Gesamtprozess-Beschreibung

Beweiswerterhaltung durch das Zusammenspiel von E-Scannen, E-Akte Bund und DZAB

Stand 27.10.2026



Erstellt am:	22.10.2026
Zuletzt geändert:	22.10.2026
Bearbeitungszustand:	in Bearbeitung: Nein
	Vorgelegt: Nein
	fertig gestellt: Ja
Dateiablage	SIB-Portal

Änderungsverzeichnis

Nr.	Datum	Vers	Geänderte Kapitel	Beschreibung der Änderungen	Autor	Zustand
1	22.10.2026	1.0	Alle	Initiale Erstellung	BVA	final

Inhaltsverzeichnis

1 Über dieses Dokument 1

1.1 Zweck und Zielgruppe 1

1.2 Aufbau des Dokuments 1

2 Die drei Maßnahmen und ihr Zusammenspiel 1

2.1 Ausgangslage und rechtlicher Rahmen 1

2.2 Maßnahme E-Scannen 2

2.3 Maßnahme E-Akte Bund 2

2.4 Maßnahme DZAB 2

2.5 Wichtige Begriffe 3

3 Der Gesamtprozess im Überblick 3

4 Abschnitt A: Ersetzendes Scannen 4

4.1 Erfassung und Qualitätssicherung 4

4.2 Automatisierte Weiterverarbeitung und Siegelung 4

4.3 Übergabe an die E-Akte Bund und Umgang mit dem Papier 4

5 Abschnitt B: Speicherung in der E-Akte Bund 5

5.1 Eingang und Kennzeichnung 5

5.2 Frühzeitige Beweiswerterhaltung 5

5.3 Veraktung und Fristen 6

6 Abschnitt C: Auslagerung in das DZAB 6

6.1 Auslagerung nach Ablauf der Transferfrist 6

6.2 Langzeitspeicherung und Zugriff 6

6.3 Ende der Aufbewahrungsfrist 7

7 Beweiswerterhalt über den gesamten Lebenszyklus 7

7.1 Warum die Beweiskette trägt 7

7.2 Der Evidence Record als Nachweis 7

8 Anlagen 8

8.1 Anlage 1: Gesamtprozess 8

8.2 Anlage 2: Beweiswerterhaltung ohne Anbindung an das DZAB 8

8.2.1 Ausgangslage 8

8.2.2 Das Hashbaum-Verfahren der Maßnahme E-Scannen 8

8.2.3 Warum das Verfahren nur übergangsweise trägt 9

8.2.4 Verantwortung der Nutzerbehörde 9

1 Über dieses Dokument

1.1 Zweck und Zielgruppe

Dieses Dokument beschreibt den Gesamtprozess des ersetzenden Scannens in der Bundesverwaltung: von der Annahme des Papiereingangs bis zur Löschung nach Ablauf der Aufbewahrungsfrist. Im Fokus seht das Zusammenspiel der drei Maßnahmen E-Scannen, E-Akte Bund und Digitales Zwischenarchiv des Bundes (DZAB).

1.2 Aufbau des Dokuments

Kapitel 2 stellt die drei Maßnahmen vor und erläutert, warum sie nur gemeinsam das Ziel des rechtssicheren ersetzenden Scannens erreichen. Kapitel 3 zeigt den Gesamtprozess im Überblick. Die Kapitel 4 bis 6 beschreiben die drei Abschnitte des Prozesses. Kapitel 7 erläutert, warum die Beweiskette über den gesamten Lebenszyklus trägt.

Die Darstellung in den Kapiteln 3 bis 7 beschreibt den Regelfall: Die Digitalisate werden in der E-Akte Bund gespeichert und über diese an das DZAB übergeben. Für Nutzerbehörden, bei denen diese Kette noch nicht vollständig besteht, beschreibt Anlage 2 die zulässige Übergangslösung und die damit verbundene Verantwortung.

Der vollständige Gesamtprozess als BPMN-Darstellung ist als Anlage 1 beigefügt.

2 Die drei Maßnahmen und ihr Zusammenspiel

2.1 Ausgangslage und rechtlicher Rahmen

Ersetzendes Scannen bedeutet: Ein Papierdokument wird gescannt, das dabei entstehende elektronische Dokument – das Digitalisat – tritt an die Stelle des Papiers, und das Papier wird anschließend vernichtet oder zurückgegeben. Der Nutzen liegt auf der Hand, die Anforderung ebenso: Es muss über die gesamte Aufbewahrungsdauer nachweisbar bleiben, dass das Digitalisat das Papierdokument vollständig und inhaltlich unverändert wiedergibt und seit dem Scannen nicht verändert wurde.

