

Muster-Verfahrens-dokumentation für das Scannen von Urkunden

Bundesnotarkammer

Körperschaft des öffentlichen Rechts

|  |  |
| --- | --- |
| ***Version:*** | ***1.3*** |
| ***Erscheinungsdatum:*** | ***6. November 2024*** |

Dokumenthistorie

|  |  |  |
| --- | --- | --- |
| Version | Datum | Beschreibung |
| **1.0** | **11. November 2021** |  |
| **1.1** | **9. Mai 2022** | Korrektur: Einführung der elektronischen Urkundensammlung am 1. Juli 2022 (Abschnitt 2.2)  Korrektur: Nachträgliches Drehen von Seiten in XNP ist doch möglich (Abschnitt 2.5.3 unter „Nachbearbeitung“)  Löschung des Veröffentlichungszeitpunktes der Handreichung „IT-Sicherheit für Notarinnen und Notare“ (Abschnitte 3.2.2.2, 3.2.2.4 und 3.5.3) |
| **1.2** | **5. August 2022** | Klarstellung: Das nachträgliche Drehen von Seiten muss nicht zwingend im Übereinstimmungsvermerk dokumentiert werden, insbesondere dann nicht, wenn es der Korrektur von automatischen Drehungen durch das Scansystem dient.  (Abschnitt 2.5.3 unter „Nachbearbeitung“) |
| **1.3** | **6. November 2024** | Ergänzung des Ausnahmefalls von Einzelnotarinnen und Einzelnotaren (Abschnitt 2.5.4)  Ergänzung zu der Aufnahme des Ergebnisses der Qualitätssicherung in den Übereinstimmungsvermerk (Abschnitt 2.5.4)  Verlinkung der Handreichung „IT-Sicherheit für Notarinnen und Notare“ (Abschnitte 3.2.2.2, 3.2.2.4 und 3.5.3) sowie der Schulungsunterlagen (Abschnitt 3.2.2.1)  Aktualisierung des Titels „Grundlegende Sicherheitsmaßnahmen im Scanprozess“ (Abschnitt 3.3.1) |

Vorbemerkung

Das vorliegende Dokument ist das Muster einer Verfahrensdokumentation für die Umsetzung des Scanverfahrens nach dem Stand der Technik im Sinne von § 56 Abs. 1 BeurkG. Dieses Muster wurde aus der Verfahrensdokumentation der Bundesnotarkammer zum Scannen von Urkunden entwickelt, die im Rahmen der Zertifizierung eines rechtskonformen Prozesses für das Scannen von Urkunden unter Berücksichtigung der Technischen Richtlinie 03138 − Ersetzendes Scannen (RESISCAN) des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Musternotariat erstellt wurde.

Diese Muster-Verfahrensdokumentation dient als Vorlage für die Ausgestaltung eines Scan-Verfahrens nach dem Stand der Technik im Sinne von § 56 Abs. 1 BeurkG[[1]](#footnote-2) im einzelnen Notarbüro. Die Notarin / der Notar füllt dieses Muster entsprechend den Gegebenheiten in seinem Notarbüro aus (grau hinterlegte Kästchen). Da die Ausfüllvorschläge und das Muster aus der zertifizierten Verfahrensdokumentation entwickelt sind, erlauben sie die Darlegung, dass die Vorgaben der RESISCAN eingehalten sind. Bei individuellen Abweichungen muss die Vereinbarkeit mit der RESISCAN ggf. selbst dargelegt werden.

Inhalt

[1. Einleitung 7](#_Toc84590079)

[2. Grundlegende Anforderungen 8](#_Toc84590080)

[2.1 Organisatorisches Umfeld 8](#_Toc84590081)

[2.2 Rechtliche Rahmenbedingungen 8](#_Toc84590082)

[2.3 Art der verarbeiteten Dokumente 9](#_Toc84590083)

[2.4 Nicht verarbeitbare und nicht zu verarbeitende Dokumente 9](#_Toc84590084)

[2.5 Der Scanprozess 10](#_Toc84590085)

[2.5.1 Dokumentenvorbereitung 11](#_Toc84590086)

[2.5.2 Scannen 14](#_Toc84590087)

[2.5.3 Nachverarbeitung 17](#_Toc84590088)

[2.5.4 Integritätssicherung 18](#_Toc84590089)

[2.5.5 Typische Fehlerquellen und Empfehlungen 19](#_Toc84590090)

[2.5.6 Aufbewahrung und Übergabe an das Elektronische Urkundenarchiv (Langzeitspeicher) 20](#_Toc84590091)

[2.5.7 Verbleib des Originals 20](#_Toc84590092)

[2.6 Das Scansystem 21](#_Toc84590093)

[2.6.1 Scannen 21](#_Toc84590094)

[2.6.2 Integritätssicherung 21](#_Toc84590095)

[3. Maßnahmen 23](#_Toc84590096)

[3.1 Organisatorische Maßnahmen 23](#_Toc84590097)

[3.1.1 Zuständigkeiten und Regelungen 23](#_Toc84590098)

[3.1.2 Dokumentenvorbereitung 23](#_Toc84590099)

[3.1.3 Scanvorgang 23](#_Toc84590100)

[3.1.4 Qualitätssicherung und Nachbearbeitung 24](#_Toc84590101)

[3.1.5 Integritätssicherung 24](#_Toc84590102)

[3.1.6 Übergabe an das Elektronische Urkundenarchiv 24](#_Toc84590103)

[3.1.7 Regelungen für die Administrations-, Wartungs- und Reparaturarbeiten 24](#_Toc84590104)

[3.1.8 Abnahme- und Freigabeverfahren für Hard- und Software 26](#_Toc84590105)

[3.1.9 Einhaltung der Informationssicherheit 27](#_Toc84590106)

[3.2 Personelle Maßnahmen 28](#_Toc84590107)

[3.2.1 Verpflichtung der Mitarbeiterinnen und Mitarbeiter 28](#_Toc84590108)

[3.2.2 Maßnahmen zur Qualifizierung und Sensibilisierung 28](#_Toc84590109)

[3.2.2.1 Einweisung zur ordnungsgemäßen Bedienung des Scansystems 28](#_Toc84590110)

[3.2.2.2 Einweisung zu Sicherheitsmaßnahmen im Scanprozess 29](#_Toc84590111)

[3.2.2.3 Schulung des Wartungs- und Administrationspersonals 29](#_Toc84590112)

[3.2.2.4 Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Informationssicherheit 30](#_Toc84590113)

[3.3 Technische Maßnahmen 31](#_Toc84590114)

[3.3.1 Grundlegende Sicherheitsmaßnahmen im Scanprozess 31](#_Toc84590115)

[3.3.2 Zulässige Kommunikationsverbindungen 31](#_Toc84590116)

[3.3.3 Schutz vor Schadprogrammen 32](#_Toc84590117)

[3.3.4 Zuverlässige Speicherung 33](#_Toc84590118)

[3.4 Sicherheitsmaßnahmen bei der Dokumentenvorbereitung 34](#_Toc84590119)

[3.4.1 Sorgfältige Vorbereitung der Papierdokumente 34](#_Toc84590120)

[3.4.2 Vorbereitung der Vollständigkeitsprüfung 34](#_Toc84590121)

[3.5 Sicherheitsmaßnahmen beim Scannen 34](#_Toc84590122)

[3.5.1 Auswahl und Beschaffung geeigneter Scangeräte 34](#_Toc84590123)

[3.5.2 Zutritts- und Zugriffskontrollen für Scangeräte 34](#_Toc84590124)

[3.5.3 Änderung voreingestellter Passwörter 35](#_Toc84590125)

[3.5.4 Sorgfältige Durchführung von Konfigurationsänderungen 36](#_Toc84590126)

[3.5.5 Geeignete Benutzung des Scangeräts 36](#_Toc84590127)

[3.5.6 Geeignete Scaneinstellungen 37](#_Toc84590128)

[3.5.7 Geeignete Erfassung von Metainformationen 37](#_Toc84590129)

[3.5.8 Qualitätssicherung der Scanprodukte 37](#_Toc84590130)

[3.5.9 Sichere Außerbetriebnahme von Scangeräten 38](#_Toc84590131)

[3.5.10 Informationsschutz und Zugriffsbeschränkung bei netzwerkfähigen Scangeräten 38](#_Toc84590132)

[3.5.11 Protokollierung beim Scannen 39](#_Toc84590133)

[3.5.12 Auswahl geeigneter Bildkompressionsverfahren 40](#_Toc84590134)

[3.6 Sicherheitsmaßnahmen bei der Nachverarbeitung 40](#_Toc84590135)

[3.6.1 Geeignete und nachvollziehbare Nachverarbeitung 40](#_Toc84590136)

[3.6.2 Qualitätssicherung der nachverarbeiteten Scanprodukte 41](#_Toc84590137)

[3.6.3 Durchführung der Vollständigkeitsprüfung 41](#_Toc84590138)

[3.6.4 Übereinstimmungsvermerk 41](#_Toc84590139)

[3.7 Sicherheitsmaßnahmen bei der Integritätssicherung 41](#_Toc84590140)

[3.7.1 Nutzung geeigneter Dienste und Systeme für den Integritätsschutz 41](#_Toc84590141)

[4. Aufbaumodule 41](#_Toc84590142)

[4.1 Generelle Maßnahmen bei erhöhtem Schutzbedarf 42](#_Toc84590143)

[4.1.1 Beschränkung des Zugriffs auf sensible Papierdokumente 42](#_Toc84590144)

[4.1.2 Pflicht zur Protokollierung beim Scannen 43](#_Toc84590145)

[4.1.3 Pflicht zur regelmäßigen Auditierung 43](#_Toc84590146)

[4.2 Zusätzliche Maßnahmen bei hohen Integritätsanforderungen 43](#_Toc84590147)

[4.2.1 Einsatz kryptographischer Mechanismen zum Integritätsschutz 43](#_Toc84590148)

[4.2.2 Geeignetes Schlüsselmanagement 43](#_Toc84590149)

[4.2.3 Auswahl eines geeigneten kryptographischen Verfahrens 43](#_Toc84590150)

[4.2.4 Auswahl eines geeigneten kryptographischen Produktes 44](#_Toc84590151)

[4.2.5 Langfristige Datensicherung bei Einsatz kryptographischer Verfahren 44](#_Toc84590152)

[4.2.6 Verhinderung ungesicherter Netzzugänge 44](#_Toc84590153)

[4.3 Zusätzliche Maßnahmen bei hohen Vertraulichkeitsanforderungen 44](#_Toc84590154)

[4.3.1 Sensibilisierung und Verpflichtung der Mitarbeitenden 44](#_Toc84590155)

[4.3.2 Verhinderung ungesicherter Netzzugänge 44](#_Toc84590156)

[4.3.3 Löschen von Zwischenergebnissen 44](#_Toc84590157)

[4.4 Zusätzliche Maßnahmen bei hohen Verfügbarkeitsanforderungen 45](#_Toc84590158)

[4.4.1 Erweiterte Qualitätssicherung 45](#_Toc84590159)

[4.4.2 Fehlertolerante Protokolle und redundante Datenhaltung 45](#_Toc84590160)

[5. Anlagenverzeichnis 45](#_Toc84590161)

# Einleitung

Diese Verfahrensdokumentation enthält die Festlegung der konkreten Maßnahmen, um die bildliche und inhaltliche Übereinstimmung von nach § 56 Abs. 1 BeurkG in die elektronische Form übertragenen Dokumenten mit der papierförmigen Vorlage nach dem Stand der Technik zu gewährleisten.

Für die Einrichtung, Durchführung und Änderung der Maßnahmen ist ausschließlich die Notarin / der Notar bzw. sind die Notare (Sozietät) verantwortlich. Im Falle einer Sozietät genügt die Erstellung einer gemeinsamen Muster-Verfahrensdokumentation.

|  |  |
| --- | --- |
| **Verantwortlichkeit** | |
| Verantwortliche Notarin/verantwortlicher Notar/verantwortliche Notare [im Falle einer Sozietät] | […] |

Das Dokument behält seine Gültigkeit bis zu einer Überarbeitung.

|  |  |
| --- | --- |
| **Verfahrensdokumentation zum Scanprozess** | |
| Freigabe am | [Datum der Fertigstellung und Freigabe des ausgefüllten Dokuments] |
| Freigabe durch | [verantwortliche Notarin / verantwortlicher Notar / verantwortliche Notare] |
| Version | 1.3 |
| Gültig ab | 6. November 2024 |

Diese Verfahrensdokumentation beinhaltet alle Maßnahmen und Verfahrensschritte, die für den Scanprozess in der Verantwortung der o.g. Notarin / des o.g. Notars gelten. Die beschriebenen Maßnahmen und Verfahren sind von allen Personen, die an den einzelnen Prozessschritten beteiligt sind sowie für diese unterwiesen und autorisiert wurden, zu befolgen. Sie soll sicherstellen, dass alle in § 56 Abs. 1 BeurkG genannten Vorgaben an die Übertragung von Originalurkunden in die elektronische Form eingehalten werden.

# Grundlegende Anforderungen

## 2.1 Organisatorisches Umfeld

In dieser Verfahrensdokumentation sind alle Prozesse und Regelungen im Zusammenhang mit dem Scanverfahren definiert. Diese Verfahrensdokumentation gilt für das folgende Notarbüro:

|  |  |
| --- | --- |
| **Notarbüro** | |
| Name | [Name der Notarin oder des Notars oder der Sozien und ggf. der Sozietät] |
| Anschrift | […] |
| Arbeitsorganisatorische Besonderheiten | […]  *Beispiele: Es sind keine arbeitsorganisatorischen Besonderheiten vorhanden. / Es besteht eine weitere Geschäftsstelle in [Ort 2]. Die dort entstehenden Urkunden werden zum Einscannen und zur Ausfertigung in die erste Geschäftsstelle in [Ort 1] verbracht. / Es besteht eine weitere Geschäftsstelle in [Ort 2]. Dort ist der Scanprozess auch vollständig realisiert. An den relevanten Stellen in dieser Dokumentation werden die sich daraus ergebenden Alternativen dargestellt.* |

## 

## 2.2 Rechtliche Rahmenbedingungen

Die Notwendigkeit der Übertragung von notariellen Urkunden in die elektronische Form ergibt sich rechtlich aus § 55 Abs. 3 BeurkG, wonach die Notarin / der Notar die im Urkundenverzeichnis registrierten Urkunden ab dem 1. Juli 2022 u. a. in einer elektronischen Urkundensammlung verwahrt; diese ist zu führen im Elektronischen Urkundenarchiv (§ 55 Abs. 2 BeurkG, § 78h BNotO).

