



OPS.1.2.2 Archivierung

1. Beschreibung

1.1. Einleitung

Die Archivierung spielt im Dokumentenmanagementprozess eine besondere Rolle. Denn es wird einerseits erwartet, dass die digitalen Dokumente bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sind. Andererseits soll ihre Vertraulichkeit und Integrität bewahrt bleiben. Zusätzlich muss der Kontext erhalten werden, damit der jeweilige gespeicherte Vorgang rekonstruierbar ist.

Während der gesamten Dauer der Langzeitspeicherung müssen daher entsprechende Maßnahmen zur Informationserhaltung und, falls erforderlich, Maßnahmen zur Beweiswerterhaltung umgesetzt werden.

Im deutschen informationstechnischen Sprachgebrauch wird mitunter der Begriff „elektronische Archivierung“ synonym zum Begriff „elektronische Langzeitspeicherung“ verwendet. Zur besseren Verständlichkeit wird in diesem Baustein daher allgemein nur von „Archivierung“ oder auch „digitalem Langzeitarchiv“ gesprochen. Ein IT-Verfahren zur Aufbewahrung elektronischer Dokumente wird als „Archivsystem“ bzw. „digitales Archiv“ oder „Langzeitspeicher“ bezeichnet. Die Aufbewahrungsdauer der Dokumente bemisst sich nach den rechtlichen und sonstigen Vorgaben sowie dem Anwendungszweck der Daten.

Der in diesem Baustein verwendete Begriff „Dokumente“ beinhaltet Daten und digitale Dokumente, sofern sie nicht ausdrücklich in anderer Bedeutung gebraucht werden.

Aus rechtlicher Sicht ist der Begriff „Archivierung“ in Deutschland durch die Archivgesetze des Bundes und der Länder konkretisiert und belegt. „Archivierung“ im juristisch korrekten Sinne betrifft allein Unterlagen der öffentlichen Verwaltung. Sie bezieht sich darauf, dass Unterlagen einer Behörde, sobald sie für deren Zwecke nicht mehr benötigt werden, ausgesondert und durch eine zuständige staatliche Einrichtung (Bundesarchiv) auf unbegrenzte Zeit verwahrt werden sollen (vergleiche §§ 1 und 2 BArchG). Diese Art der Archivierung ist von der in diesem Baustein betrachteten zeitlich beschränkten Aufbewahrung zu unterscheiden.

1.2. Zielsetzung

Der Baustein beschreibt, wie digitale Dokumente langfristig, sicher, unveränderbar und wieder reproduzierbar archiviert werden können. Dazu werden Anforderungen definiert, mit denen sich ein Archivsystem sicher planen, umsetzen und betreiben lässt.

Die Aufbewahrung von Papierdokumenten wird in diesem Baustein nicht betrachtet, es werden aber Anforderungen gestellt, wie diese digitalisiert und archiviert werden können.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.2.2 *Archivierung* ist auf den Informationsverbund einmal anzuwenden, wenn eine Langzeitarchivierung von elektronischen Dokumenten erfolgt. Dabei kann eine Langzeitarchivierung aufgrund von externen oder internen Vorgaben erforderlich sein oder es ist bereits ein System zur Langzeitarchivierung elektronischer Dokumente im Betrieb.

Der Baustein behandelt nicht die zeitlich unbegrenzte Archivierung im Sinne der Archivgesetze des Bundes und der Länder.

Der vorliegende Baustein beschreibt Sicherheitsmaßnahmen, mit denen elektronische Dokumente für die Langzeitspeicherung im Rahmen von geltenden Aufbewahrungsfristen aufbewahrt und erhalten werden können. Maßnahmen für eine operative Datensicherung werden in diesem Baustein nicht behandelt. Anforderungen dazu werden in CON.3 *Datensicherungskonzept* dargestellt.

Ein digitaler Langzeitspeicher besteht aus einzelnen Komponenten, z. B. einer Datenbank. Wie sich solche Komponenten detailliert sicher betreiben lassen, ist jedoch ebenfalls nicht Thema des vorliegenden Bausteins. Dazu sind zusätzlich die Anforderungen aus den entsprechenden Bausteinen, wie APP.4.3 *Relationale Datenbanken*, SYS.1.1 *Allgemeiner Server* sowie SYS.1.8 *Speicherlösungen*, zu berücksichtigen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.2 *Archivierung* von besonderer Bedeutung.