Für Bundesbehörden, die elektronische Akten führen, ist die Verpflichtung zum rechtssicheren ersetzenden Scannen in § 7 des E-Government-Gesetzes des Bundes (EGovG) festgehalten. Die technischen und organisatorischen Anforderungen ergeben sich aus der Technischen Richtlinie TR RESISCAN (BSI TR-03138). Ihr liegt der nachfolgend dargestellte generische Scanprozess zugrunde.

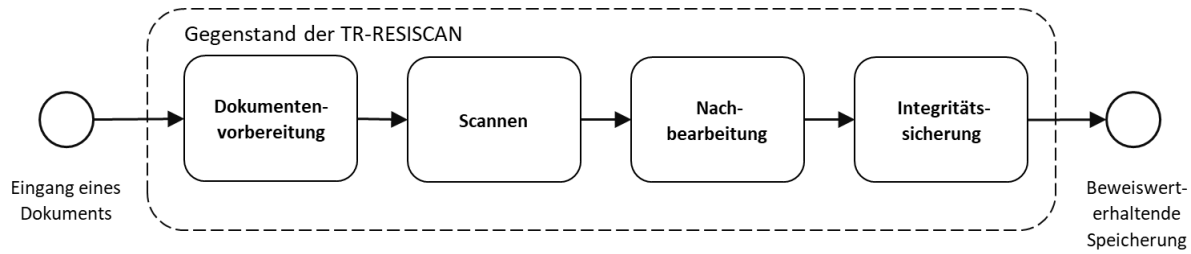


Abbildung 1: Generischer Scanprozess gemäß TR RESISCAN

Für Dokumente mit hohem Schutzbedarf verlangt die TR RESISCAN für die Integritätssicherung qualifizierte elektronische Signaturen oder Siegel. Damit ist die Anforderung aber nur für den Moment des Scannens erfüllt. Weil kryptografische Verfahren mit der Zeit an Sicherheit verlieren können, muss der Beweiswert zusätzlich über die gesamte Aufbewahrungsdauer erhalten werden. Genau aus dieser Anforderung ergibt sich, warum die drei Maßnahmen zusammenwirken müssen.

2.2 Maßnahme E-Scannen

Die Maßnahme E-Scannen stellt einen zentral im ITZBund betriebenen Scandienst bereit, der die Anforderungen der TR RESISCAN umsetzt und das ersetzende Scannen von Dokumenten bis zu einem Schutzbedarf von maximal „hoch“ ermöglicht. Die Nutzerbehörde muss weder eigene Scan-Software betreiben noch eine eigene Siegelinfrastruktur aufbauen.

Der Dienst erzeugt aus den Bilddaten eine PDF/A-Datei, integriert einen Transfervermerk (als PDF in PDF) und sichert seine Integrität durch ein qualifiziertes elektronisches Siegel. Die Siegelung erfolgt über eine Siegelanwendungskomponente (SAK) im ITZBund im Zusammenspiel mit dem Fernsiegeldienst seal-me der Bundesdruckerei.

Was die Maßnahme nicht leistet: Sie verwahrt die Digitalisate nicht. Nach der Übergabe an das Zielsystem werden Stapel und Zwischenspeicher gelöscht. Der Beweiswert ist damit im Moment des Scannens gesichert, aber nicht dauerhaft erhalten.

2.3 Maßnahme E-Akte Bund

Die E-Akte Bund ist der zentrale Basisdienst zur einheitlichen elektronischen Aktenführung. Sie nimmt die gesiegelten Digitalisate über das Schnittstelleninterface (SSI) entgegen, registriert sie als Eingangsdokumente und stellt sie den Beschäftigten in Arbeitsvorräten zur Verarbeitung und Veraktung bereit.

Für den Gesamtprozess ist ihre zweite Rolle entscheidend: Die E-Akte Bund ist das steuernde System. Sie stößt alle Übergaben an das DZAB, alle Rückholungen und alle Löschungen an. Anwenderinnen und Anwender müssen das DZAB nicht gesondert bedienen; sie steuern es mittelbar über die Veraktung und über die gesetzten Fristen.