Wie die Übertragung in die elektronische Form im Einzelnen zu erfolgen hat, bestimmt § 56 Abs. 1 BeurkG. Demnach muss durch geeignete Vorkehrungen nach dem Stand der Technik sichergestellt werden, dass die elektronischen Dokumente mit den in Papierform vorhandenen Schriftstücken inhaltlich und bildlich übereinstimmen. Diese Verfahrensdokumentation wurde erstellt, um den Nachweis der Einhaltung solcher Vorkehrungen nach dem Stand der Technik zu ermöglichen.

Die inhaltliche und bildliche Übereinstimmung ist von der Notarin / dem Notar in einem Vermerk unter Angabe des Orts und der Zeit seiner Ausstellung zu bestätigen (§ 56 Abs. 1 Satz 2 BeurkG); das elektronische Dokument und der Vermerk müssen mit einer qualifizierten elektronischen Signatur der Notarin / des Notars versehen werden, § 56 Abs. 1 Satz 3 BeurkG. Erst dann kann das elektronische Dokument in die elektronische Urkundensammlung eingestellt werden.

## 2.3 Art der verarbeiteten Dokumente

§ 34 Abs. 1 NotAktVV bestimmt, dass die Dokumente in der elektronischen Urkundensammlung zu verwahren sind, die auch in der Urkundensammlung gemäß § 31 NotAktVV verwahrt werden. Demnach müssen grundsätzlich die in § 31 Abs. 1 NotAktVV aufgezählten Dokumente und gegebenenfalls die nach § 31 Abs. 4 NotAktVV zusätzlich in der elektronischen Urkundensammlung zu verwahrenden Dokumente gemäß dem in § 56 Abs. 1 BeurkG beschriebenen Verfahren in die elektronische Form übertragen werden. Nach § 34 Abs. 2 Nr. 2 und 3 NotAktVV können bei Dokumenten, die keine Urschriften sind, anstelle der nach dem Scanprozess erstellten elektronischen Fassungen nach § 56 Abs. 1 BeurkG auch elektronisch beglaubigte Abschriften bzw. einfache elektronische Abschriften aufgenommen werden.

**Alle in die elektronische Urkundensammlung aufzunehmenden Dokumente werden nach der vorliegenden Verfahrensdokumentation in die elektronische Form übertragen. Ausnahmen werden nur im Einzelfall bestimmt.**

**Hinweis**: Diese Verfahrensdokumentation behandelt das Scanverfahren bei der Urschrift einer notariellen Urkunde gemäß § 45 Abs. 1 BeurkG. Für alle weiteren scanrelevanten Dokumententypen gehen die bestehenden Anforderungen nicht über diejenigen hinaus, die für notarielle Urschriften zu beachten sind.

## 2.4 Nicht verarbeitbare und nicht zu verarbeitende Dokumente

Urschriften von Verfügungen von Todes wegen (Erbverträge und Testamente) dürfen nach § 34 Abs. 4 BeurkG nicht in die elektronische Form übertragen werden. Zulässig ist hingegen die Aufnahme einer in die elektronische Form übertragenen beglaubigten Abschrift. Diese kann von einer zuvor erstellten beglaubigten Abschrift gemäß § 56 Abs. 1 BeurkG mittels des in dieser Verfahrensdokumentation beschriebenen Verfahren erstellt werden. Alternativ kann auch eine elektronische beglaubigte Abschrift der Urschrift gem. §§ 39a, 42 BeurkG erstellt werden, wofür § 56 BeurkG und wofür damit das in dieser Verfahrensdokumentation beschriebene Scanverfahren nicht angewandt werden muss.

Daneben kann eine Übertragung von Papierdokumenten in die elektronische Form gemäß § 37 Abs. 1 NotAktVV unterbleiben, wenn der Scanvorgang aufgrund der Beschaffenheit des Dokuments unmöglich oder unzumutbar ist. Die davon betroffenen Dokumente sind in Papierform in der Sondersammlung gemäß § 37 Abs. 3 NotAktVV zu verwahren.

**Exkurs:** Nach § 37 Abs. 2 Satz 2 NotAktVV soll in diesem Fall eine elektronisch beglaubigte Abschrift in die elektronische Urkundensammlung aufgenommen werden, wenn deren Herstellung zumutbar ist. Für die Herstellung dieser elektronisch beglaubigten Abschrift gilt weder § 56 Abs. 1 BNotO noch die Bindung an den vorliegenden Scanprozess. Es sind dann lediglich § 39a, § 42 BeurkG einzuhalten.

Die demnach nicht zu scannenden Dokumente werden im Rahmen der Dokumentenvorbereitung aussortiert. Sie werden jedoch (ggf. nur teilweise) in einem (ggfs. vereinfachten) Scanprozess gescannt, um eine (ggf. auszugsweise) elektronisch beglaubigte Abschrift zu erstellen.

|  |  |
| --- | --- |
| **Ablage der vom Scanprozess ausgenommenen Originalurkunden** | |
| Raum, Dokumentenablage | […]  *Beispiel: Die vom Scanprozess ausgenommenen Originalurkunden werden zunächst auf der Ablage […] in Raum […] abgelegt, bevor sie weiterbearbeitet werden.* |

## 2.5 Der Scanprozess

Der Scanprozess umfasst folgende Schritte:

* Dokumentenvorbereitung
* Scannen
* Nachverarbeitung
* Integritätssicherung

Die notarielle Urkunde kann gescannt werden, wenn die Niederschrift abgeschlossen ist. Das ist in der Regel der Fall, wenn die Urkundsbeteiligten und die Notarin / der Notar die Urkunde unterschrieben haben (zu Sonderfällen s. §§ 22 ff. BeurkG). Weiterhin muss **vor** dem Scannen die **Urkundenverzeichnisnummer** auf die Urkunde aufgebracht sein. Die Verbindung der Urkunde mit **Schnur und Prägesiegel** sollte erst **nach dem Scannen** erfolgen. Andernfalls muss entweder die Verbindung aufgehoben (und anschließend neu hergestellt) werden oder es muss mithilfe von spezieller Scan-Hardware gearbeitet werden, die gebundene Papierdokumente verarbeiten kann.

**Hinweis**: Nach Eintragung in das Urkundenverzeichnis sollen die notariellen Urkunden unverzüglich in die elektronische Urkundensammlung eingestellt und damit gescannt werden, § 35 Abs. 1 NotAktVV. Die Eintragung in das Urkundenverzeichnis soll ihrerseits zeitnah, spätestens 14 Tage nach der Beurkundung oder der sonstigen Amtshandlung vorgenommen werden, § 18 NotAktVV. Der Eingang beispielsweise von Genehmigungserklärungen oder Eintragungsmitteilungen darf nach dem Ermessen des Notars abgewartet werden, um diese zusammen mit der Urkunde in die elektronische Urkundensammlung aufnehmen zu können (vgl. BR-Drs. 420/20 (neu), S. 56). Es wird empfohlen, dass die Urkunden so früh wie möglich gescannt werden, spätestens, wenn mit dem (Erst-)Vollzug der Urkunde begonnen werden kann (z. B. weil alle zur Rechtswirksamkeit erforderlichen Genehmigungen eingegangen sind).

Die folgenden Festlegungen gelten ausnahmslos für alle notariellen Urkunden bzw. scanrelevanten Dokumente.

Die notariellen Urkunden sind vor Beginn der Dokumentenvorbereitung an dem folgenden Ort abgelegt:

|  |  |
| --- | --- |
| **Ablage der zu scannenden Urkunde** | |
| Raum, Dokumentenablage | […]  *Beispiele: Die für das Scannen vorgesehenen Urkunden werden vom Sachbearbeiter im Raum „Ausfertigung“ auf der Ablage „Vorbereitung Scannen“ abgelegt. / Die für das Scannen vorgesehen Urkunden werden nach Erfassung im Urkundenverzeichnis von dem zuständigen Mitarbeitenden (in der Regel Assistenz der Sachbearbeiterin / des Sachbearbeiters) für Referat 1 in Raum 0815, für Referat 2 im Raum 0816 und für Referat 3 im Raum 0817 jeweils auf der Ablage „Vorbereitung Scannen“ / „Scannen“ (wenn immer gleich nach Dokumentenvorbereitung gescannt wird) abgelegt.* |

### 2.5.1 Dokumentenvorbereitung

Bei der sorgfältigen Vorbereitung der Dokumente führen die in Anlage 1 genannten zuständigen Mitarbeiterinnen / Mitarbeiter die folgenden Prüfschritte durch:

* Überprüfung der Urkunde auf offensichtliche Manipulationen

Manipulationen können z. B. unrechtmäßige handschriftliche Ergänzungen sein, die nicht von der Notarin / vom Notar gekennzeichnet wurden.

|  |
| --- |
| **Überprüfung der Urkunde** |
| […]  *Beispiel: Alle Seiten der Urkunde werden sorgfältig auf Manipulationen, insbesondere auf nicht von der Notarin / dem Notar gekennzeichnete handschriftliche Ergänzungen oder sonstige Auffälligkeiten untersucht.* |

* Überprüfung der Scanfähigkeit

Es ist zu prüfen, ob die Urkunde mit dem zur Verfügung stehenden Scangerät gescannt werden kann, ohne dass eine Beschädigung der Seiten oder das Auslassen von Inhalten befürchtet werden muss. Urkunden, die aufgrund ihrer Beschaffenheit nicht gescannt werden können, sind gemäß § 37 Abs. 3 NotAktVV in der Sondersammlung zu verwahren.

* Bewahrung des logischen Kontextes der zu erfassenden Urkunden

Es sollten unverwechselbare Merkmale der Urkunde (wie z. B. die Urkundenverzeichnisnummer, Name der Urkundsbeteiligten) festgelegt werden, die im weiteren Verlauf auch für die Auswertung bzw. Weiterverarbeitung des Scanprodukts verwendet werden. Auf diese Weise ist die Zuordnung von Original zu Scanprodukt eindeutig möglich.

* Korrekte Orientierung der erfassten Blätter

Eine Nachbearbeitung wie ein Drehen der Seiten ist grundsätzlich nicht vorgesehen, daher sollten die Seiten der Urkunde gleich orientiert sein, d. h. der Text sollte in Leserichtung sichtbar sein. Falls nur einseitig gescannt wird, muss sichergestellt werden, dass die richtige Seite erfasst wird.

|  |
| --- |
| **Korrekte Seitenorientierung** |
| […]  *Beispiel: Es wird sorgfältig überprüft, ob alle Seiten der Urkunde in Leserichtung angeordnet sind.* |

* Bewahrung der korrekten Reihenfolge

Sofern es zu einer falschen Sortierung gekommen ist, werden die betroffenen Seiten der Urkunde wieder in die korrekte Reihenfolge gebracht. Das Ziel ist es, die Nachbearbeitung bzw. das Umsortieren des gescannten Dokuments zu vermeiden.

|  |
| --- |
| **Korrekte Seitenreihenfolge** |
| […]  *Beispiel: Anhand der auf der Urkunde aufgedruckten Seitenzahlen wird überprüft, ob alle Seiten der Urkunde in der richtigen Reihenfolge angeordnet sind.* *Sind Seitenzahlen nicht vorhanden, wird anhand des Textes am Seitenwechsel oder anhand des inhaltlichen Zusammenhangs überprüft, ob alle Seiten der Urkunde in der richtigen Reihenfolge angeordnet sind. Gegebenenfalls werden die Seiten in die korrekte Reihenfolge gebracht.* |

* Überprüfung der Vollständigkeit der Urkunde

Es ist sorgfältig zu überprüfen, ob die Urkunde vollständig ist. Dabei ist besonders darauf zu achten, dass alle Seiten der Urkunde und sämtliche Anlagen vorliegen.

|  |
| --- |
| **Überprüfung der Vollständigkeit** |
| […]  *Beispiel: Die Vollständigkeit der Urkunde wird anhand der aufgedruckten Seitenzahlen festgestellt. Es ist besonders zu überprüfen, ob sämtliche Anlagen zur Urkunde vorliegen.* *Sind keine Seitenzahlen angebracht, wird die Vollständigkeit der Urkunde durch die Überprüfung des inhaltlichen Zusammenhangs festgestellt.* |

* Zuverlässige Trennung von mehreren Urkunden

Sofern mehrere Urkunden gleichzeitig für das Scannen bereitliegen, muss gewährleistet sein, dass die Seiten der einzelnen Urkunden nicht miteinander vermischt werden.

|  |
| --- |
| **Maßnahmen zur Verhinderung der Vermischung von Urkunden** |
| […]  *Beispiel: An die Dokumentenvorbereitung schließt sich stets unmittelbar der Schritt „Scannen“ an, der vom gleichen Mitarbeitenden ausgeführt wird, sodass keine Vermischung von Urkunden entstehen kann.*  *Alternativ: Mehrere nicht verbundene Urkunden, die zum Scannen vorgesehen sind, werden jeweils in einer separaten Dokumentenmappe (Klarsichthülle) in der Ablage „Scannen“ aufbewahrt.* |

* Vorbereitung technischer Verfahren bei Stapel-Scans mehrerer Urkunden

**Hinweis:** Dieser Punkt ist nur von Bedeutung, wenn mehrere Urkunden in einem Arbeitsschritt per Einzelblatteinzug gescannt werden sollen. Um fehlerhafte Scanvorgänge zu vermeiden, rät die Bundesnotarkammer grundsätzlich von dieser Vorgehensweise ab.

|  |
| --- |
| **Maßnahmen zur Dokumententrennung** |
| […]  *Beispiel: Stapel-Scans mehrerer Urkunden in einem technischen Arbeitsgang werden zur Vermeidung von Fehlern nicht durchgeführt.*  *Alternativ, dann näher auszuführen: Zur automatisierten Stapeltrennung werden Trennblätter eingesetzt. Nach dem Scanvorgang werden die Trennblätter wieder entfernt und die Urkunden in separate Dokumentenmappen einsortiert.* |

* Herstellung der Scanfähigkeit der Urkunden

Alle Klammern, Klebezettel etc. sind vor dem Scanprozess von der Urkunde zu entfernen. Klebezettel oder sonstige lose Informationen müssen nur dann jeweils auf einer separaten Seite gescannt werden, wenn sie Teil der Urkunde sind (§§ 8 ff. BeurkG, § 13 BeurkG). Dies gilt bei anderen scanrelevanten Dokumenten entsprechend.