2.1. Überalterung von Archivsystemen

Archivierte Daten sollen typischerweise über einen sehr langen Zeitraum gespeichert bleiben. Während dieses Zeitraums können die zugrundeliegenden technischen Systemkomponenten, Speichermedien und Datenformate aber physisch oder technisch altern und dadurch unbrauchbar werden. Es können sich z. B. im Laufe der Zeit Probleme mit der Kompatibilität der verwendeten Datenformate ergeben.

Wird auf den Alterungsprozess nicht reagiert, ist langfristig damit zu rechnen, dass beispielsweise archivierte Rohdaten nicht mehr von den Archivmedien lesbar sind. Auch können archivierte Daten durch physische Fehler an Archivsystem und -medien verändert werden.

2.2. Unzureichende Ordnungskriterien für Archive

Elektronische Archive können sehr große Datenmengen enthalten. Die einzelnen Datensätze werden dabei nach bestimmten Ordnungskriterien abgelegt, die nach Indexdaten der Geschäftsanwendungen und Indexdaten des Archivsystems unterschieden werden. Werden ungeeignete Ordnungskriterien verwendet, können archivierte Dokumente eventuell nicht mehr oder nur sehr aufwändig recherchiert werden. Auch ist es möglich, dass die Semantik der Dokumente nicht eindeutig bestimmbar ist. Durch eine ungeeignete oder begrenzte Auswahl von Ordnungskriterien könnten auch die Ziele der Aufbewahrung verfehlt werden, z. B. die Nachweisfähigkeit gegenüber Dritten.

2.3. Unbefugte Archivzugriffe aufgrund unzureichender Protokollierung

Unbefugte Archivzugriffe werden üblicherweise mithilfe von Protokolldateien aufgedeckt. Wurde jedoch nicht umfangreich genug protokolliert, könnten solche Zugriffe nicht entdeckt werden. In der Folge könnten Angreifende unbemerkt an die dort gespeicherten Informationen gelangen und sie z. B. kopieren oder verändern.

2.4. Unzulängliche Übertragung von Papierdaten in ein elektronisches Archiv

Wenn Dokumente eingescannt werden, kann dabei das Erscheinungsbild oder die Semantik der aufgenommenen Daten verfälscht werden. Auch können dabei Dokumente verloren gehen. Dadurch können die Informationen im Dokument falsch interpretiert und berechnet werden, z. B. wenn wichtige Teile des Dokuments oder des Dokumentenstapels beim Scannen vergessen werden.

2.5. Unzureichende Erneuerung von kryptografischen Verfahren bei der Archivierung

Kryptografische Verfahren, die z. B. bei Signaturen, Siegeln, Zeitstempeln, technischen Beweisdaten (Evidence Records) oder Verschlüsselungen verwendet werden, müssen regelmäßig an den aktuellen Stand der Technik angepasst werden, damit die Schutzwirkung erhalten bleibt. Geschieht dies nicht, kann beispielsweise aufgrund einer veralteten unsicheren Signatur die Integrität des Dokumentes nicht mehr garantiert werden. Darüber hinaus wird die Datei eventuell nicht als Beweismittel vor Gericht zugelassen, selbst wenn das Dokument noch völlig korrekt ist. Auch geht so die Vertraulichkeit eines verschlüsselten Dokumentes verloren.

2.6. Unzureichende Revisionen der Archivierung

Wenn der Archivierungsprozess zu selten oder zu ungenau überprüft wird, kann dies dazu führen, dass die Fehlfunktionen nicht erkannt werden. Damit kann die Integrität der archivierten Dokumente selbst angezweifelt werden. Hieraus können sich für die Institution rechtliche und wirtschaftliche Nachteile ergeben: So kann unter Umständen eine Datei nicht als Beweismittel vor Gericht zugelassen werden, weil nicht ausgeschlossen werden kann, dass sie manipuliert wurde.

2.7. Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivierung

Bei der Archivierung von elektronischen Dokumenten sind verschiedene rechtliche Rahmenbedingungen zu beachten. Werden diese nicht eingehalten, kann das zivil- oder strafrechtliche Konsequenzen haben, z. B. bei Mindestaufbewahrungsfristen, die sich aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen ergeben.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.2 *Archivierung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Fachverantwortliche
Weitere Zuständigkeiten	Benutzende, IT-Betrieb, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.2.2.A1 Ermittlung von Einflussfaktoren für die elektronische Archivierung (B)

Bevor entschieden wird, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden, MÜSSEN die technischen, rechtlichen und organisatorischen Einflussfaktoren ermittelt und dokumentiert werden. Die Ergebnisse MÜSSEN in das Archivierungskonzept einfließen.