Was die Maßnahme nicht leistet: Die E-Akte Bund verfügt selbst nicht über die Fähigkeit zur beweiswerterhaltenden Langzeitspeicherung. Sie kann weder Zeitstempel erneuern noch Hashwerte mit stärkeren Verfahren neu bilden.

2.4 Maßnahme DZAB

Das Digitale Zwischenarchiv des Bundes wird im Auftrag des Bundesarchivs betrieben und allen öffentlichen Stellen des Bundes als Zwischenarchiv im Sinne des § 8 Bundesarchivgesetz (BArchG) zur Verfügung gestellt. Es erfüllt die Anforderungen der Technischen Richtlinie TR-ESOR (BSI TR-03125) und ist hierfür zertifiziert.

Das DZAB ist die einzige der drei Maßnahmen, die den Beweiswert dauerhaft erhalten kann. Es verfügt über die Digitalisate selbst und kann deshalb Zeitstempel übersignieren und Hashwerte mit stärkeren Verfahren neu bilden, sobald die verwendeten kryptografischen Verfahren an Sicherheit verlieren. Das DZAB stellt zwei getrennte Mandanten bereit, die im Gesamtprozess unterschiedliche Aufgaben haben:

Mandant	Aufgabe
Mandant für die frühzeitige Beweiswerterhaltung („Schließfach-Mandant“)	Nimmt bereits während der laufenden Verarbeitung eine Kopie jedes gesiegelten Schriftstücks auf. Damit ist der Beweiswert gesichert, lange bevor der Vorgang abgeschlossen ist.
Mandant für die Langzeitspeicherung („Aussonderungsmandant“)	Nimmt den abgeschlossenen Vorgang als logische Einheit auf und erhält dessen Beweiswert bis zum Ablauf der Aufbewahrungsfrist.

Mit der Nutzung des DZAB kommt eine Behörde zugleich ihrer gesetzlichen Anbietungspflicht nach § 5 Absatz 1 BArchG nach.

2.5 Wichtige Begriffe

Begriff	Bedeutung
Digitalisat	Das beim Scannen entstandene elektronische Dokument, das an die Stelle des Papierdokuments tritt.
Transfervermerk	Ein im Digitalisat eingebetteter Vermerk, der die Umwandlung vom Papier in das elektronische Dokument dokumentiert.
Hashwert	Eine eindeutige mathematische Prüfsumme einer Datei, vergleichbar mit einem digitalen Fingerabdruck. Sie verändert sich, sobald der Dateiinhalt verändert wird.
Qualifiziertes elektronisches Siegel	Ein von einem Vertrauensdiensteanbieter ausgestelltes elektronisches Siegel, das Herkunft und Unversehrtheit einer Datei nachweist. Mit diesem werden die Siegel erstellt.
XAIP	XML-basiertes Archivinformationspaket. Format, in dem Dateien nach den Vorgaben der TR-ESOR im DZAB gespeichert werden.
AOID	Archive Object ID. Kennzeichen, unter dem ein Objekt im DZAB gespeichert ist; wird an die E-Akte Bund zurückgemeldet.
Transferfrist	Frist, nach deren Ablauf ein abgeschlossener Vorgang aus der E-Akte Bund in die Langzeitspeicherung des DZAB ausgelagert wird.
Aufbewahrungsfrist	Frist, nach deren Ablauf ein Vorgang ausgesondert bzw. gelöscht wird.
Evidence Record	Nachweis darüber, dass ein Digitalisat seit dem Zeitpunkt des Scannens unverändert geblieben ist.

3 Der Gesamtprozess im Überblick

Der Gesamtprozess gliedert sich in drei aufeinander folgende Abschnitte. Der vollständige Ablauf einschließlich aller Systembeteiligten ist als BPMN-Darstellung in Anlage 1 dargestellt.

Abschnitt	Gegenstand	Ergebnis
A – Ersetzendes Scannen (Kapitel 4)	Von der Annahme des Papiereingangs bis zur Übergabe an die E-Akte Bund	Aus dem Papierdokument ist ein gesiegeltes Digitalisat geworden, das in der E-Akte Bund vorliegt. Das Papier kann nach Ablauf, der von der Nutzerbehörde frei gewählte Zwischenlagerungsfrist, vernichtet werden.