Sofern, etwa aufgrund eines Irrtums, bereits eine Verbindung mit Schnur und Siegel erfolgt ist, muss entweder die Verbindung aufgehoben (und anschließend neu hergestellt) werden oder es muss mithilfe von spezieller Scan-Hardware gearbeitet werden, die gebundene Papierdokumente verarbeiten kann.

Bei Beschädigungen durch Risse kann versucht werden, die Seite(n) zu kleben. Je nach Art und Umfang der Wiederherstellung muss dies durch einen Vermerk der Notarin / des Notars dokumentiert werden (Zusatz im Übereinstimmungsvermerk, siehe Abschnitt 2.5.4).

* Vorgehen bei Zweifelsfragen oder Manipulationsverdacht

Kommt es bei der Dokumentenvorbereitung zu Problemen oder bestehen Zweifelsfragen, die die zuständige Mitarbeiterin / der zuständige Mitarbeiter nicht lösen kann, muss die Arbeit unterbrochen und die Notarin / der Notar informiert werden. Manipulationen oder ein Manipulationsverdacht sind sofort mitzuteilen. Über das weitere Vorgehen hat die Notarin / der Notar situationsabhängig zu entscheiden.

|  |
| --- |
| **Verfahren bei Zweifelsfragen und Manipulationsverdacht** |
| […]  *Beispiel: Ergibt sich bei der Dokumentenvorbereitung ein Problem, das die zuständige Mitarbeiterin / der zuständige Mitarbeiter nicht selbstständig lösen kann oder besteht ein Manipulationsverdacht oder eine sonstige Zweifelsfrage, ist die Notarin / der Notar unverzüglich anzusprechen, um über das weitere Vorgehen zu entscheiden.* |

### 2.5.2 Scannen

Der Scanvorgang beginnt mit dem Auflegen der Urkunde auf das Scangerät bzw. mit dem Einlegen der Urkunde in den automatischen Einzug durch die in Anlage 1 genannten zuständigen Mitarbeiterinnnen / Mitarbeiter. Der Scanvorgang endet mit der Ausgabe des Scanprodukts und der Speicherung im Format PDF/A-1b.

* Ort des Scanvorgangs

Der Scanvorgang findet in den folgenden Räumlichkeiten statt:

|  |
| --- |
| **Raum und Arbeitsplätze** |
| […]  *Beispiel: Der Scanvorgang wird im Raum […] durchgeführt. Die Qualitäts- und Integritätssicherung findet getrennt in den weiteren nur für Mitarbeitende zugänglichen Räumen des Büros an den dort vorhandenen Arbeitsplätzen statt.*  *Alternativ: Der Scanvorgang findet ausschließlich im Raum […] statt. Alle für den Scanprozess benötigten Komponenten befinden sich in diesem Raum, einschließlich der verwendeten Arbeitsplatzrechner.* |

Zunächst überprüft die zuständige Mitarbeiterin / der zuständige Mitarbeiter, ob alle technischen Komponenten betriebsbereit und funktionstüchtig sind. Auch sämtliche im Voraus festgelegten Grundeinstellungen am Scangerät werden überprüft.

* Die Grundeinstellungen für den Scanprozess sind wie folgt definiert:

|  |  |
| --- | --- |
| **Grundeinstellungen** | |
| Zielformat | PDF/A-1b |
| Auflösung | 300 dpi / Grundrisse und Lagepläne werden mit einer Auflösung von 600 dpi gescannt, sofern nicht 300 dpi genügen. |
| Scannen in Farbe | Farb-Scan |
| Kontrast | […] |
| Helligkeit | […] |
| Einzug | automatisch  manuell  einseitig  beidseitig (Duplex) |
| Weitere Einstellungen | […] |

* Scannen in Farbe

In § 56 Abs. 1 BeurkG wird die inhaltliche und bildliche Übereinstimmung von elektronischem und dem in Papierform vorhandenen Dokument gefordert. Um diese Voraussetzung zu erfüllen, muss jede Urkunde in Farbe gescannt werden.

* Auswahl geeigneter Bildkompressionsverfahren

Es muss auf die Auswahl geeigneter Bildkompressionsverfahren geachtet werden. Grundsätzlich geeignet sind sowohl verlustfreie als auch verlustbehaftete Verfahren. Nicht eingesetzt dürfen Verfahren, die zur Bildkompression das sogenannte „Symbol Coding“ verwenden (z. B. JBIG2).

|  |
| --- |
| **Geeignete Bildkompressionsverfahren** |
| […]  *Beispiel: Eingesetztes Bildkompressionsverfahren: JPEG, hohe Qualität*  *Alternativ: Eingesetztes Bildkompressionsverfahren: TIFF, hohe Qualität* |

* Umgang mit der Vorder- und Rückseite

Es muss festgelegt werden, wie grundsätzlich mit den Vorder- und Rückseiten der Urkunde zu verfahren ist. Hält sich die Notarin / der Notar konsequent daran, Urkunden und Anlagen nur einseitig zu beschreiben, kann die Festlegung erfolgen, dass ausschließlich die Vorderseiten der Urkunde gescannt werden. Dies wird nur selten der Fall sein, weil bei Unterschriftsbeglaubigungen ohne Entwurf dennoch doppelseitige Vorlagen vorkommen können.

**Hinweis:** Steht ein beidseitiges Scanverfahren (Duplex) zur Verfügung, kann festgelegt werden, dass immer beidseitig gescannt wird und die leeren Seiten im Rahmen der Nachbearbeitung entfernt werden.

|  |
| --- |
| **Umgang mit der Vorder- und Rückseite der Urkunde** |
| […]  *Beispiel: Ergibt die sorgfältige Überprüfung der Urkunde vor dem Scanvorgang, dass die Urkunde nur einseitig beschrieben ist, werden in diesem Einzelfall nur die Vorderseiten gescannt. Sonst wird Duplex gescannt.*  *Alternativ: Es wird grundsätzlich im beidseitigen Scanverfahren (Duplex) gescannt, die leeren Seiten werden im Rahmen der Nachbearbeitung gelöscht.*  *Alternativ: Es werden grundsätzlich nur die Vorderseiten der Urkunde gescannt, da alle Urkunden im Notarbüro konsequent einseitig beschrieben werden. Bei Fremddokumenten ist in jedem Einzelfall zu prüfen, ob beidseitiger Inhalt vorliegt, und gegebenenfalls Duplex zu scannen.* |

* Zwischenablage und Benennung der erzeugten Scandateien

Es muss festgelegt werden, wo die Scandateien abgelegt und wie sie benannt werden.

|  |  |
| --- | --- |
| **Zwischenablage und Benennung** | |
| Ablage/Verzeichnis | […]  *Beispiel: L:\Ablage\Scandateien* |
| Benennung | […]  *Beispiel: (Jahrgang)−(fortlaufende Nummer im Urkundenverzeichnis – xy-stellig mit führenden Nullen)-(Nummer des Dokuments – xy-stellig mit führender Null).pdf*  *Beispiel für Sozietäten: (Notarkürzel)-(Jahrgang)−(fortlaufende Nummer im Urkundenverzeichnis – xy-stellig mit führenden Nullen)-(Nummer des Dokuments – xy-stellig mit führender Null).pdf* |

* Die Papieroriginale müssen während bzw. nach dem Scanvorgang an einem gegen unbefugten Zugriff gesicherten Ort aufbewahrt werden. Muss der Scanvorgang kurzzeitig unterbrochen werden, muss zu jedem Zeitpunkt die Kontrolle über die Vorlage gewahrt bleiben, z. B. durch Mitnahme oder sichere Ablage am persönlichen Arbeitsplatz, zu dem nur berechtigte Mitarbeitende Zugriff haben.

|  |  |
| --- | --- |
| **Ablage der Urkunde während und nach dem Scanvorgang** | |
| Raum, Dokumentenablage | […]  *Beispiel: Die Urkunden werden während des Scannens in Raum […] in der Dokumentenablage […] abgelegt.*  *Alternativ: Werden mehrere Urkunden in einem Arbeitsgang gescannt, werden die fertig gescannten Urkunden sogleich nach 2.5.3 abgelegt.* |

* Beschädigung oder Zerstörung der Urkunde

Kommt es beim Scannen zu einer Beschädigung oder einer vollständigen Zerstörung der Urkunde, ist umgehend die Notarin / der Notar zu verständigen.

|  |
| --- |
| **Vorgehen bei Beschädigung oder Zerstörung der Urkunde** |
| […]  *Beispiel: Falls die Urkunde beim Scanvorgang beschädigt oder zerstört wird, hält die zuständige Mitarbeiterin / der zuständige Mitarbeiter unverzüglich Rücksprache mit der Notarin / dem Notar zur Klärung des weiteren Vorgehens.* |

### 

### 2.5.3 Nachverarbeitung

Nach dem Scanvorgang führen die in Anlage 1 genannten zuständigen Mitarbeiterinnen / Mitarbeiter eine Qualitätskontrolle des Scanprodukts durch. Dafür wird die Urkunde zunächst vollständig und in unveränderter Ordnung in einer gegen unbefugten Zugriff geschützten Weise abgelegt.

|  |  |
| --- | --- |
| **Ablage der gescannten Urkunde** | |
| Raum, Dokumentenablage | […]  *Beispiel: Die vollständig gescannte Urkunde wird im Raum […] in der Ablage […] abgelegt.* |

|  |
| --- |
| **Ausschluss eines unautorisierten manuellen Zugriffs auf das Scanprodukt** |
| […]  *Beispiel: Der Zugang zum Arbeitsplatz ist für unbefugte Personen nicht unbeaufsichtigt möglich. Eine Authentisierung am Arbeitsplatz durch Log-in am Computer ist erforderlich. Zugriff auf die verwendete Dateiablage haben nur Mitarbeitende, die am Scanprozess beteiligt sind.*  *Empfohlen, aber nicht zwingend: Der Computer wird nur von Mitarbeitenden benutzt, die am Scanprozess beteiligt sind.*  *Empfohlen, aber nicht zwingend erforderlich: Das Scanprodukt wird auf einer verschlüsselten Festplatte abgelegt. Dadurch besteht ein zusätzlicher Schutz gegen Angreifer, die physischen Zugriff auf den Datenträger erlangen.* |

* Qualitätssicherung / Überprüfung des Scanprodukts

Die ursprünglichen Scanprodukte dürfen nicht vor Abschluss der Qualitätskontrolle gelöscht werden.

Die zuständige Mitarbeiterin / Der zuständige Mitarbeiter stellt im Rahmen einer **vollständigen Sichtkontrolle** sicher, dass jede Seite der Urkunde gescannt wurde. Fehlende oder nicht vollständig übertragene Seiten werden noch einmal gescannt. Bei Seiten, die versehentlich mehrfach gescannt wurden, werden die überzähligen Kopien gelöscht.

Weiterhin wird die bildliche und inhaltlich korrekte Übertragung des Inhalts der papiernen Urkunde zum elektronischen Dokument überprüft, um einem Informationsverlust oder -veränderungen vorzubeugen. Hier ist insbesondere darauf zu achten, dass etwaige handschriftliche Ergänzungen der Notarin / des Notars, die aufgestempelte Urkundenverzeichnisnummer und ggf. aufgedruckte Siegel vollständig und lesbar übertragen worden sind.

|  |
| --- |
| **Überprüfung des Scanprodukts** |
| […]  *Beispiel: Zur Überprüfung der Vollständigkeit wird zunächst die Gesamtzahl der gescannten Seiten mit der Seitenanzahl des Papieroriginals verglichen. Die Reihenfolge des gescannten Dokuments wird anhand der aufgedruckten Seitenzahlen der Originalurkunde oder anderer geeigneter Merkmale (inhaltlicher Zusammenhang) überprüft. Die bildliche und inhaltliche Übereinstimmung wird durch einen seitenweisen Abgleich mit dem Papieroriginal überprüft*. |

* Nachbearbeitung

Die Nachbearbeitung des Scanprodukts, wie die Änderung von Kontrasten oder der Helligkeit, Farbreduktion, Beschneiden oder Rauschunterdrückung, ist in diesem Scanprozess grundsätzlich ausgeschlossen. Bei aufgetretenen Fehlern oder Ungenauigkeiten am Scanprodukt soll der gesamte Scanvorgang wiederholt bzw. die einzelnen Scanparameter entsprechend angepasst werden.