OPS.1.2.2.A2 Entwicklung eines Archivierungskonzepts (B)

Es MUSS definiert werden, welche Ziele mit der Archivierung erreicht werden sollen. Hierbei MUSS insbesondere berücksichtigt werden, welche Regularien einzuhalten sind, welche Mitarbeitende zuständig sind und welcher Funktions- und Leistungsumfang angestrebt wird.

Die Ergebnisse MÜSSEN in einem Archivierungskonzept erfasst werden. Die Institutionsleitung MUSS in diesen Prozess einbezogen werden. Das Archivierungskonzept MUSS regelmäßig an die aktuellen Gegebenheiten der Institution angepasst werden.

OPS.1.2.2.A3 Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien (B) [IT-Betrieb]

Die IT-Komponenten eines Archivsystems MÜSSEN in gesicherten Räumen aufgestellt werden. Es MUSS sichergestellt sein, dass nur berechtigte Personen die Räume betreten dürfen. Archivspeichermedien MÜSSEN geeignet gelagert werden.

OPS.1.2.2.A4 Konsistente Indizierung von Daten bei der Archivierung (B) [IT-Betrieb, Benutzende]

Alle in einem Archiv abgelegten Daten, Dokumente und Datensätze MÜSSEN eindeutig indiziert werden. Dazu MUSS bereits während der Konzeption festgelegt werden, welche Struktur und welchen Umfang die Indexangaben für ein Archiv haben sollen.

OPS.1.2.2.A5 Regelmäßige Aufbereitung von archivierten Datenbeständen (B) [IT-Betrieb]

Über den gesamten Archivierungszeitraum hinweg MUSS sichergestellt werden, dass

- das verwendete Datenformat von den benutzten Anwendungen verarbeitet werden kann,
- die gespeicherten Daten auch zukünftig lesbar und so reproduzierbar sind, dass Semantik und Beweiskraft beibehalten werden,
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
- die Speichermedien jederzeit technisch einwandfrei gelesen werden können sowie

- die verwendeten kryptografischen Verfahren zur Verschlüsselung und zum Beweiswerterhalt mittels digitaler Signatur, Siegel, Zeitstempel oder technischen Beweisdaten (Evidence Records) dem Stand der Technik entsprechen.

OPS.1.2.2.A6 Schutz der Integrität der Indexdatenbank von Archivsystemen (B) [IT-Betrieb]

Die Integrität der Indexdatenbank MUSS sichergestellt und überprüfbar sein. Außerdem MUSS die Indexdatenbank regelmäßig gesichert werden. Die Datensicherungen MÜSSEN wiederherstellbar sein. Mittlere und große Archive SOLLTEN über redundante Indexdatenbanken verfügen.

OPS.1.2.2.A7 Regelmäßige Datensicherung der System- und Archivdaten (B) [IT-Betrieb]

Alle Archivdaten, die zugehörigen Indexdatenbanken sowie die Systemdaten MÜSSEN regelmäßig gesichert werden (siehe CON.3 *Datensicherungskonzept*).

OPS.1.2.2.A8 Protokollierung der Archivzugriffe (B) [IT-Betrieb]

Alle Zugriffe auf elektronische Archive MÜSSEN protokolliert werden. Dafür SOLLTEN Datum, Uhrzeit, Benutzender, Client und die ausgeführten Aktionen sowie Fehlermeldungen aufgezeichnet werden. Im Archivierungskonzept SOLLTE festgelegt werden, wie lange die Protokolldaten aufbewahrt werden.

Die Protokolldaten der Archivzugriffe SOLLTEN regelmäßig ausgewertet werden. Dabei SOLLTEN die institutionsinternen Vorgaben beachtet werden.

Auch SOLLTE definiert sein, welche Ereignisse welchen Mitarbeitenden angezeigt werden, wie z. B. Systemfehler, Timeouts oder wenn Datensätze kopiert werden. Kritische Ereignisse SOLLTEN sofort nach der Erkennung geprüft und, falls nötig, weiter eskaliert werden.

OPS.1.2.2.A9 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten (B) [IT-Betrieb]

Für die Archivierung MUSS ein geeignetes Datenformat ausgewählt werden. Es MUSS gewährleisten, dass sich Archivdaten sowie ausgewählte Merkmale des ursprünglichen Dokumentmediums langfristig und originalgetreu reproduzieren lassen.