Abschnitt	Gegenstand	Ergebnis
B – Speicherung in der E-Akte Bund (Kapitel 5)	Von der Entgegennahme des Digitalisats bis zur Verfügung des abgeschlossenen Vorgangs	Das Digitalisat ist veraktet, sein Beweiswert ist frühzeitig im DZAB gesichert, und der Vorgang ist nach der Verarbeitung mit Fristen zu den Akten verfügt.
C – Auslagerung in das DZAB (Kapitel 6)	Von der Auslagerung des abgeschlossenen Vorgangs bis zu dessen Löschung	Der Vorgang liegt vollständig und beweiswerterhaltend im DZAB und wird nach Ablauf der Aufbewahrungsfrist gelöscht.

4 Abschnitt A: Ersetzendes Scannen

Dieser Abschnitt umfasst den Weg vom Papiereingang bis zum gesiegelten Digitalisat in der E-Akte Bund. Er findet in der Post- bzw. Scanstelle der Nutzerbehörde statt.

4.1 Erfassung und Qualitätssicherung

Der Papiereingang wird gesichtet und für das Scannen vorbereitet. Dabei wird entschieden, welche Dokumente ersetzend gescannt werden und welche hiervon ausgenommen sind. Nach dem Scannen folgen die Kontrollschritte: die Prüfung auf Vollständigkeit, die Prüfung der Scanqualität und eine Stichprobenkontrolle im Vier-Augen-Prinzip. Zudem werden die Metadaten erfasst, und die Angabe, in welchen Arbeitsvorrat der E-Akte Bund das Digitalisat übergeben werden soll.

Diese Kontrollschritte sind der organisatorische Kern des ersetzenden Scannens. Ihr Umfang wird im Scankonzept der Behörde festgelegt und ist dort zu dokumentieren, denn im Streitfall wird nicht nur die technische Sicherung betrachtet, sondern auch die Frage, ob der Scanprozess ordnungsgemäß organisiert war. Die konkrete Ausgestaltung der Arbeitsschritte regelt die Verfahrensanweisung.

4.2 Automatisierte Weiterverarbeitung und Siegelung

Ab der Übergabe an den Scan-Server im ITZBund läuft die Verarbeitung ohne manuelle Tätigkeiten ab. Die Bilddaten durchlaufen die Volltexterkennung und werden zu einer PDF-Datei zusammengeführt. Anschließend wird der Transfervermerk erstellt und in die Datei eingebettet.

Erst danach beginnt die Integritätssicherung. Die Siegelanwendungskomponente bildet den Hashwert der PDF-Datei einschließlich des eingebetteten Transfervermerks und übergibt ihn an den Fernsiegeldienst der Bundesdruckerei. Dort wird der Hashwert mit einem qualifizierten Zertifikat gesiegelt. Der zurückgegebene gesiegelte Hashwert wird geprüft und in die PDF-Datei eingebettet.

4.3 Übergabe an die E-Akte Bund und Umgang mit dem Papier

Die gesiegelte Datei wird über das Schnittstelleninterface (SSI) an die E-Akte Bund übergeben. Erst nach deren Bestätigung werden Stapel und Zwischenspeicher automatisch gelöscht. Damit ist ausgeschlossen, dass Dateien bei der Übergabe verloren gehen.

Die Papierdokumente werden bis zum Ablauf der festgelegten Zwischenlagerungsfrist aufbewahrt und erst danach vernichtet. Die Zwischenlagerung dient als Sicherheitsnetz für den Fall, dass sich ein Fehler im Scanvorgang erst später zeigt. Urkunden und andere Dokumente, deren Originale aus rechtlichen Gründen erhalten bleiben müssen, werden nicht vernichtet, sondern gemäß den Festlegungen des Scankonzepts (Umsetzung in der Negativliste) aufbewahrt oder zurückgegeben.

5 Abschnitt B: Speicherung in der E-Akte Bund

Dieser Abschnitt umfasst die Verarbeitung des Digitalisats in der E-Akte Bund und die frühzeitige Sicherung seines Beweiswerts im DZAB.

5.1 Eingang und Kennzeichnung

Die E-Akte Bund nimmt die gesiegelte Datei über das Schnittstelleninterface (SSI) entgegen, registriert sie als Schriftstück in einem Eingangsdokument und weist sie dem beim Scannen festgelegten Arbeitsvorrat zu. Signierte und gesiegelte Dateien werden in der Trefferliste gesondert gekennzeichnet.