Die von der Bundesnotarkammer zur Verfügung gestellte Software XNP mit dem Modul „Urkundenverzeichnis / Urkundensammlung“ ermöglicht als einzige Nachbearbeitungsfunktionen das Löschen und Hinzufügen (Zusammenführen) sowie das Drehen von Seiten. Das nachträgliche Drehen von Seiten, sollte grundsätzlich bereits durch die Vorbereitung des Scanprozesses vermieden werden. Ist dies doch erforderlich, sollte es im Übereinstimmungsvermerk angegeben werden. Kommt es durch die Scangeräte beispielsweise aufgrund der Nutzung der OCR-Funktion zu automatischen Drehungen, können diese ohne eine Dokumentation im Übereinstimmungsvermerk wieder korrigiert werden.  
Es kann grundsätzlich auch auf eine andere Software zur Nachbearbeitung zurückgegriffen werden. Die vorstehenden Einschränkungen der Nachbearbeitung sind dabei einzuhalten.

### 2.5.4 Integritätssicherung

Im Anschluss an die Qualitätssicherung durch die zuständige Mitarbeiterin / den zuständigen Mitarbeiter überprüft die verantwortliche Notarin / der verantwortliche Notar die bildliche und inhaltliche Übereinstimmung des elektronischen Dokuments mit dem Originaldokument. Ist die Übereinstimmung gegeben, bestätigt die Notarin / der Notar dies in einem entsprechenden Vermerk (Übereinstimmungsvermerk).

Hinweis: Falls eine Notarin / ein Notar keine Mitarbeitenden beschäftigt, ist es zulässig, dass sie / er sowohl den Scanvorgang, als auch die Qualitäts- und Integritätssicherung in einer Person durchführt. Diese Ausnahme ist im Übereinstimmungsvermerk zu dokumentieren.

Der Übereinstimmungsvermerk soll nach RESISCAN die folgenden Informationen enthalten:

* Erstellerin / Ersteller des Scanproduktes[[2]](#footnote-3),
* technisches und organisatorisches Umfeld des Erfassungsvorganges in Form einer Referenz auf die geltende Verfahrensdokumentation,
* etwaige Auffälligkeiten, die während des Scanprozesses aufgetreten sind,
* Zeitpunkt der Erfassung,
* Ergebnis der Qualitätssicherung (wird im Übereinstimmungsvermerk nicht gesondert dokumentiert, da bereits die inhaltliche und bildliche Übereinstimmung von Urschrift in Papierform und dem elektronischen Dokument ausdrücklich bestätigt wird),
* die Tatsache, dass es sich um ein Scanprodukt handelt, das bildlich und inhaltlich mit der Papierurkunde übereinstimmt.

Der Übereinstimmungsvermerk wird für das Scannen notarieller Urkunden im rechtlichen Rahmen des § 56 BeurkG wie folgt formuliert:

|  |
| --- |
| **Übereinstimmungsvermerk** |

|  |
| --- |
| *Die bildliche und inhaltliche Übereinstimmung des vorliegenden elektronischen Dokuments mit der Urschrift [bzw. Abschrift oder Ausfertigung] in Papierform wird hiermit bestätigt.*  *Die Übertragung in die elektronische Form ist nach meiner am Tag der Bestätigung gültigen Verfahrensdokumentation erfolgt.*  *[Ort], [Datum]*  *[Name der Notarin oder des Notars], Notarin / Notar in [Amtssitz]*  *Eventuelle Mängel des Ausgangsdokuments werden im Vermerk erwähnt, soweit sie nicht aus dem elektronischen Dokument eindeutig ersichtlich sind (§ 56 Abs. 1 Satz 3 BeurkG). Gleiches gilt für Mängel des Scanprodukts.*  *Beispiele: „Die Seiten 5 bis 27 mussten aufgrund eines Helligkeitsunterschieds erneut gescannt und im Dokument ersetzt werden.“ / „Aufgrund eines Papierstaus entstand auf Seite 23 des Dokuments ein Riss, der geklebt wurde.“ / „Seite 12 enthält eine schon im Original verschwommene Überschrift.“* |

Der Übereinstimmungsvermerk wird mit dem Scanprodukt zu einer PDF/A-Datei verbunden. Die Notarin / Der Notar bestätigt die bildliche und inhaltliche Übereinstimmung mit dem Originaldokument abschließend mit der qualifizierten elektronischen Signatur. Eine unautorisierte Durchführung der Signatur ist ausgeschlossen, da die Signaturkarte bzw. N-Karte persönlich verwahrt wird und die zugehörige PIN nur der Notarin / dem Notar bekannt ist (§ 33 Abs. 3 BNotO).

### 2.5.5 Typische Fehlerquellen und Empfehlungen

Als typische Fehlerquellen bei der Dokumentenvorbereitung, dem Scannen und der Nachverarbeitung gelten folgende Fälle:

* Ursprünglich geklammerte Papierdokumente werden nicht hinreichend sorgfältig auf ihre Vollständigkeit geprüft.
* Zu scannende Originaldokumente werden mit der falschen Seite zum Scangerät in den Einzug gelegt.

|  |
| --- |
| **Vorsichtsmaßnahmen** |
| […]  *Beispiel: Ursprünglich geklammerte Papierdokumente sind besonders sorgfältig auf ihre Vollständigkeit und die korrekte Reihenfolge der Seiten zu überprüfen. Vor dem Scanvorgang ist darauf zu achten, wie die Urkunde korrekt in das Scangerät gelegt wird (siehe Aufkleber am Scangerät). Grundsätzlich wird ein Testlauf durchgeführt, wenn Unklarheiten bestehen.* |

### 2.5.6 Aufbewahrung und Übergabe an das Elektronische Urkundenarchiv (Langzeitspeicher)

Die integritätsgeschützten elektronischen Dokumente müssen bis zur Übergabe an das Elektronische Urkundenarchiv sicher aufbewahrt werden. Ein unautorisierter manueller Zugriff auf die elektronischen Dokumente ist aus den folgenden Gründen ausgeschlossen:

|  |
| --- |
| **Ausschluss eines unautorisierten manuellen Zugriffs auf die elektronischen Dokumente** |
| […]  *Beispiel: Der Zugang zum Arbeitsplatz ist für unbefugte Personen nicht ohne Begleitung von Mitarbeitenden möglich. Eine Authentisierung am Arbeitsplatz durch Log-in ist bei allen Computern erforderlich, von denen aus ein Zugriff auf die elektronischen Dokumente erfolgen kann.*  *Empfohlen, nicht zwingend: Der Computer wird nur von Mitarbeitenden benutzt, die am Scanprozess beteiligt sind.* |

Nach der Integritätssicherung werden die elektronischen Dokumente unverzüglich in das Elektronische Urkundenarchiv eingestellt. Die Übergabe der Urkunde an das Elektronische Urkundenarchiv erfolgt über das abgesicherte Notarnetz der Bundesnotarkammer mithilfe der Software XNP mit dem Modul „Urkundenverzeichnis / Urkundensammlung“.

Der Scanprozess ist nach der erfolgreichen Übergabe an das Elektronische Urkundenarchiv abgeschlossen.

### 2.5.7 Verbleib des Originals

Die Papieroriginale der gescannten Urkunden müssen gemäß § 50 Abs. 1 Nr. 3 NotAktVV für einen Zeitraum von 30 Jahren in der Urkundensammlung aufbewahrt werden. Nach dem Ablauf der Aufbewahrungsfrist muss das Originaldokument gemäß § 35 Abs. 6 BNotO im Regelfall vernichtet werden.

## 2.6 Das Scansystem

*[Für die Einrichtung des Scanverfahrens im Notarbüro sollen die Anforderungen des IT-Grundschutz-Kompendiums des Bundesamts für Sicherheit in der Informationstechnik (BSI) berücksichtigt werden. Zur Vorbereitung der Umsetzung dient der folgende Abschnitt für die Angabe der individuellen Hardware- und Softwarekonfiguration. Die Umsetzung der einzelnen Maßnahmen kann in Zusammenarbeit mit einem Systembetreuer oder einem Systemhaus erfolgen.]*

### 2.6.1 Scannen

Für den Scanvorgang werden ausschließlich die folgenden hardwaretechnischen Geräte eingesetzt:

|  |
| --- |
| **Scan-Hardware** |
| *Scangerät: [Angabe des Herstellers und Typenbezeichnung, Software-Version]*  *Server: [Angabe zum Betriebssystem des Servers]*  *Client: [Angabe zum Betriebssystem des Clients]* |

Die softwaretechnisch unterstützten Prozessschritte werden ausschließlich durch die folgende Software oder Softwarebestandteile realisiert:

|  |
| --- |
| **Scan-Software** |
| […]  *Beispiel: XNP (Basisanwendung der Bundesnotarkammer) mit dem Modul „Urkundenverzeichnis“ wird zur Qualitätssicherung, zur Nachbearbeitung (soweit zulässig) und zur Integritätssicherung durch Signatur genutzt.*  *Über die auf der Scan-Hardware integrierte Software hinaus wird keine Scan-Software eingesetzt.*  *Alternativ: Angabe der eingesetzten Scan-Software mit Produktbezeichnung, Hersteller, Version; (das ist nur relevant, falls ein (Arbeitsplatz-)Scanner eingesetzt wird, der nicht ohne externe Software bereits PDF-Dateien erzeugen und auf einer Netzwerkablage speichern kann)* |

### 

### 2.6.2 Integritätssicherung

Die gescannte notarielle Urkunde ist während des gesamten Scanvorgangs durch die folgenden Mechanismen integritätsgeschützt:

|  |
| --- |
| **Mechanismen zum Integritätsschutz** |
| […]  *Beispiel: Die Integrität der Zwischenprodukte wird organisatorisch durch Ablage auf einem Datenträger gewährleistet, auf den ausschließlich die am Scanprozess beteiligten Mitarbeitenden Zugriff erhalten. Es werden verschlüsselte Netzwerkverbindungen genutzt. [Dies sichert gegen physischen Zugriff auf die Verbindungen.]*  *Empfohlen, aber nicht zwingend erforderlich: Der verwendete Datenträger ist verschlüsselt. (Dadurch besteht ein zusätzlicher Schutz gegen Angreifer, die physischen Zugriff auf den Datenträger erlangen.)*  *Der Zugriff auf alle Teile des Scan-Systems ist über die Benutzerverwaltung auf berechtigte Mitarbeitende begrenzt. [Wenn am Scanner selbst keine Authentisierung umgesetzt ist, muss sichergestellt sein, dass nur berechtigte Mitarbeitende physisch auf den Scanner zugreifen können.]* |

Zur Erzeugung der qualifizierten elektronischen Signatur wird die folgende Hardware eingesetzt:

|  |
| --- |
| **Hardware zum Anbringen der elektronischen Signatur** |
| […]  *Beispiel:  N-Karte / Signaturkarte der Zertifizierungsstelle der Bundesnotarkammer*  *Kartenlesegerät der Sicherheitsklasse 3 [Angabe des Herstellers und Typenbezeichnung* |

Für die Integritätssicherung der Scanprodukte kommt die folgende Software zum Einsatz:

|  |
| --- |
| **Software zur Integritätssicherung** |
| […]  *Beispiel: Zum Signieren wird XNP (Basisanwendung der Bundesnotarkammer) mit dem Modul „Urkundenverzeichnis“ genutzt.* |

|  |
| --- |
| **Weitere Informationen zur eingesetzten Hard- und Software** |
| […]  *Beispiel: Benutzerhandbücher für Scanner und Kartenlesegerät*  *Onlinehilfe der Bundesnotarkammer zu den XNP-Modulen „Urkundenverzeichnis / Urkundensammlung“*  *[Ggf. Angabe, wo weitere Informationen zum Betreibe der eingesetzten Hard- und Software zu finden sind.]* |

Für den Schutz der Integrität der in den Scanprozess involvierten Systeme sind die in Abschnitt 3.7.1 näher erläuterten Maßnahmen vorgesehen.

# Maßnahmen

## 3.1 Organisatorische Maßnahmen

### 3.1.1 Zuständigkeiten und Regelungen

Die in der Anlage 1 aufgeführten Mitarbeiterinnen und Mitarbeiter sind von der Notarin / dem Notar zur Durchführung der einzelnen Prozessschritte im Scanverfahren bestimmt worden.[[3]](#footnote-4) Anlage 1 ist Bestandteil dieser Muster-Verfahrensdokumentation. Die Notarin / Der Notar berücksichtigt dabei potenzielle Interessenskonflikte im Notarbüro (eigene Beteiligung an einem Urkundsgeschäft) und trägt Sorge dafür, dass Mitarbeitende in einem solchen Fall nicht an dem konkreten Scanprozess mitwirken. Die folgenden Maßnahmen stellen sicher, dass nur die zuständigen Mitarbeiterinnen / Mitarbeiter die am Scanprozess beteiligten Komponenten verwenden können.

|  |
| --- |
| **Ausschließliche Nutzung der Komponenten durch die zuständigen Mitarbeiterinnen / Mitarbeiter** |
| […]  *Beispiel: Alle eingesetzten Komponenten sind durch einen wirksamen Zugriffsschutz gesichert, sodass sie nur von am Scanprozess beteiligten Mitarbeitenden verwendet werden können.*  *Die eingesetzten Clients und Server verfügen über eine eingerichtete Nutzerkontensteuerung. Nur die für den Umgang mit Urkunden berechtigten und am Scanprozess beteiligten Mitarbeitenden verfügen über ein Nutzerkonto für diese Systeme.*  *Die für das Scannen verwendeten Komponenten befinden sich in einem geschützten Arbeitsbereich. Der Zugang zu diesem Bereich ist für dritte Personen nur in ständiger Begleitung durch einen Mitarbeitenden möglich.* |

### 3.1.2 Dokumentenvorbereitung

Die Dokumentenvorbereitung wird von den in Anlage 1 genannten Mitarbeiterinnen und Mitarbeitern durchgeführt.