Die Dokumentstruktur des ausgewählten Datenformats MUSS eindeutig interpretierbar und elektronisch verarbeitbar sein. Die Syntax und Semantik der verwendeten Datenformate SOLLTE dokumentiert und von einer Standardisierungsorganisation veröffentlicht sein. Es SOLLTE für eine beweis- und revisionssichere Archivierung ein verlustfreies Bildkompressionsverfahren benutzt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.2.2.A10 Erstellung einer Richtlinie für die Nutzung von Archivsystemen (S) [IT-Betrieb]

Es SOLLTE sichergestellt werden, dass Mitarbeitende das Archivsystem so benutzen, wie es im Archivierungskonzept vorgesehen ist. Dazu SOLLTE eine Administrations- und eine Benutzungsrichtlinie erstellt werden. Die Administrationsrichtlinie SOLLTE folgende Punkte enthalten:

- Festlegung der Verantwortung für Betrieb und Administration,

- Vereinbarungen über Leistungsparameter beim Betrieb (unter anderem Service Level Agreements),
- Modalitäten der Vergabe von Zutritts- und Zugriffsrechten,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Regelungen zum Umgang mit archivierten Daten und Archivmedien,
- Überwachung des Archivsystems und der Umgebungsbedingungen,
- Regelungen zur Datensicherung,
- Regelungen zur Protokollierung sowie
- Trennung von Produzenten und Konsumenten (OAIS-Modell).

OPS.1.2.2.A11 Einweisung in die Administration und Bedienung des Archivsystems (S) [IT-Betrieb, Benutzende]

Die zuständigen Mitarbeitende des IT-Betriebs und die Benutzenden SOLLTEN für ihren Aufgabenbereich geschult werden.

Die Schulung der Mitarbeitenden des IT-Betriebs SOLLTE folgende Themen umfassen:

- Systemarchitektur und Sicherheitsmechanismen des verwendeten Archivsystems und des darunterliegenden Betriebssystems,
- Installation und Bedienung des Archivsystems und Umgang mit Archivmedien,
- Dokumentation der Administrationstätigkeiten sowie
- Eskalationsprozeduren.

Die Schulung der Benutzende SOLLTE folgende Themen umfassen:

- Umgang mit dem Archivsystem,
- Bedienung des Archivsystems sowie
- rechtliche Rahmenbedingungen der Archivierung.

Die Durchführung der Schulungen sowie die Teilnahme SOLLTEN dokumentiert werden.

OPS.1.2.2.A12 Überwachung der Speicherressourcen von Archivmedien (S) [IT-Betrieb]

Die auf den Archivmedien vorhandene freie Speicherkapazität SOLLTE kontinuierlich überwacht werden. Sobald ein definierter Grenzwert unterschritten wird, MÜSSEN zuständige Mitarbeitende automatisch alarmiert werden. Die Alarmierung SOLLTE rollenbezogen erfolgen. Es MÜSSEN immer ausreichend leere Archivmedien verfügbar sein, um Speicherengpässen schnell vorbeugen zu können.

OPS.1.2.2.A13 Regelmäßige Revision der Archivierungsprozesse (S)

Es SOLLTE regelmäßig überprüft werden, ob die Archivierungsprozesse noch korrekt und ordnungsgemäß funktionieren. Dazu SOLLTE eine Checkliste erstellt werden, die Fragen zu Verantwortlichkeiten, Organisationsprozessen, zum Einsatz der Archivierung, zur Redundanz der Archivdaten, zur Administration und zur technischen Beurteilung des Archivsystems enthält. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

OPS.1.2.2.A14 Regelmäßige Beobachtung des Marktes für Archivsysteme (S) [IT-Betrieb]

Der Markt für Archivsysteme SOLLTE regelmäßig und systematisch beobachtet werden. Dabei SOLLTEN unter anderem folgende Kriterien beobachtet werden:

- Veränderungen bei Standards,
- Wechsel der Technik bei herstellenden Unternehmen von Hard- und Software,
- veröffentlichte Sicherheitslücken oder Schwachstellen sowie
- der Verlust der Sicherheitseignung bei kryptografischen Algorithmen.

OPS.1.2.2.A15 Regelmäßige Aufbereitung von kryptografisch gesicherten Daten bei der Archivierung (S) [IT-Betrieb]

Es SOLLTE kontinuierlich beobachtet werden, wie sich das Gebiet der Kryptografie entwickelt, um beurteilen zu können, ob ein Algorithmus weiterhin zuverlässig und ausreichend sicher ist (siehe auch OPS.1.2.2.A20 *Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung*).

Archivdaten, die mit kryptografischen Verfahren gesichert wurden, die sich in absehbarer Zeit nicht mehr zur Sicherung eignen werden, SOLLTEN rechtzeitig mit geeigneten Verfahren neu gesichert werden.