Ist der Funktionskreis zur Nutzung des DZAB aktiviert, wird auf Ebene des Schriftstücks zusätzlich der Metadatenkarteireiter „DZAB Beweiswerterhaltung“ angezeigt.

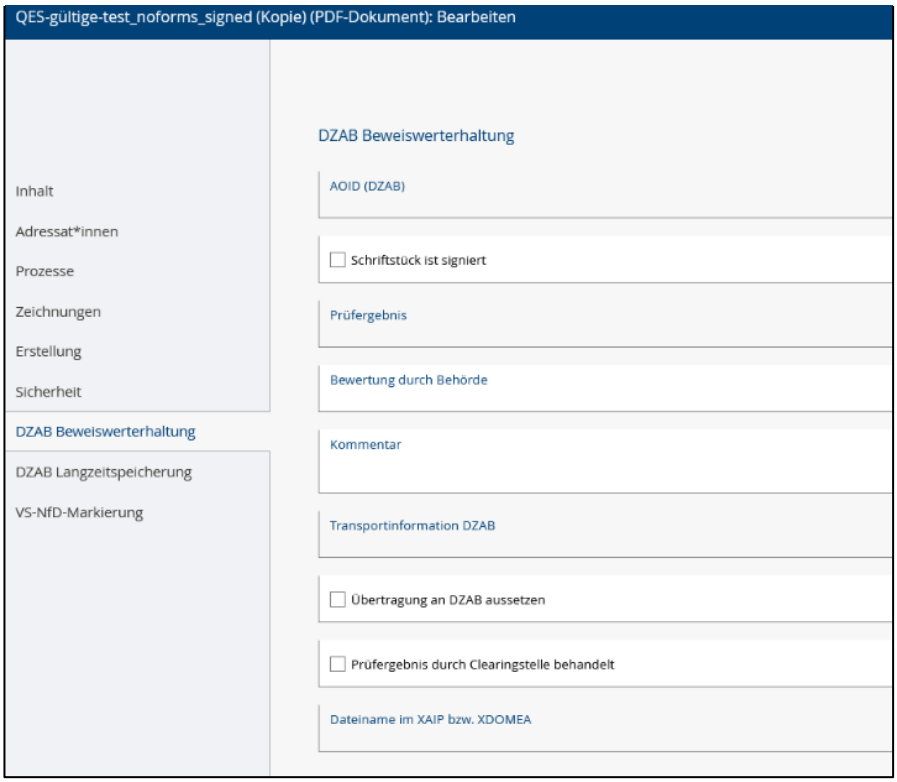


Abbildung 2: Metadatenkarteireiter DZAB Beweiswerterhaltung

Die dort verortete Checkbox „Schriftstück ist signiert“ ist bei Nutzung des SSI ab der Version 3.0 automatisch gesetzt; bei älteren SSI-Versionen muss sie manuell gesetzt werden. Eine vorherige Veraktung ist dafür nicht erforderlich.

5.2 Frühzeitige Beweiswerterhaltung

Der Übergang in das DZAB setzt bewusst früh an: Der Beweiswert wird bereits während der laufenden Verarbeitung gesichert und nicht erst beim Abschluss des Vorgangs. Andernfalls entstünde zwischen Scannen und Aussonderung eine Lücke von möglicherweise mehreren Jahren, in der der

Nachweis allein auf dem ursprünglichen Siegel beruhen würde.

Ein Job der E-Akte Bund sucht regelmäßig nach allen gesiegelten Schriftstücken, denen noch keine AOID zugeordnet ist und stößt für diese die Auslagerung an.

Der weitere Ablauf erfolgt ohne manuelle Tätigkeiten: Die Datei wird bitgleich dupliziert, die Kopie nach den Vorgaben der TR-ESOR in ein XAIP überführt und an den Schließfach-Mandanten übergeben. Das DZAB prüft das kryptografische Siegel, lagert das XAIP bei positivem Ergebnis ein und meldet die AOID sowie das Prüfergebnis an die E-Akte Bund zurück.

Das Schriftstück selbst verbleibt in der E-Akte Bund und kann weiterverarbeitet werden. Zu beachten ist, dass Änderungen am Schriftstück zur Ungültigkeit des Siegels führen; die eingelagerte Kopie bleibt davon unberührt.