### 3.1.3 Scanvorgang

Der Scanvorgang wird von den in Anlage 1 genannten Mitarbeiterinnen und Mitarbeitern durchgeführt. Die Urkunde ist durch die folgenden Regelungen stets vor fremden Zugriff geschützt.

|  |
| --- |
| **Regelungen zum Schutz der Urkunde vor fremdem Zugriff** |
| […]  *Beispiel: Für den Scanvorgang wird ein Multifunktionsgerät verwendet. Der Scanvorgang wird direkt am Gerät durchgeführt und von dort gesteuert. Der für den Scanprozess zuständige Mitarbeitende ist während des Scanvorgangs anwesend und überwacht den Vorgang.*  *Alternativ: Die Scan-Hardware ist direkt neben dem Arbeitsplatz positioniert. Ein unbefugter Zugriff auf die Urkunde während des Scanvorgangs ist nicht möglich.* |

### 

### 3.1.4 Qualitätssicherung und Nachbearbeitung

Die Qualitätssicherung und Nachbearbeitung der gescannten Urkunde wird von den in Anlage 1 genannten Mitarbeiterinnen und Mitarbeitern durchgeführt.

### 

### 3.1.5 Integritätssicherung

Die Integritätssicherung wird ausschließlich von der verantwortlichen Notarin / dem verantwortlichen Notar durchgeführt (siehe Abschnitt 2.5.4).

### 

### 3.1.6 Übergabe an das Elektronische Urkundenarchiv

Die Übergabe der vollständig gescannten Urkunden an das Elektronische Urkundenarchiv wird grundsätzlich von der verantwortlichen Notarin / von dem verantwortlichen Notar durchgeführt. In besonderen Fällen (z. B. wenn die ursprünglich vom Notar beabsichtigte Übergabe fehlschlägt) kann die vollständig gescannte Urkunde auch von den in Anlage 1 genannten Mitarbeiterinnen / Mitarbeitern an das Elektronische Urkundenarchiv übergeben werden.

### 

### 3.1.7 Regelungen für die Administrations-, Wartungs- und Reparaturarbeiten

Die Wartung und die Reparatur der für den Scanvorgang eingesetzten IT-Systeme, Anwendungen und Netze sind wie folgt geregelt:

* Die Zuständigkeiten für die Beauftragung, Durchführung und gegebenenfalls Kontrolle von Wartungs- und Reparaturarbeiten sind in Anlage 1 aufgeführt.
* Verfahren für die regelmäßige Bereitstellung und Anwendung von sicherheitsrelevanten Updates:

|  |
| --- |
| **Verfahren im Hinblick auf sicherheitsrelevante Updates** |
| […]  *Beispiel: Antiviren-Software führt Updates der Virensignaturen automatisiert durch.*  *Alle vier Wochen werden durch einen externen Administrator (Systembetreuer) das System, Firmware der Geräte und die installierte Software auf Updates geprüft. Falls stabile Update-Versionen vorhanden sind, werden diese installiert.*  *Alternativ: Die / der in Anlage 1 dafür angegebene zuständige Mitarbeitende informiert sich regelmäßig über Updates für Software, Firmware etc. und veranlasst gegebenenfalls ein Update. Einmal monatlich, und zwar immer am zweiten Arbeitstag des Monats, prüft die/der Mitarbeitende die Hard- und Software auf relevante Updates prüft und führt diese gegebenenfalls durch.* |

* Regelungen zur Authentisierung und zum Nachweis der Autorisierung des Wartungspersonals:

|  |
| --- |
| **Regelungen zum Nachweis der Autorisierung des Wartungspersonals** |
| […]  *Beispiel: Sofern das Wartungspersonal nicht persönlich bekannt ist und Kenntnis über die Beauftragung besteht, werden eine Legitimation (Dienstausweis o. Ä.) und die Beauftragung geprüft.* |

* Regelungen zum Schutz personenbezogener oder anderweitig besonders schützenswerter Daten (z. B. Betriebsgeheimnisse) auf den zu wartenden IT-Systemen:

|  |
| --- |
| **Regelungen zum Schutz von Daten auf den zu wartenden IT-Systemen** |
| […]  *Beispiel: Mit den externen Dienstleistern, z. B. Wartungspersonal, wird eine Auftragsverarbeitungsvereinbarung (AVV) im Sinne der DS-GVO und eine Vereinbarung nach § 26a BNotO abgeschlossen.*  *Schreibtische und Ablagen sind aufgeräumt zu hinterlassen. Es ist insbesondere darauf zu achten, dass Originalurkunden nicht offen einsehbar sind oder im Scangerät vergessen werden.* |

* Die Zuständigkeit für die Dokumentation von sicherheitsrelevanten Veränderungen an den involvierten IT-Systemen und Anwendungen ist in Anlage 1 aufgeführt.
* Die Zuständigkeit für die Dokumentation der erfolgreichen Durchführung der Maßnahmen zur Qualitätskontrolle und Freigabe vor der Wiederaufnahme des regulären Betriebs ist in Anlage 1 aufgeführt.

### 3.1.8 Abnahme- und Freigabeverfahren für Hard- und Software

Durch die ordnungsgemäße und ununterbrochene Nutzung der in Abschnitt 2.6 aufgeführten Hard- und Software wird sichergestellt, dass die in Abschnitt 2.2 erläuterten rechtlichen Rahmenbedingungen eingehalten werden.

Um eine unbemerkte Manipulation der zum Scannen verwendeten IT-Systeme und -Anwendungen zu verhindern und die Ordnungsmäßigkeit der Systeme zu dokumentieren, muss ein geregeltes Verfahren für die Abnahme und Freigabe der eingesetzten Hard- und Software etabliert werden. Neben der erstmaligen Inbetriebnahme ist dieses Abnahmeverfahren auch bei der Wiederaufnahme des Betriebs nach Wartungs- und Reparaturarbeiten durchzuführen.

Bei einer Änderung der digitalisierungs- und / oder archivierungsrelevanten Hard- und / oder Software wird neben der Dokumentation der Systemänderung sichergestellt, dass die Lesbarkeit der gescannten Urkunden gewährleistet bleibt.

|  |
| --- |
| **Abnahme- und Freigabeverfahren bei Änderung von Hard- und Software-Komponenten** |
| […] *Beispiel:*   * *Es wird eine Sicherung der Konfiguration vor einer Änderung durchgeführt (gegebenenfalls auch als Ausdruck auf Papier).* * *Neben der geänderten Einstellung sind die grundsätzlichen, nicht von der Änderung betroffenen, Einstellungen aus der vorhergehenden Konfiguration zu übernehmen (z. B. Farb-Scan).* * *Es wird insbesondere sichergestellt, dass als Ausgabe-Format PDF/A-1b konfiguriert ist.* * *Scanprofile sind aus der vorhergehenden Konfiguration zu übernehmen.* * *Schutzmechanismen sind grundsätzlich zu übernehmen. Wie bei der initialen Verwendung müssen z. B. Standard-Passwörter geändert werden und die Zugänge für Mitarbeitende wiederhergestellt bzw. erstellt werden.*   *Beim Austausch bzw. Änderung (auch durch Updates) einer Komponente, die für den Scanprozess eingesetzt wird, wird ein Testlauf mit einem Testdokument durchgeführt. Das Testdokument enthält neben einfachen Textzeilen auch Bilder in unterschiedlichen Farben. Der Scanvorgang wird vollständig durchgeführt, in XNP wird das Dokument jedoch nur im Modul „Dokumente“ geöffnet und nicht im Modul „Urkundenverzeichnis“. Sofern bei der bildlichen und inhaltlichen Überprüfung Abweichungen festgestellt werden, ist unter Berücksichtigung der festgelegten Grundeinstellungen (siehe Abschnitt 2.5.2) eine Kalibrierung des Systems vorzunehmen.*  *Das Ergebnis des Freigabeverfahrens wird dokumentiert.* |

### 3.1.9 Einhaltung der Informationssicherheit

Für die Einhaltung der Informationssicherheit im Scanprozess sind folgende Personen verantwortlich (siehe auch Anlage 1):

|  |
| --- |
| **Zuständigkeit für die Informationssicherheit** |
| […]  *Beispiel: Notarin …. oder Notar…*  *Alternativ: Bürovorsteherin / Bürovorsteher / Datenschutzbeauftragte / Datenschutzbeauftragter / externer Dienstleister* |

Mindestens alle drei Jahre erfolgt eine Überprüfung der Wirksamkeit und Vollständigkeit der für die Informationssicherheit beim ersetzenden Scannen vorgesehenen Maßnahmen. Zusätzlich wird geprüft, ob die eingesetzten Maßnahmen vor potenziellen Bedrohungen schützen und ob gegebenenfalls weitere Sicherheitsmaßnahmen notwendig sind. Hierzu kann auch ein externer Berater, gegebenenfalls ein Systemhaus beauftragt werden. Die Ergebnisse dieser Überprüfung werden dokumentiert. Sofern Sicherheitslücken oder andere Probleme gefunden werden, werden entsprechende Korrekturmaßnahmen durchgeführt. Für die Korrekturmaßnahmen wird ein Zeitplan mit den zuständigen Mitarbeitenden definiert.

|  |
| --- |
| **Korrekturmaßnahmen mit Zeitplan und Verantwortlichkeiten** |
| *[Dieses Formularfeld ist erst nach der erstmaligen Überprüfung der Maßnahmen zur Einhaltung der Informationssicherheit auszufüllen, die nach spätestens drei Jahren stattfindet; siehe vorstehender Hinweis.]*  *Beispiel: Das Protokoll der Überprüfung vom [Datum] wird bei dieser Verfahrensdokumentation aufbewahrt. Korrekturmaßnahmen sind nicht notwendig.*  *Alternativ: Das Protokoll der Überprüfung vom [Datum] wird bei dieser Verfahrensdokumentation aufbewahrt. Für die Umsetzung der Korrekturmaßnahmen ist [die Notarin / der Notar / der Mitarbeitende …] verantwortlich.* |

## 

## 3.2 Personelle Maßnahmen

### 3.2.1 Verpflichtung der Mitarbeiterinnen und Mitarbeiter

Die verantwortliche Notarin / Der verantwortliche Notar nimmt die nach § 26 Satz 1 BNotO vorgeschriebene förmliche Verpflichtung der Mitarbeiterinnen und Mitarbeiter nach § 1 des Verpflichtungsgesetzes vor. Er weist in diesem Zusammenhang auch auf die Einhaltung der einschlägigen Gesetze, Vorschriften, Regelungen und diese Verfahrensdokumentation hin.

Darüber hinaus sollen die Mitarbeiterinnen und Mitarbeiter von den wesentlichen rechtlichen Rahmenbedingungen (Anlage 3) Kenntnis nehmen.

Sind im Notarbüro Beschäftigte von der förmlichen Verpflichtung nicht betroffen oder werden ihnen erst zu einem späteren Zeitpunkt Aufgaben im Scanverfahren zugewiesen, werden sie gesondert auf die Einhaltung der einschlägigen Gesetze, Vorschriften, Regelungen und diese Verfahrensdokumentation verpflichtet.

|  |
| --- |
| **Verpflichtungserklärungen** |
| […]  *Beispiel: Im Zusammenhang mit der Verpflichtung nach dem Verpflichtungsgesetz (§ 26 BNotO) werden die Mitarbeiterinnen und Mitarbeiter auch über die datenschutzrechtlichen Vorschriften sowie die rechtlichen Rahmenbedingungen des Scannens belehrt und auf die Verfahrensdokumentation hingewiesen. Die Belehrung und Unterweisung werden in der Personalakte dokumentiert.* |

### 3.2.2 Maßnahmen zur Qualifizierung und Sensibilisierung

### 3.2.2.1 Einweisung zur ordnungsgemäßen Bedienung des Scansystems

Die gemäß Anlage 1 hierfür zuständige Person weist die für den Scanprozess zuständigen Mitarbeitenden in die Nutzung der eingesetzten Geräte und Anwendungen sowie die sonstigen Abläufe ein.

Die Einweisung in das Scansystem umfasst insbesondere die folgenden Themen:

* die grundsätzlichen Abläufe im Scanprozess einschließlich der Dokumentenvorbereitung, dem Scan-vorgang, gegebenenfalls der Indexierung, der zulässigen Nachbearbeitung und der Qualitäts- und Integritätssicherung,
* die geeignete Konfiguration und Nutzung der Scan-Hardware,
* Anforderungen hinsichtlich der Qualitätssicherung,
* Abläufe und Anforderungen bei der Erstellung des Übereinstimmungsvermerks,
* Konfiguration und Nutzung der Systeme zur Integritätssicherung und
* das Verhalten im Fehlerfall.

Für die Einweisung werden die folgenden Schulungsunterlagen genutzt:

|  |
| --- |
| **Schulungsunterlagen für die Einweisung in das Scansystem** |
| […]  *Beispiel: Online-Hilfe zu* [*XNP*](https://onlinehilfe.bnotk.de/einrichtungen/bundesnotarkammer/xnp.html) *und zum* [*Modul „Urkundenverzeichnis“*](https://onlinehilfe.bnotk.de/einrichtungen/elektronisches-urkundenarchiv/urkundenverzeichnis-uvz-und-elektronische-urkundensammlung-euvz.html)  *Verfahrensdokumentation für das Scannen von Urkunden (vorliegendes Dokument)*  [*Leitfaden zum Ausfüllen der Verfahrensdokumentation zum Scannen von Urkunden*](https://www.elektronisches-urkundenarchiv.de/scanprozess)  *Benutzerhandbücher für das Scangerät und ggf. für Software zur Ansteuerung des Scanners* |

### 3.2.2.2 Einweisung zu Sicherheitsmaßnahmen im Scanprozess

Die gemäß Anlage 1 hierfür zuständige Person weist die mit dem Scanprozess betrauten Mitarbeiterinnen und Mitarbeiter in geeigneter Weise hinsichtlich der umzusetzenden sowie der implementierten Sicherheitsmaßnahmen ein.

