAK muss die Risikoanalyse erneut durchgeführt werden, um zu schauen, ob weitere Risiken betrachtet werden müssen.

Im ersten Schritt wurden die relevanten Gefährdungen ermittelt. Tabelle 8 zeigt die Ergebnisse der Gefährdungsermittlung.

Zielobjekt (gemäß Strukturanalyse)	**Bemerkung**
G 0.14 Ausspähen von Informationen / Spionage	Die Kommunikation zwischen den SAK beinhaltet unter anderem personenbezogene Daten, teilweise auch personenbezogene Daten besonderer Kategorien. Die SAK haben keine Daten, welche "at rest" gespeichert werden. Es könnten lediglich Daten "in transit" ausgespäht werden. Die Übermittlung von Daten zwischen dem SAK-DC und SAK-DP erfolgt mittels mTLS 1.3
G 0.15 Abhören	Die Kommunikation zwischen den SAK beinhaltet unter anderem personenbezogene Daten, teilweise auch personenbezogene Daten besonderer Kategorien. Die SAK haben keine Daten, welche "at rest" gespeichert werden. Es könnten lediglich Daten "in transit" abgehört werden. Die Übermittlung von Daten zwischen dem SAK-DC und SAK-DP erfolgt mittels mTLS 1.3
G 0.18 Fehlplanung oder fehlende Anpassung	Die SAK werden von vielen verschiedenen Teilnehmern betrieben, sodass diese Gefährdung von der betreibenden Stelle bewertet werden muss.
G 0.19 Offenlegung schützenswerter Informationen	Die Kommunikation zwischen den SAK beinhaltet unteranderem personenbezogene Daten, teilweise auch personenbezogene Daten besonderer Kategorie. Die SAK haben keine Daten, welche "at rest" gespeichert werden. Es könnten lediglich Daten "in transit" offengelegt werden. (Siehe G.0.14 und G.0.15)

Zielobjekt (gemäß Strukturanalyse)	**Bemerkung**
G 0.22 Manipulation von Informationen	Der SAK bietet Schutzmechanismen, um eine Manipulation von "Dritten" zu verhindern (APP.3.2.A1 Sichere Konfiguration eines Webservers, APP.3.2.A2 Schutz der Webserver-Dateien, APP.3.2.A5 Authentifizierung). Darüber hinaus muss allerdings von der betreibenden Stelle sichergestellt werden, dass der Zugriff auf das System, auf dem der SAK ausgeführt wird auf einen berechtigten Personenkreis beschränkt ist.
G 0.23 Unbefugtes Eindringen in IT-Systeme	Der SAK bietet Schutzmechanismen, um ein Eindringen zu verhindern (APP.3.2.A1 Sichere Konfiguration eines Webservers, APP.3.2.A2 Schutz der Webserver-Dateien, APP.3.2.A5 Authentifizierung usw.). Darüber hinaus muss allerdings von der betreibenden Stelle sichergestellt werden, dass eine Kontrolle und Monitoring auf den jeweiligen Systemen stattfinden.
G 0.28 Software-Schwachstellen oder -Fehler	Es gibt etablierte Release-Prozesse für den SAK, sodass ggf. Fehler oder Schwachstellen zeitnah behandelt werden können. Unteranderem werden Schwachstellenscanner eingesetzt.
G 0.46 Integritätsverlust schützenswerter Informationen	Der SAK wird vom Softwarehersteller signiert, welcher es der betreibenden Stelle erlaubt die Integrität der Datei zu verifizieren. Diese Gefährdung muss im Sicherheitskonzept der Betriebsumgebung der betreibenden Stelle bewertet werden. Ebenso müssen in den jeweiligen Sicherheitskonzepten der angeschlossenen Fachverfahren und Onlinedienste diese Gefährdung bewertet werden.

Tabelle 8: Ermittelte Risiken

Für die Risikobewertung muss anschließend noch eine Zuordnung der Risiken stattfinden. Die Zuordnung basiert darauf, wie hoch Eintrittswahrscheinlichkeit und Schadenhöhe für die jeweilige Gefährdung sind. Aus der Kombination von Eintrittswahrscheinlichkeit und Schadenhöhe, welche in eine Risikomatrix (Tabelle 9 zeigt eine beispielhafte Risikomatrix, jeder NOOTS-Teilnehmer muss die Schwellenwerte für sich definieren) eingetragen werden, ergibt sich die zuzuordnende Risikokategorie.

		Eintrittswahrscheinlichkeit			
		selten	mittel	häufig	Sehr häufig
Schadenhöhe	Gering	Gering	Gering	Mittel	Mittel
	Begrenzt	Gering	Mittel	Mittel	Hoch
	Beträchtlich	Mittel	Mittel	Hoch	Sehr Hoch
	Existenz-bedrohend	Hoch	Hoch	Sehr Hoch	Sehr Hoch

Tabelle 9: Beispiel einer Risikomatrix

Durch das Eintragen der Gefährdungen in die Risikomatrix ergeben sich für die Gefährdungen folgende Risikokategorien.