Über die zurückgemeldete AOID kann der Beweiswert des eingelagerten gesiegelten Dokuments jederzeit direkt im DZAB abgerufen werden. Verlief die Siegelprüfung nicht positiv, kann die Behörde den Sachverhalt über die Metadatenfelder „Bewertung durch Behörde“, „Kommentar“ und „Prüfergebnis durch Clearingstelle behandelt“ rechtlich und formell einordnen.

5.3 Veraktung und Fristen

Unabhängig von der Beweiswerterhaltung werden die Schriftstücke verarbeitet, mit Metadaten versehen und Vorgängen zugeordnet. Ist die Verarbeitung abgeschlossen, wird der Vorgang abgeschlossen und damit zu den Akten (zdA) verfügt. Dabei werden die Transferfrist und die Aufbewahrungsfrist gesetzt. Mit diesen beiden Angaben steuert die Nutzerbehörde den gesamten Abschnitt C, ohne weitere Eingriffe vornehmen zu müssen.

6 Abschnitt C: Auslagerung in das DZAB

Dieser Abschnitt umfasst die Langzeitspeicherung des abgeschlossenen Vorgangs und dessen Löschung. Er läuft vollständig automatisiert ab.

6.1 Auslagerung nach Ablauf der Transferfrist

HINWEIS: Das folgende beschriebene Verfahren kann in der E-Akte Bund erst ab der Version 5.26.x genutzt werden.

Ein Job der E-Akte Bund sucht regelmäßig nach Vorgängen mit abgelaufener Transferfrist. Für diese werden zunächst die bereits im Schließfach-Mandanten liegenden XAIP angefordert und zurück übertragen; im Schließfach-Mandanten werden sie anschließend gelöscht, da sie dort nicht länger benötigt werden.

In der E-Akte Bund werden die zurück übertragenen XAIP mit allen weiteren, noch nicht ausgelagerten Schriftstücken des Vorgangs zusammengeführt. Auch diese werden in XAIP überführt. Der gesamte Vorgang wird als logische Einheit paketiert und an den Aussonderungsmandanten des DZAB übergeben.

6.2 Langzeitspeicherung und Zugriff

Das DZAB bestätigt die Annahme und speichert die Schriftstücke beweiswerterhaltend, soweit sie signiert sind.

Nach der Bestätigung stößt die E-Akte Bund die Bereinigung von Schriftstück-Zwischenversionen *(HINWEIS: Die hier beschrieben Bereinigung ist geplant und wurde noch nicht realisiert.)* der ausgelagerten Schriftstücke an. Im Ergebnis liegt der Vorgang, aufgeteilt in einer Struktur- und diversen Datei-XAIP, vollständig und als logische Einheit im DZAB vor.

Ausgelagerte Vorgänge bleiben über die E-Akte Bund zugänglich. Das Wiederauflebenlassen eines Vorgangs sowie die Anpassung von Fristen sind jederzeit möglich; ein direkter Zugriff auf das DZAB ist dafür nicht erforderlich.

6.3 Ende der Aufbewahrungsfrist

Ein Job der E-Akte Bund sucht regelmäßig nach Vorgängen, deren Aufbewahrungsfrist endet, und stößt die Löschung der betroffenen XAIP im DZAB an. Anschließend werden auch die in der E-Akte Bund verbliebenen Primär- und Metadaten des Vorgangs gelöscht. Zurück bleibt ein Eintrag in der Löschhistorie der übergeordneten Akte.

7 Beweiswerterhalt über den gesamten Lebenszyklus

7.1 Warum die Beweiskette trägt

Wird ein Papierdokument vernichtet, muss das Digitalisat an seine Stelle treten können – auch dann, wenn es Jahre später vor Gericht oder gegenüber einer Prüfstelle verwendet wird. Dafür genügt es nicht, die Datei sicher abzulegen. Es muss nachweisbar sein, dass sie seit dem Scannen unverändert geblieben ist.

Diesen Nachweis leisten zwei aufeinander aufbauende Elemente:

1. Das qualifizierte elektronische Siegel sichert die Integrität des Digitalisats im Moment des Scannens.
2. Das DZAB übernimmt die Digitalisate physisch, siegelt sie bei der Übernahme erneut und erneuert Zeitstempel und Hashwerte, sobald die verwendeten kryptografischen Verfahren an Sicherheit verlieren.