Die Einweisung in die Sicherheitsmaßnahmen umfasst insbesondere die folgenden Themen:

* die grundsätzliche Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Informationssicherheit,
* personenbezogene Sicherheitsmaßnahmen im Scanprozess,
* systembezogene Sicherheitsmaßnahmen im Scansystem,
* Verhalten bei Auftreten von Schadsoftware,
* Bedeutung der Datensicherung und deren Durchführung,
* Umgang mit personenbezogenen und anderen sensiblen Daten und
* Einweisung in die zu ergreifenden Vorsichts- und Notfallmaßnahmen.

Für die Einweisung werden die folgenden Schulungsunterlagen genutzt:

|  |
| --- |
| **Schulungsunterlagen für die Einweisung in die Sicherheitsmaßnahmen** |
| […]  *Beispiel:* [*Handreichung der Bundesnotarkammer „IT-Sicherheit für Notarinnen und Notare“*](https://www.elektronisches-urkundenarchiv.de/scanprozess)[…] |

### 3.2.2.3 Schulung des Wartungs- und Administrationspersonals

Die gemäß Anlage 1 hierfür zuständige Person schult die Mitarbeiterinnen und Mitarbeiter, die für die Wartungs- und Administrationsaufgaben für die in den Scanprozess involvierten IT-Systeme und Anwendungen zuständig sind, hinsichtlich der hierfür notwendigen Kenntnisse über die eingesetzten IT-Komponenten.

Die Schulung umfasst insbesondere die folgenden Themen:

* selbstständige Durchführung von alltäglichen Administrationsaufgaben,
* selbstständige Fehlererkennung und -behebung,
* regelmäßige selbsttätige Durchführung von Datensicherungen,
* Nachvollziehbarkeit von Eingriffen durch externes Wartungspersonal,
* das Erkennen und Beheben von Manipulationsversuchen oder unbefugten Zugriffen auf die Systeme.

Für die Schulung des Wartungs- und Administrationspersonals werden die folgenden Unterlagen genutzt:

|  |
| --- |
| **Unterlagen für die Schulung des Wartungs- und Administrationspersonals** |
| […]  *Beispiel: Die Wartung und Administration aller in den Scanprozess involvierten IT-Systeme und Anwendungen übernimmt der Dienstleister [...]. Aus diesem Grund ist eine Schulung der Mitarbeitenden im Notarbüro nicht erforderlich.*  *Alternativ:* *Es ist eine in Anlage 1 genannte, im Notarbüro beschäftige Person benannt, um die Wartungs- und Administrationsarbeiten vorzunehmen. Diese Person wird durch den in Anlage 1 genannten externen Dienstleister geschult.*  *Alternativ: Diese Verfahrensdokumentation, Leitfaden zum Ausfüllen der Verfahrensdokumentation, Benutzerhandbuch für das Scangerät* |

### 3.2.2.4 Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Informationssicherheit

Zur Einweisung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für die Informationssicherheit erfolgt für die in Abschnitt 3.1 genannten Aufgaben eine regelmäßige Unterweisung in den Scan-, Archivierungs- und Vernichtungsprozess sowie zu generellen Sicherheitsmaßnahmen, der sicherheitsbewussten Handhabung von Dokumenten, Daten und IT-Systemen und zu ergreifenden Vorsichtsmaßnahmen. Über die Schulung wird ein Protokoll angefertigt und archiviert.

Bei einem Wechsel der personellen Zuständigkeit erfolgt eine Unterweisung in den Scan-, Archivierungs- und Vernichtungsprozess sowie eine Schulung zur ordnungsmäßigen Bedienung des Scan- und Archivierungssystems durch die verantwortliche Notarin / den verantwortlichen Notar oder einen damit beauftragten leitenden Mitarbeitenden.

|  |
| --- |
| **Schulung zur Informationssicherheit** |
| […]  *Beispiel: Den Mitarbeitenden wird die* [*Handreichung der Bundesnotarkammer „IT-Sicherheit für Notarinnen und Notare“*](https://www.elektronisches-urkundenarchiv.de/scanprozess) *zugänglich gemacht.*  *Ergänzend werden zentralen Punkte mit der Notarin / dem Notar oder der Bürovorsteherin / dem Bürovorsteher durchgesprochen.*  *Durchsprache und Aushändigung der Handreichung werden dokumentiert.*  *Es wird regelmäßig in Bürobesprechungen das Thema Informationssicherheit angesprochen und auf die Handreichung hingewiesen.*  *Alternativ: Es werden halbjährlich externe Schulungen zur Informationssicherheit für alle Mitarbeitenden durchgeführt.* |

## 3.3 Technische Maßnahmen

Für den Fall, dass einzelne der beschriebenen technischen Empfehlungen nicht mittels Hard- und Software realisiert werden, sind folgende alternative Maßnahmen vorgesehen:

|  |
| --- |
| **Alternative organisatorische oder zusätzliche technische Maßnahmen** |
| […]  *Beispiel: Die eingesetzte Scan-Hardware wird (entgegen der Empfehlung) über einen Firewire-Anschluss angebunden. Der Raum, in dem die Scan-Hardware aufgestellt ist, ist nur den Mitarbeiterinnen und Mitarbeitern zugänglich, die für den Scanprozess zuständig sind. Vor der Benutzung der Scan-Hardware wird der Firewire-Anschluss auf offensichtliche Veränderungen überprüft.* |

### 3.3.1 Grundlegende Sicherheitsmaßnahmen im Scanprozess

Für die in den Scanprozess involvierten IT-Systeme, Anwendungen und Sicherungsmittel werden die im IT-Grundschutz-Kompendium vorgesehenen Sicherheitsmaßnahmen umgesetzt.

### 3.3.2 Zulässige Kommunikationsverbindungen

Sofern die für das Scannen eingesetzten IT-Systeme über ein Netzwerk verbunden sind, muss ein ungesicherter Zugang zu diesem Netzwerksegment verhindert werden. Ein Zugriff aus dem Internet auf dieses Netzsegment darf nicht erfolgen, es sei denn die Kommunikation wird über einen Proxy oder ein Gateway vermittelt und der Verbindungsaufbau erfolgt von innen.

|  |
| --- |
| **Schutz der zulässigen Kommunikationsverbindungen vor Zugriffen von außerhalb** |
| […]  *Beispiel: Folgende in den Notarbüros übliche Konfiguration entspricht den Anforderungen:*   * *Zwischen dem internen Netz und dem Internet regeln ein Router / eine Firewall den Datenverkehr.* * *Alle netzwerkfähigen IT-Systeme, mit welchen auf das Elektronische Urkundenarchiv oder grundsätzlich auf XNP zugegriffen wird, sind entweder über die Registerbox oder über die Notarnetzbox mit dem Notarnetz verbunden.*   *Alternativ: Alle am Scanprozess beteiligten Komponenten und Netzwerke sind mit dem gesamten Büronetzwerk durch eine Firewall geschützt. Netzwerkverbindungen können nur innerhalb dieses abgeschlossenen Netzwerks aufgebaut werden. Für die Übertragung von elektronischen Dokumenten an das Elektronische Urkundenarchiv besteht eine Verbindung mit dem Notarnetz.*  *ggf. ergänzend, falls Service-Schnittstelle vorhanden: Die Scan-Hardware verfügt über eine Service-Schnittstelle, die über das Internet Daten vom Gerätehersteller abruft. Durch eine Firewall wird sichergestellt, dass nur diese Verbindung zum Gerätehersteller außerhalb des internen Netzwerks möglich ist.* |

Die nach Anlage 1 zuständigen Mitarbeiterinnen / Mitarbeiter prüfen die Wirksamkeit der zum Schutz der IT-Infrastruktur vorgesehenen Sicherheitsmaßnahmen, indem er die ordnungsgemäße Umsetzung der Schutzmaßnahmen prüft oder sich diese vom externen Dienstleister bestätigen lässt.

### 3.3.3 Schutz vor Schadprogrammen

Zum effektiven Schutz vor Schadprogrammen müssen die folgenden Maßnahmen durch die gemäß Anlage 1 zuständigen Mitarbeiterinnen / Mitarbeiter umgesetzt werden:

* Auswahl eines geeigneten Viren-Schutzprogramms

|  |
| --- |
| **Eingesetztes Viren-Schutzprogramm** |
| *Produkt […], Version […]* |

* Entgegennahme von Meldungen von Schadprogramm-Infektionen
* Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen:

|  |
| --- |
| **Aktualisierung von Viren-Schutzprogrammen und Signaturen** |
| […]  *Beispiel: Die Aktualisierung erfolgt automatisch.*  *Alternativ: Die Aktualisierung wird von der zuständigen Mitarbeiterin / vom zuständigen Mitarbeiter […] regelmäßig alle […] Tage durchgeführt.* |

* Regelmäßige Datensicherung:

|  |
| --- |
| **Eingesetztes Datensicherungsverfahren** |
| *Beispiel: [keine besondere Empfehlung; vielfältige andere Gestaltungen möglich]*  *Die Vollsicherung erfolgt einmal täglich über USB-Festplatten im Rotationsprinzip. Die nicht angeschlossenen USB-Festplatten werden räumlich getrennt aufbewahrt (Keller).*  *Es erfolgen eine wöchentliche Vollsicherung sowie tägliche inkrementelle Datensicherungen.* |

### 3.3.4 Zuverlässige Speicherung

Die für eine eventuelle Aufbewahrung der Datenobjekte (Scanprodukt, Metadaten etc.) verwendeten Speichermedien, Verfahren (z. B. zur Datensicherung) und Konfigurationen müssen für die notwendige Aufbewahrungsdauer bzw. bis zur zuverlässigen Übergabe an das Elektronische Urkundenarchiv eine Verfügbarkeit gewährleisten, die dem Schutzbedarf „hoch“ entspricht. Der Schutzbedarf „hoch“ gilt uneingeschränkt für alle von dieser Verfahrensdokumentation erfassten Dokumente.

Folgende Maßnahmen gewährleisten die angemessene Verfügbarkeit:

|  |
| --- |
| **Maßnahmen zur Gewährleistung der angemessenen Verfügbarkeit** |
| […]  *Beispiel: Es wird zertifizierte Marken-Hardware (Festplatten) verwendet.*  *Es werden interne und externe Back-ups angefertigt (die Hinterlegung erfolgt an unterschiedlichen Orten).* |

## 3.4 Sicherheitsmaßnahmen bei der Dokumentenvorbereitung

### 3.4.1 Sorgfältige Vorbereitung der Papierdokumente

Die sorgfältige Vorbereitung der Papierdokumente wird unter Abschnitt 2.5.1 behandelt.

### 3.4.2 Vorbereitung der Vollständigkeitsprüfung

Die Vorbereitung der Vollständigkeitsprüfung wird unter Abschnitt 2.5.1 behandelt.

## 3.5 Sicherheitsmaßnahmen beim Scannen

### 3.5.1 Auswahl und Beschaffung geeigneter Scangeräte

Die Bundesnotarkammer benennt Anforderungen an Scansysteme zum Einsatz mit dem Elektronischen Urkundenarchiv. Die Einzelheiten sind in Anlage 2 aufgeführt. Bei der Auswahl und Beschaffung des Scangeräts soll berücksichtigt werden, dass ausreichender Support durch den Hersteller oder den Verkäufer gewährleistet ist.

|  |
| --- |
| **Support-Vereinbarungen** |
| […]  *Beispiel: Mit dem Anbieter wurde ein Wartungsvertrag abgeschlossen, welcher ausreichende Reaktionszeiten im Support-Fall beinhaltet.* |

### 3.5.2 Zutritts- und Zugriffskontrollen für das Scansystem

Um Störungen während des Erfassungsvorgangs und Manipulationen am Scansystem zu verhindern, soll sichergestellt werden, dass unberechtigte Personen keinen Zugang zum Scansystem erhalten. Hierfür sollen geeignete Zugangskontrollen und Besucherregelungen vorgesehen werden. Um insbesondere einen hohen Schutz gegen Manipulationen des Scanners bzw. seiner Konfigurationen, der Dokumente beim Scannen oder gegen das nachträgliche Auslesen von Scanprodukten vom internen Datenträger des Scanners zu erreichen, soll der Zugang zum Scanner generell (d. h. auch außerhalb des Scanvorgangs) auf ein Minimum beschränkt werden. Die folgenden Maßnahmen stellen sicher, dass ausschließlich die zuständigen Mitarbeiterinnen und Mitarbeiter Zugang zu den im Zusammenhang mit dem Scannen eingesetzten Geräten haben.