OPS.1.2.2.A16 Regelmäßige Erneuerung technischer Archivsystem-Komponenten (S) [IT-Betrieb]

Archivsysteme SOLLTEN über lange Zeiträume auf dem aktuellen technischen Stand gehalten werden. Neue Hard- und Software SOLLTE vor der Installation in einem laufenden Archivsystem ausführlich getestet werden. Wenn neue Komponenten in Betrieb genommen oder neue Dateiformate eingeführt werden, SOLLTE ein Migrationskonzept erstellt werden. Darin SOLLTEN alle Änderungen, Tests und erwarteten Testergebnisse beschrieben sein. Die Konvertierung der einzelnen Daten SOLLTE dokumentiert werden (Transfervermerk).

Wenn Archivdaten in neue Formate konvertiert werden, SOLLTE geprüft werden, ob die Daten aufgrund rechtlicher Anforderungen zusätzlich in ihren ursprünglichen Formaten zu archivieren sind.

OPS.1.2.2.A17 Auswahl eines geeigneten Archivsystems (S) [IT-Betrieb]

Ein neues Archivsystem SOLLTE immer auf Basis der im Archivierungskonzept beschriebenen Vorgaben ausgewählt werden. Es SOLLTE die dort formulierten Anforderungen erfüllen.

OPS.1.2.2.A18 Verwendung geeigneter Archivmedien (S) [IT-Betrieb]

Für die Archivierung SOLLTEN geeignete Medien ausgewählt und benutzt werden. Dabei SOLLTEN folgende Aspekte berücksichtigt werden:

- das zu archivierende Datenvolumen,
- die mittleren Zugriffszeiten sowie
- die mittleren gleichzeitigen Zugriffe auf das Archivsystem.

Ebenfalls SOLLTEN die Archivmedien die Anforderungen an eine Langzeitarchivierung hinsichtlich Revisionssicherheit und Lebensdauer erfüllen.

OPS.1.2.2.A19 Regelmäßige Funktions- und Recoverytests bei der Archivierung (S) [IT-Betrieb]

Für die Archivierung SOLLTEN regelmäßige Funktions- und Recoverytests durchgeführt werden. Die Archivierungsdatenträger SOLLTEN mindestens einmal jährlich daraufhin überprüft werden, ob sie noch lesbar und integer sind. Für die Fehlerbehebung SOLLTEN geeignete Prozesse definiert werden.

Weiterhin SOLLTEN die Hardwarekomponenten des Archivsystems regelmäßig auf ihre einwandfreie Funktion hin geprüft werden. Es SOLLTE regelmäßig geprüft werden, ob alle Archivierungsprozesse fehlerfrei funktionieren.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.2.2.A20 Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung (H) [IT-Betrieb]

Um lange Aufbewahrungsfristen abdecken zu können, SOLLTEN Archivdaten nur mit kryptografischen Verfahren auf Basis aktueller Standards und Normen gesichert werden.

OPS.1.2.2.A21 Übertragung von Papierdaten in elektronische Archive (H)

Werden z. B. Dokumente auf Papier digitalisiert und in ein elektronisches Archiv überführt, SOLLTE sichergestellt werden, dass die digitale Kopie mit dem Originaldokument bildlich und inhaltlich übereinstimmt.

4. Weiterführende Informationen

4.1. Wissenswertes

Die Bundesnetzagentur (BNetzA) listet in ihrer Veröffentlichung „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung: Auflistung geeigneter Algorithmen und Parameter“ als geeignet eingestufte Algorithmen und Parameter auf.

Das Deutsche Institut für Normung e. V. (DIN) definiert in der DIN 31644:2012-04 „Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive“ Kriterien für vertrauenswürdige digitale Langzeitarchive. In der DIN 31647:2015-05 „Information und Dokumentation - Beweiserhaltung kryptographisch signierter Dokumente“ werden technische und sicherheitsrelevante Anforderungen an die langfristige Aufbewahrung von digital signierten Dokumenten unter Wahrung der Rechtskraft der digitalen Signatur definiert.

Das BSI hat in seiner technischen Richtlinie „BSI TR-03138 RESISCAN: Ersetzendes Scannen“ die sicherheitsrelevanten technischen und organisatorischen Maßnahmen, die beim ersetzenden Scannen zu berücksichtigen sind, zusammengestellt.

In der technischen Richtlinie „BSI TR-03125 TR-ESOR: Beweiserhaltung kryptographisch signierter Dokumente“ nebst seinen Anhängen stellt das BSI einen Leitfaden zur Verfügung, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume, bis zum Ende der Aufbewahrungsfristen, im Sinne eines rechtswirksamen Beweiserhalts vertrauenswürdig gespeichert werden können.