Zielobjekt (gemäß Strukturanalyse)	Risikokategorie gering	Risikokategorie mittel	Risikokategorie hoch	Risikokategorie sehr hoch
G 0.14	X			
G 0.15	X			
G 0.18	X			
G 0.19	X			
G 0.22	X			
G 0.23		X		
G 0.28	X			
G 0.46	X			

Tabelle 10: Brutto-Risiken der einzelnen Gefährdungen

Anschließend muss entschieden werden, wie mit den Risiken umgegangen wird. Diese können, akzeptiert, reduziert, transferiert oder vermieden werden. Es sind jeweils Maßnahmen zu definieren, welche umgesetzt werden müssen, um das gewünschte Netto-Risiko zu erreichen. In der Risikoanalyse des Dienstleisters wird nur G 0.23 verringert, da die Erfüllung der Anforderung APP.BDB.WAS.BDA12 (siehe Anhang) zu einer Risikoreduktion führt.

Zielobjekt (gemäß Strukturanalyse)	Risikokategorie gering	Risikokategorie mittel	Risikokategorie hoch	Risikokategorie sehr hoch
G 0.14	X			
G 0.15	X			
G 0.18	X			
G 0.19	X			
G 0.22	X			
G 0.23	X			
G 0.28	X			
G 0.46	X			

Tabelle 11: Netto-Risiken der einzelnen Gefährdungen

9. Anhang

Anforderung 12 auf dem benutzerdefinierten Baustein APP.BDB.WAS.BDA12.

Anforderung	Umsetzungsstatus	Beschreibung SAK-Betreiber
APP.BDB.WAS.BDA12 Absicherung der Administrations-Schnittstellen		
Beschreibung	(**TA1**) Stellt der Server Administrations-Schnittstellen zur Verfügung, SOLLTEN die folgenden Sicherheitseinstellungen umgesetzt werden: • Zugriff beschränken: Der Zugriff auf das Tool sollte auf die erforderlichen Personen beschränkt werden. • Der Zugriff auf das Tool sollte auf ausgewählte IP-Adressen beschränkt werden. • Zur Authentisierung sind starke und komplexe Passwörter einzusetzen. • Rechte sollten granular vergeben werden.	
Status	Muss von SAK-Betreiber umgesetzt werden.	
Umsetzungs-kommentar	TA1 muss vom SAK-Betreiber umgesetzt werden.	

10. Referenzverzeichnis

Bezeichnung	Quelle
Ref01	Integrationsanleitung Data Provider / Data Consumer NOOTS Referenzumgebung Link: https://kundenportal.dataport.de/websites/1159/Qualittsmanagement/Dokumente/integrationsanleitung%20DP%20%20DC%20v%201.4.pdf
Ref02	Liste aller BSI IT-Grundschutz-Bausteine: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

11. Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
DC	Data Consumer
DP	Data Provider
IAM-B	Identity and Accessmanagement für Behörden
ISK	Informationssicherheitskonzept
JAR	Java Archive
MVP	Minimum Viable Product
NOINF	NOOTS Infrastruktur
NOOTS	National Once Only Technical System
RDN	Registerdatennavigation
RegMo	Registermodernisierung
REST	Representational State Transfer
SAK	Sicherer Anschlussknoten

12. Glossar

Brutto-Risiko	Beschreibt das Risiko, bevor Maßnahmen zur Vermeidung definiert wurden.
Informationsverbund	Der Informationsverbund beinhaltet alle IT-Komponenten, welche im Geltungsbereich definiert wurden.
Integrität	Stellt sicher, dass die Information korrekt und unversehrt ist.
Vertraulichkeit	Stellt sicher, dass die Informationen von keiner unberechtigten Person betrachtet wurden.
Verfügbarkeit	Stellt sicher, dass die Information zur Verfügung steht, wenn sie gebraucht werden.
Risiko-Akzeptanz	Bewusste Entscheidung einer Organisation, ein identifiziertes Risiko zu akzeptieren.
Risiko-Verringerung	Bewusste Entscheidung einer Organisation, die Eintrittswahrscheinlichkeit ein identifiziertes Risiko zu reduzieren.
Risiko-Vermeidung	Bewusste Entscheidung einer Organisation, ein identifiziertes Risiko vollständig auszuschließen.
Risiko-Transfer	Bewusste Entscheidung einer Organisation, ein identifiziertes Risiko auf eine andere Partei zu verlagern.

13. Abbildungsverzeichnis

14. Tabellenverzeichnis