Hinweis: Hier kann auf bereits im Notarbüro geltende Regelungen Bezug genommen oder weitere Maßnahmen konkretisiert werden (z. B. Verteilung von Eingangsschlüsseln, generelle Anwesenheit der zuständigen Mitarbeiterinnen und Mitarbeiter).

|  |
| --- |
| **Zugang zum Scansystem** |
| […]  *Beispiel: Der Zutritt zum Büro ist nur mit Schlüsseln möglich; die Schlüssel der Mitarbeitenden werden von der Notarin / dem Notar verwaltet.*  *Personen, die nicht im Notarbüro beschäftigt sind, werden im Büro außerhalb des Wartebereichs und der sanitären Anlagen ständig von Mitarbeitenden begleitet.*  *Der Zugriff auf alle Teile des Scansystems ist über die Benutzerverwaltung auf berechtigte Mitarbeitende begrenzt.*  *Nicht zwingend, aber empfohlen: Das Scangerät kann nur bedient werden, wenn sich ein Mitarbeitender authentifiziert hat. [Wenn am Scangerät selbst keine Authentifizierung oder andere Zugriffskontrolle umgesetzt ist, muss sichergestellt sein, dass ausschließlich die in Anlage 1 genannten Mitarbeitenden, physisch auf das Scangerät zugreifen können.] Ein Mitarbeitender ist während des ganzen Scanvorgangs anwesend.* |

Der Administrationsbereich des Scanners bzw. die Konfiguration der Kommunikationsschnittstellen bei netzwerkfähigen Scannern soll durch ein geeignetes Authentisierungsverfahren (d. h. mindestens durch ein geeignetes Passwort) gegen unbefugten Zugriff geschützt werden. Außerdem soll der Zugriff auf die Administrationsschnittstelle durch eine geeignete Netzwerk-Konfiguration auf die notwendigen Systeme eingeschränkt werden.

|  |
| --- |
| **Zugriff auf die Administration des Scangeräts** |
| […]  *Beispiel: Der Administrationsbereich des Scangeräts ist durch ein geeignetes Passwort geschützt. Dieses ist nur der Notarin / dem Notar und der Bürovorsteherin / dem Bürovorsteher bekannt und unterscheidet sich von den Zugangsdaten der Mitarbeiterinnen und Mitarbeiter, die das Scansystem bedienen.*  *Die Fern-Administrationsschnittstelle wurde so konfiguriert, dass der Zugriff nur für den zuständigen Support-Dienstleister (über die IP-Adresse des Dienstleisters) möglich ist.*  *Alternativ: Die Fern-Administrationsschnittstelle wurde deaktiviert.* |

### 3.5.3 Änderung voreingestellter Passwörter

Sofern die Administration des Scanners bzw. die Konfiguration der Kommunikationsschnittstellen bei netzwerkfähigen Scannern mit einem Passwort gesichert ist, muss das Passwort nach der Installation des Scangeräts zurückgesetzt bzw. geändert werden. Als Grundlage für die Vergabe der Passwörter sollen explizit formulierte interne Sicherheitsrichtlinien dienen.

|  |
| --- |
| **Interne Sicherheitsrichtlinien zur Vergabe von Passwörtern** |
| […]  *Beispiele für Richtlinien bei der Vergabe von Passwörtern (aus:* [*Handreichung der Bundesnotarkammer „IT-Sicherheit für Notarinnen und Notare“*](https://www.elektronisches-urkundenarchiv.de/scanprozess)*)*  *Es sind individuelle Kennungen und Passwörter zu verwenden. Jeder Benutzer erhält ein persönliches und geheimes Passwort.*  *Sollte es sich bei der Kennung um eine PIN handeln, muss diese mindestens 4 Ziffern haben.*  *Das Passwort darf nirgendwo aufgeschrieben und niemals weitergegeben werden. Es wird ein sicherer Passwort-Manager benutzt.*  *Ein Passwort muss aus mindestens zwölf Zeichen bestehen.*  *Das Passwort sollte Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen enthalten und nie in einem Wörterbuch zu finden sein.*  *Ein Passwort darf bei der Eingabe nicht am Bildschirm angezeigt werden.*  *Ein Passwort muss umgehend geändert werden, wenn der Verdacht besteht, dass jemand unbefugt Kenntnis erlangt hat.*  *Passwort-Änderungen müssen von den jeweiligen Benutzern selbst durchgeführt werden können.*  *Alle Passwörter von System- oder Anwendungssoftware, die vom Hersteller voreingestellt wurden, sind nach der Installation des Systems umgehend zu ändern.* |

### 3.5.4 Sorgfältige Durchführung von Konfigurationsänderungen

Die Durchführung von Konfigurationsänderungen an einem IT-System im Echtbetrieb, wie z. B. einem Scanner und den entsprechenden Software-Komponenten, ist immer als kritisch einzustufen, weshalb entsprechend sorgfältig vorgegangen werden muss. Vor einer Änderung der Konfiguration soll die alte Konfiguration gesichert werden. Darüber hinaus sollen alle durchgeführten Änderungen von einer weiteren Mitarbeiterin / einem weiteren Mitarbeiter überprüft werden, bevor sie in den Echtbetrieb übernommen werden.

Die Zuständigkeit für die Durchführung von Konfigurationsänderungen ist in Anlage 1 aufgeführt.

### 3.5.5 Geeignete Benutzung des Scangeräts

Um eine zuverlässige und vollständige Erfassung der Papierdokumente zu gewährleisten, muss ein gemäß den Vorgaben des Herstellers gepflegter Scanner eingesetzt werden. Falls das Scanprodukt Streifen, Schlieren oder andere Auffälligkeiten aufweisen sollte, ist das Scangerät entsprechend den Vorgaben aus dem Betriebshandbuch (Herstellerempfehlung) zu reinigen.

Die Dokumente müssen gemäß den Vorgaben der Produkthandbücher und der physikalischen Struktur der Dokumente dem Scanner übergeben werden. Für Dokumente, die nicht für den automatischen Einzug geeignet sind (z. B. ungeeignete Papiersorten, beschädigte Seiten, gebundene Dokumente), sind geeignete Verfahren zu beschreiben.

|  |
| --- |
| **Scanverfahren für Dokumente, die nicht für den automatischen Einzug geeignet sind** |
| […]  *Beispiel: Dokumente, die nicht mithilfe des automatischen Einzugs gescannt werden können, müssen einzeln auf das Vorlagenglas gelegt und gescannt werden. Kann das Dokument aufgrund seiner Beschaffenheit nicht gescannt werden, wird es gemäß § 37 NotAktVV in der Sondersammlung verwahrt.* |

### 3.5.6 Geeignete Scaneinstellungen

Die Scaneinstellungen werden in Abschnitt 2.5.2 behandelt.

### 3.5.7 Geeignete Erfassung von Metainformationen

Damit eine spätere Zuordnung der Scanprodukte zu einem bestimmten Vorgang möglich ist, sollen Metadaten in geeigneter Weise übergeben werden. Bei einem hohen Scan-Durchsatz können Spezifikationen von weiteren Metainformationen, wie z. B. Seitenzahl, Scaneinstellungen, Dokumentenkontext oder Indexinformationen genutzt werden. In diesem Fall kann das Scansystem diese Informationen gegebenenfalls automatisiert auswerten, die Einstellungen anpassen, Scanprodukte entsprechend zusammenfassen und die Metadaten zum Scanprodukt hinzufügen. Es können auch Lösungen zum automatischen Auslesen von Indexinformationen genutzt werden. Allerdings soll dann eine zuverlässige Konfiguration der Applikation bezüglich der Erkennung und Gültigkeit der ausgelesenen Werte und eine sorgfältige manuelle Qualitätssicherung und Nachbearbeitung erfolgen.

|  |
| --- |
| **Maßnahmen für eine geeignete Erfassung von Metainformationen** |
| […]  *Beispiel: Die Zuordnung zu Vorgängen erfolgt im XNP-Modul „Urkundenverzeichnis“.*  *Unmittelbar vor dem Scannen wird der Dateiname über das Bedienpanel des Scangeräts als Metadatum eingegeben, und zwar entsprechend folgendem Schema: [Jahrgang] – [fortlaufende Nummer im Urkundenverzeichnis – xy-stellig, gegebenenfalls durch führende Nullen ergänzt] – [fortlaufende Nummer der Dokumente zum Urkundenverzeichniseintrag, zweistellig, gegebenenfalls durch führende Null ergänzt]. Das Scanprodukt wird dann als entsprechend benannte PDF-Datei ausgegeben, siehe auch Abschnitt 2.5.2 „Zwischenablage und Benennung“.* |

### 3.5.8 Qualitätssicherung der Scanprodukte

Die Qualitätssicherung des Scanprodukts muss durch eine vollständige Sichtkontrolle erfolgen.

### 3.5.9 Sichere Außerbetriebnahme von Scangeräten

Bei der dauerhaften Außerbetriebnahme von Geräten müssen alle sicherheitsrelevanten Informationen sowie zwischenzeitlich gespeicherte Informationen im Scan-Cache oder auf der Scan-Software zuverlässig von den Geräten gelöscht oder anderweitig (z. B. durch entsprechende Maßnahmen in der zur Schlüsselverwaltung vorgesehenen Infrastruktur) deaktiviert werden. Dies gilt auch für Authentisierungsinformationen (z. B. Passwörter, kryptographische Schlüssel), insbesondere dann, wenn die Komponenten ausgesondert und an Dritte weitergegeben werden. Darüber hinaus sollen spezifische Konfigurationsinformationen (z. B. IP-Adressen), die Rückschlüsse auf interne Netzwerkstrukturen liefern können, gelöscht werden.

Sofern das Scangerät einen internen Datenträger besitzt, muss der Datenträger vor der Entsorgung des Scanners zuverlässig gelöscht werden. Sofern es möglich ist, soll der Datenträger hierfür aus dem Scanner ausgebaut und mit einem geeigneten Verfahren zuverlässig gelöscht oder notfalls zerstört werden.

In den Verträgen mit Dienstleistern ist zu regeln, dass ein zuverlässiges und für das Notarbüro nachvollziehbares Lösch- und Entsorgungsverfahren etabliert wird.

|  |
| --- |
| **Maßnahmen bei der Außerbetriebnahme von Scangeräten** |
| […]  *Beispiel: Die Daten werden von allen Datenträgern durch sicheres, nicht-rekonstruierbares Löschen entfernt.*  *Auf den außer Betrieb zu nehmenden Komponenten werden alle Einstellungen, Passwörter und Benutzerkonten gelöscht oder zurückgesetzt.* |

### 3.5.10 Informationsschutz und Zugriffsbeschränkung bei netzwerkfähigen Scangeräten

Bei Scannern, die über ein Netzwerk angesprochen werden können, sollen geeignete Maßnahmen zur Zugriffsbeschränkung und für den Schutz der über das Netzwerk übertragenen Informationen vorgesehen werden. Dies umfasst die Absicherung der Datenübertragung zwischen Scanner und Scan-Workstation oder Scan-Cache sowie die sichere Speicherung und Löschung von Daten auf einem internen Datenträger des Scanners. Sofern Netzlaufwerke für die Ablage von Zwischenergebnissen oder Scanprodukten genutzt werden, muss der Zugriff auf diese Netzlaufwerke auf das notwendige Minimum beschränkt werden. Bei der Nutzung von Multifunktionsgeräten, die eine Scan-to-Mail- oder Scan-to-Fax-Funktion unterstützen, muss durch eine geeignete Konfiguration der für die Übermittlung verwendeten Server der Versand an ungewünschte Empfängerkreise verhindert werden.

|  |
| --- |
| **Maßnahmen und Konfiguration zur Zugriffsbeschränkung** |
| […]  *Beispiel: Grundsätzlich existieren verschlüsselte oder direkte Verbindungen zwischen den IT-Systemen:*   * *Das Scangerät ist über eine direkte LAN-Verbindung mit dem Server verbunden.* * *Der Rechner erhält das Scanprodukt über eine verschlüsselte Verbindung zur Weiterverarbeitung.*   *Der Zugriff auf die Datenablage (Server) ist nur über eine Authentifizierung möglich.*  *Die Möglichkeit von Scan-to-Mail und Scan-to-Fax ist deaktiviert bzw. wird nicht genutzt.* |

### 3.5.11 Protokollierung beim Scannen

Für eine zuverlässige Betriebsführung und die Sicherstellung der Nachvollziehbarkeit des Scanprozesses muss eine geeignete Protokollierung erfolgen, die die folgenden Punkte umfasst:

* Änderung von kritischen Konfigurationsparametern sowie Authentisierungs- und Berechtigungsinformationen:

|  |
| --- |
| **Protokollierung von Änderungen** |
| […]  *Beispiel: Die Notarin / der Notar oder die zuständige Mitarbeiterin / der zuständige Mitarbeiter führt ein elektronisches Protokoll [oder: Protokoll in Papierform] hinsichtlich der Änderung von kritischen Konfigurationsparametern sowie der Änderung von Authentisierungs- und Berechtigungsinformationen. Gegebenenfalls unterstützt der Scanner die automatische Protokollierung der genannten Punkte.* |

* Information, wer das Scansystem, wann und in welcher Weise genutzt hat.

|  |
| --- |
| **Information, wer das Scansystem, wann und in welcher Weise genutzt hat** |
| […]  *Beispiel: Das Gerät wird ausschließlich von nach § 26 BNotO verpflichteten Mitarbeitenden, die in Anlage 1 aufgenommen sind, zum Einscannen von Urkunden und für die Unterstützung der sonstigen notariellen Amtstätigkeit verwendet. [Wenn dies gegeben ist, ist es nur empfohlen, nicht aber zwingend vorgegeben, eine der anderen Maßnahmen umzusetzen.]*  *Empfohlen, aber nicht zwingend: In der Nebenakte zur Urkunde wird (auf einem Laufblatt) vermerkt, wann und von wem (Kürzel) die Urkunde gescannt wurde.*  *Alternativ, nicht zwingend: Die zuständige Mitarbeiterin / Der zuständige Mitarbeiter führt ein Protokoll (z. B. Excel-Liste) mit der Information, wer das Scansystem, wann und in welcher Weise genutzt hat.*  *Alternativ, nicht zwingend: Das Scangerät bietet die Möglichkeit, automatisiert Protokolldateien über die Authentisierung und Verwendung anzulegen.* |

* Information, ob eine manuelle Nachbearbeitung des Scanproduktes stattgefunden hat:

|  |
| --- |
| **Information über eine manuelle Nachbearbeitung des Scanproduktes** |
| […]  *Beispiel: Jede manuelle bildliche Nachbearbeitung der gescannten Urkunde, wird im Übereinstimmungsvermerk erwähnt (siehe Abschnitt 2.5.4). Bei einem Mangel der Scandatei, der zu einer solchen Erwähnung im Übereinstimmungsvermerk führen würde, wird im Normalfall der Scanvorgang noch einmal durchgeführt.* |

* Fehlgeschlagene Authentisierungsvorgänge und sonstige aufgetretene Fehler:

|  |
| --- |
| **Fehlgeschlagene Authentisierungsvorgänge / Sonstige Fehler** |
| […]  *Beispiel: Auffälligkeiten und Fehler bei der Authentisierung werden sogleich der Notarin / dem Notar / der Bürovorsteherin / dem Bürovorsteher mitgeteilt, um das weitere Vorgehen zu klären.*  *Weiteres Beispiel: Das Scangerät bietet die Möglichkeit, automatisiert Protokolldateien über fehlgeschlagene Authentisierungsvorgänge und sonstige Fehler anzulegen.* |

* Die Protokolldaten müssen gemäß den geltenden datenschutzrechtlichen Bestimmungen verarbeitet und insbesondere vor unautorisiertem Zugriff geschützt werden:

|  |
| --- |
| **Schutz gemäß den datenschutzrechtlichen Bestimmungen** |
| […]  *Beispiel: Eine automatisierte Protokollierung von personenbezogenen Daten findet nicht statt. Für die jegliche sonstige Protokollierung werden nur die Kürzel der Mitarbeitenden verwendet. Die Protokolldaten sind nur befugten Mitarbeitenden zugänglich.*  *Alternativ: Für jegliche Protokollierung werden nur die Kürzel der Mitarbeitenden verwendet. Die Protokolldaten sind nur befugten Mitarbeitenden zugänglich.*  *Protokolldaten werden nach 30 Tagen vernichtet bzw. gelöscht, soweit sie nicht Bestandteil von Aufzeichnungen mit längerer Aufbewahrungsfrist sind (z.B. Nebenakte).*  *[ggf.] Die automatisiert erfassten Protokolldaten werden nach 30 Tagen gelöscht.* |

### 3.5.12 Auswahl geeigneter Bildkompressionsverfahren

Die Auswahl geeigneter Bildkompressionsverfahren wird in Abschnitt 2.5.2 behandelt.