Der zweite Punkt ist der Grund, weshalb das DZAB anzubinden ist. Wird der ursprünglich verwendete Hash-Algorithmus unsicher, müssen die Hashwerte neu berechnet werden – dafür werden die Digitalisate selbst benötigt. Nur das DZAB verfügt dauerhaft über sie. Ein Verfahren, das lediglich Prüfsummen vorhält, kann diese Erneuerung nicht leisten und sichert den Beweiswert nur so lange dem verwendeten Verfahren vertraut wird.

Solange eine Nutzerbehörde das DZAB noch nicht angebunden hat, steht eine Übergangslösung zur Verfügung. Ihre Voraussetzungen, ihre Grenzen und die damit verbundene Verantwortung der Nutzerbehörde sind in Anlage 2 beschrieben.

7.2 Der Evidence Record als Nachweis

Ein Evidence Record ist der Nachweis, dass ein bestimmtes Digitalisat seit dem Zeitpunkt des ersetzenden Scannens unverändert geblieben ist. Er wird benötigt, wenn die Echtheit eines Digitalisats zweifelsfrei nachgewiesen werden muss oder wenn Zweifel an der Sicherheit des verwendeten Zertifikats bestehen.

Für Schriftstücke, die im DZAB eingelagert sind, wird der Evidence Record über das DZAB

bereitgestellt. Benötigt wird dafür die im Metadatenfeld „AOID (DZAB)“ hinterlegte Kennung, unter der das Objekt im DZAB gespeichert ist. Weil das DZAB die Erneuerung von Zeitstempeln und Hashwerten fortlaufend dokumentiert, umfasst der Nachweis den gesamten Zeitraum seit der Einlagerung.

Für Digitalisate, die noch nicht im DZAB eingelagert werden können, beschreibt Anlage 2 den möglichen übergangsweisen Weg.

8 Anlagen

8.1 Anlage 1: Gesamtprozess

Der Gesamtprozess „E-Akte Bund – E-Scannen – DZAB“ wurde als eigenständige BPMN-Prozessdarstellung (Datei: 20260920_Gesamtprozess-Darstellung E-Scannen-EAB-DZAB_v1.bpmn) erstellt.

8.2 Anlage 2: Beweiswerterhaltung ohne Anbindung an das DZAB

8.2.1 Ausgangslage

Die Beschreibung des Gesamtprozesses geht vom Regelfall aus: Die Digitalisate werden in der E-Akte Bund gespeichert und von dort an das DZAB übergeben. In der Praxis der Einführung ist dieser Weg jedoch nicht in allen Fällen von Beginn an verfügbar. Zwei Konstellationen treten auf:

- Die Digitalisate werden nicht in die E-Akte Bund, sondern über eine andere Schnittstelle in ein anderes Zielsystem übergeben, das noch nicht an das DZAB angeschlossen ist.
- Die Digitalisate werden in die E-Akte Bund übergeben, für die der Funktionskreis zur Nutzung des DZAB noch nicht aktiviert ist.

In beiden Fällen ist die Integrität des Digitalisates zwar im Moment des Scannens durch ein qualifiziertes elektronisches Siegel gesichert, es steht aber kein Verfahren zur Verfügung, das diesen Nachweis bei Bedarf über die gesamte Aufbewahrungsdauer erneuert. Für diese Übergangszeit stellt die Maßnahme E-Scannen ein eigenes Verfahren bereit.

8.2.2 Das Hashbaum-Verfahren der Maßnahme E-Scannen

Die gesiegelten Hashwerte der ersetzend gescannten Dokumente werden auf dem SAK-Server in Hashbäumen organisiert. Bei einem Hashbaum handelt es sich um eine Datenstruktur, in der die Hashwerte systematisch gespeichert und schrittweise zu übergeordneten Knoten verknüpft werden. Die einzelnen Dokumenthashwerte bilden die Blätter des Hashbaums, der eine beliebige Anzahl an Hashwerten aufnehmen kann.

Täglich wird aus den Blättern ein Root-Hash berechnet, der stellvertretend für alle darunterliegenden Hashwerte steht. Dieser Root-Hash wird mit einem qualifizierten Zeitstempel eines Vertrauensdiensteanbieters signiert, wodurch der Hashbaum abgeschlossen wird. Damit lässt sich nachweisen, dass die erfassten Dokumente zum Zeitpunkt der Zeitstempelung unverändert vorlagen. Die Integrität der Digitalisate ist auf diese Weise bereits ab dem Zeitpunkt der Sicherung gewährleistet und nicht erst mit der Überführung in einen auf der TR-ESOR basierenden Speicher.

Wird ein Nachweis benötigt, übermittelt die Behörde die zu prüfende Datei an das ITZBund. Dort wird ihr Hashwert gebildet und im Hashbaum gesucht. Wird er gefunden, exportiert der SAK-Server den betreffenden Ast des Hashbaums bis zum Wurzelknoten einschließlich aller zugehörigen Zeitstempel. Aus diesem Evidence Record und der gesiegelten Datei wird ein Signaturprüfbericht erstellt, den das ITZBund an die Behörde übermittelt.

8.2.3 Warum das Verfahren nur übergangsweise trägt

Die Sicherheit der eingesetzten kryptografischen Verfahren wird fortlaufend neu bewertet. Gelten bestimmte Algorithmen oder Schlüssellängen nicht mehr als ausreichend sicher, müssen stärkere Verfahren oder längere Schlüssel eingesetzt werden. Dabei sind zwei Ebenen zu unterscheiden: Wird das Signaturverfahren des Zeitstempels unsicher, muss der vorhandene Zeitstempel rechtzeitig durch einen neuen qualifizierten Zeitstempel übersigniert werden (Zeitstempelerneuerung). Wird der eingesetzte Hashalgorithmus unsicher, müssen die archivierten Daten mit einem stärkeren Verfahren neu gehasht und der Hashbaum neu gebildet werden (Hashbaumerneuerung).

Die TR-ESOR fordert unter Bezugnahme auf das Vertrauensdienstegesetz (VDG), dass eine erneute Signatur, ein erneutes Siegel oder ein erneuter Zeitstempel rechtzeitig erfolgen muss, das heißt vor Ablauf der Sicherheitseignung der verwendeten Algorithmen und der zugehörigen Parameter. Die neue Sicherung muss zudem alle vorhandenen Signaturen, Siegel und Zeitstempel umschließen. § 15 VDG unterscheidet nicht danach, ob der Hash-Algorithmus, der Verschlüsselungsalgorithmus oder beide ihre sicherheitstechnische Eignung verloren haben. Der Bedarf einer Erneuerung entsteht folglich bereits dann, wenn eines von beiden unsicher zu werden droht.

Die Zeitstempelerneuerung kann das Hashbaum-Verfahren leisten. Die Hashbaumerneuerung kann es nicht: Sie setzt voraus, dass die Digitalisate selbst erneut gehasht werden können. Im Rahmen von E-Scannen speichert der SAK-Server jedoch ausschließlich die Dokument-Hashwerte, nicht die zugehörigen Dokumente. Sobald die verwendete Hashfunktion nicht mehr als sicher gilt, endet damit die Tragfähigkeit des Hashbaum-Verfahrens der Maßnahme E-Scannen.

Das DZAB unterliegt dieser Einschränkung nicht. Es übernimmt die gesiegelten Dokumente physisch, siegelt sie bei der Übernahme erneut qualifiziert und kann die Hashwerte jederzeit mit einer als sicher eingestuften Hashfunktion neu bilden. Der Beweiswerterhalt ist im DZAB dauerhaft gesichert.

8.2.4 Verantwortung der Nutzerbehörde

Nutzerbehörden sind grundsätzlich verpflichtet, das DZAB anzubinden und den Beweiswerterhalt ihrer Digitalisate darüber zu sichern. Das Hashbaum-Verfahren der Maßnahme E-Scannen ist keine gleichwertige Alternative, sondern eine Übergangslösung für den Zeitraum bis zur Anbindung.

Entscheidet sich eine Nutzerbehörde, Digitalisate übergangsweise allein über das Hashbaum-Verfahren abzusichern, trägt sie die Verantwortung für die daraus entstehenden Risiken. Dazu gehört insbesondere, dass der Beweiswert der betroffenen Digitalisate ab dem Zeitpunkt nicht mehr erneuert werden kann, zu dem die verwendete Hashfunktion als unsicher eingestuft wird. Wann dieser Zeitpunkt eintreten kann, kann niemand vorhersagen.

Für die Planung der Einführung folgt daraus: Der Zeitraum, in dem Digitalisate ohne Anbindung an das DZAB erzeugt werden, sollte so kurz wie möglich gehalten und dokumentiert werden. Die betroffenen Bestände sollten nachvollziehbar sein, damit sie bei einer späteren Anbindung nachträglich in das DZAB überführt werden können.