## 3.6 Sicherheitsmaßnahmen bei der Nachverarbeitung

### 3.6.1 Geeignete und nachvollziehbare Nachverarbeitung

Die Nachverarbeitung wird in Abschnitt 2.5.3 behandelt.

### 3.6.2 Qualitätssicherung der nachverarbeiteten Scanprodukte

Sofern eine Nachverarbeitung der Scanprodukte erfolgt, muss im Rahmen der durchgeführten Operationen in jedem Fall eine Qualitätssicherung erfolgen, so dass gewährleistet ist, dass durch die Nachverarbeitung keine relevanten Informationen verloren gegangen sind. Die ursprünglichen Scanprodukte dürfen nicht vor Abschluss der Qualitätskontrolle gelöscht werden. Im Übereinstimmungsvermerk wird die inhaltliche und bildliche Übereinstimmung von Urkunde und Scanprodukt bestätigt. Darin ist auch eine weitere Qualitätssicherung zu sehen.

### 3.6.3 Durchführung der Vollständigkeitsprüfung

Die Vollständigkeitsprüfung erfolgt anhand einer vollständigen Sichtkontrolle (siehe Abschnitt 2.5.3).

### 3.6.4 Übereinstimmungsvermerk

Der Übereinstimmungsvermerk wird in Abschnitt 2.5.4 behandelt.

## 3.7 Sicherheitsmaßnahmen bei der Integritätssicherung

### 3.7.1 Nutzung geeigneter Dienste und Systeme für den Integritätsschutz

Um eine unerkannte nachträgliche Manipulation der während des Scanprozesses entstehenden Datenobjekte (Scanprodukt, Übereinstimmungsvermerk, gegebenenfalls Index- und Metadaten, Protokolldaten etc.) zu verhindern, müssen geeignete Mechanismen für den Schutz der Integrität dieser Datenobjekte eingesetzt werden.

Zum Schutz von Integrität und Authentizität wird im Rahmen des Elektronischen Urkundenarchivs für alle Datenobjekte (Scanprodukt, Übereinstimmungsvermerk, gegebenenfalls durch zusätzliche Software erstellte Index- und Metadaten, Protokolldaten im Übereinstimmungsvermerk) eine qualifizierte elektronische Signatur verwendet.

Zuständig für die den signaturrechtlichen Anforderungen entsprechenden Signaturen und Zertifikate im Kontext des Elektronischen Urkundenarchivs ist die zur Bundesnotarkammer gehörende Zertifizierungsstelle als qualifizierter Vertrauensdiensteanbieter gemäß Art. 20 Abs. 1 Satz 1 eIDAS-Verordnung. Die auf den qualifizierten Zertifikaten der Zertifizierungsstelle der Bundesnotarkammer beruhenden Signaturen genügen den Anforderungen an qualifizierte elektronische Signaturen im Sinne des Art. 3 Nr. 12 eIDAS-Verordnung.

# Aufbaumodule

Die Technische Richtlinie 03138 – Ersetzendes Scannen (RESISCAN) des Bundesamts für Sicherheit in der Informationstechnik (BSI) sieht im Rahmen von Aufbaumodulen erhöhte Scananforderungen für Dokumente mit erhöhtem Schutzbedarf aufgrund erhöhter Integritäts-, Vertraulichkeits- oder Verfügbarkeitsanforderungen vor. Die im Folgenden aufgenommenen erhöhten Scananforderungen gelten uneingeschränkt für alle von dieser Verfahrensdokumentation betroffenen Dokumente.

## 4.1 Generelle Maßnahmen bei erhöhtem Schutzbedarf

### 4.1.1 Beschränkung des Zugriffs auf sensible Papierdokumente

Bei der Verarbeitung von Dokumenten mit einem Schutzbedarf von zumindest „hoch“ bzgl. der Integrität, Vertraulichkeit oder Verfügbarkeit sollen während der Vorbereitung und während des Scanvorgangs keine unbefugten Personen Zugriff auf die Papierdokumente erhalten. Deshalb sollen geeignete Maßnahmen für die Beschränkung des Zugriffs auf die sensiblen Papierdokumente getroffen werden:

* Der Zugang zu den Räumen, in denen die Urkunden verarbeitet werden, wird durch die folgenden Maßnahmen beschränkt:

|  |
| --- |
| **Zugangsbeschränkungen** |
| […]  *Beispiel: Der Raum ist nur für Mitarbeitende des Notarbüros zugänglich und es existiert eine Liste zur Schlüsselverwaltung. Personen, die nicht im Notarbüro beschäftigt sind, werden im Büro außerhalb des Wartebereichs und der sanitären Anlagen ständig von Mitarbeitenden begleitet.*  *Nicht zwingend, aber empfehlenswert: Es ist eine Einbruchmeldeanlage installiert.* |

* Aufbewahrung, die Schutz vor unbefugtem Zugriff, Einsichtnahme oder Beschädigung bietet:

|  |
| --- |
| **Geschützte Aufbewahrung der Urkunden** |
| […]  *Beispiel: Die Dokumente werden in Räumen aufbewahrt, die nur für die Mitarbeitenden zugänglich sind, die mit den Dokumenten im Rahmen ihrer Tätigkeit umgehen dürfen (Anlage 1).*  *Alternativ: Die Dokumente werden in Dokumentenmappen aufbewahrt. Die Dokumentenmappen werden in abschließbaren Aktenschränken aufbewahrt.* |

* Verpflichtung der Mitarbeitenden zur sorgfältigen Handhabung der Dokumente:

|  |
| --- |
| **Verpflichtung der Mitarbeitenden** |
| […]  *Beispiel: Die Mitarbeitenden im Notarbüro werden bei Aufnahme der Tätigkeit nach § 26 BNotO i.V.m. dem Verpflichtungsgesetz besonders verpflichtet und unterliegen u.a. § 203 StGB zur vertraulichen Handhabung. Sie werden im Übrigen in die sorgfältige Handhabung der Dokumente bei Aufnahme ihrer Tätigkeit eingewiesen.* |

### 4.1.2 Pflicht zur Protokollierung beim Scannen

Siehe Abschnitt 3.5.11 „Protokollierung beim Scannen“.

### 4.1.3 Pflicht zur regelmäßigen Auditierung

Siehe Abschnitt 3.1.9 „Einhaltung der Informationssicherheit”.

## 4.2 Zusätzliche Maßnahmen bei hohen Integritätsanforderungen

### 4.2.1 Einsatz kryptographischer Mechanismen zum Integritätsschutz

Bei der Verarbeitung von Datenobjekten mit einem Schutzbedarf von zumindest „hoch“ bezüglich der Integrität sollen geeignete kryptographische Mechanismen in Form von fortgeschrittenen elektronischen Signaturen zum Einsatz kommen. Im Rahmen des Elektronischen Urkundenarchivs werden zum Integritäts- und Authentizitätsschutz qualifizierte elektronische Signaturen verwendet.

### 4.2.2 Geeignetes Schlüsselmanagement

Sofern schlüsselbasierte kryptographische Mechanismen eingesetzt werden, müssen geeignete Verfahren für das Schlüsselmanagement vorgesehen werden. Hierbei sollen vertrauenswürdige Dienstleister (z. B. qualifizierte Vertrauensdiensteanbieter gemäß Art. 3 Nr. 20 eIDAS-Verordnung) für das Schlüsselmanagement genutzt werden.

Zuständig für die Zertifikats- und Schlüsselverwaltung im Kontext des Elektronischen Urkundenarchivs ist die zur Bundesnotarkammer gehörende Zertifizierungsstelle als qualifizierter Vertrauensdiensteanbieter im Sinne des Art. 20 Abs. 1 Satz 1 eIDAS-Verordnung. Die auf den qualifizierten Zertifikaten der Zertifizierungsstelle der Bundesnotarkammer beruhenden Signaturen genügen den Anforderungen an qualifizierte elektronische Signaturen im Sinne des Art. 3 Nr. 12 eIDAS-Verordnung.

|  |
| --- |
| **Sichere Aufbewahrung der N-Karten / Signaturkarten** |
| […]  *Beispiel: Die N-Karten / Signaturkarten werden immer persönlich von der Notarin / von dem Notar verwahrt.*  *Alternativ: Die N-Karten / Signaturkarten werden bei Nichtbenutzung im verschlossenen Aktenschrank / in einem verschlossenen Behältnis gelagert.* |

### 4.2.3 Auswahl eines geeigneten kryptographischen Verfahrens

Sofern kryptographische Verfahren eingesetzt werden, müssen geeignete kryptographische Verfahren verwendet werden, die den geltenden Richtlinien des Bundesamts für Sicherheit in der Informationstechnik entsprechen.

Zuständig für die Auswahl eines geeigneten kryptografischen Verfahrens im Kontext des Elektronischen Urkundenarchivs ist die zur Bundesnotarkammer gehörende Zertifizierungsstelle als qualifizierter Vertrauensdiensteanbieter im Sinne des Art. 20 Abs. 1 Satz 1 eIDAS-Verordnung.

### 4.2.4 Auswahl eines geeigneten kryptographischen Produktes

Zur Integritätssicherung müssen geeignete Produkte hinsichtlich Funktionalität und Vertrauenswürdigkeit eingesetzt werden. Bei der Funktionalität ist vor allem auf eine ausreichende Stärke und Widerstandsfähigkeit der eingesetzten Sicherheitsmechanismen zu achten. Hinsichtlich der Vertrauenswürdigkeit sind der Einsatz veröffentlichter und gemeinschaftlich analysierter Algorithmen und Quellen sowie durchgeführte Prüfungen nach einem anerkannten Sicherheitsstandard wie FIPS-140, Common Criteria oder ITSEC positiv zu bewerten und sollten daher primär herangezogen werden. Im Rahmen des Elektronischen Urkundenarchivs wird das kryptografische Produkt „proNEXT Signaturanwendungskomponente (SAK)” verwendet. proNEXT Secure Framework ist nach Common Criteria in der Prüfstufe EAL 4+ mit AVA VAN.5 (vollständige Missbrauchsanalyse und hohes Angriffspotential) durch den TÜV-IT auditiert und zertifiziert.

### 4.2.5 Langfristige Datensicherung bei Einsatz kryptographischer Verfahren

Für die eingesetzten kryptographischen Verfahren soll die Eignung der eingesetzten Algorithmen und Parameter regelmäßig evaluiert werden, da der Beweiswert von qualifiziert elektronisch signierten Daten über längere Zeiträume erhalten bleiben soll. Daher sind diese durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen. Die verwendeten Algorithmen zur Signaturerstellung und -prüfung werden zur Sicherung deren Aktualität stetig mit dem Algorithmenkatalog des BSI abgeglichen. Mit entsprechender Vorlaufzeit werden bei Bedarf neue bzw. andere durch den Algorithmenkatalog des BSI vorgeschlagene Algorithmen eingeführt, sodass eine langfristige Datensicherung gewährleistet werden kann.

### 4.2.6 Verhinderung ungesicherter Netzzugänge

Siehe Abschnitt 3.3.2 „Zulässige Kommunikationsverbindungen“

## 4.3 Zusätzliche Maßnahmen bei hohen Vertraulichkeitsanforderungen

### 4.3.1 Sensibilisierung und Verpflichtung der Mitarbeitenden

Siehe Abschnitt 3.2.2.4 „Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Informationssicherheit“

### 4.3.2 Verhinderung ungesicherter Netzzugänge

Siehe Abschnitt 3.3.2 „Zulässige Kommunikationsverbindungen“

### 4.3.3 Löschen von Zwischenergebnissen

Bei der Verarbeitung von Dokumenten müssen die entstandenen Zwischenergebnisse (z. B. rohe Scanprodukte, Daten im Scan-Cache, Auslagerungsdateien) zuverlässig gelöscht werden. Die Zuständigkeit für das Löschen von Zwischenergebnissen ist in Anlage 1 aufgeführt.

|  |
| --- |
| **Maßnahmen für das zuverlässige Löschen von Zwischenergebnissen** |
| […]  *Beispiel: Die Löschung von Zwischenergebnissen durch einen berechtigten Mitarbeitenden erfolgt am Ende jeder Arbeitswoche. Die Sicherheit der Scan-Räumlichkeiten durch die Anwesenheit von berechtigen Mitarbeitenden ist gewährleistet.*  *Alternativ: Vor dem Verlassen der Scan-Räumlichkeiten sind die Zwischenergebnisse auf dem Scangerät manuell zu löschen (z. B. durch eine spezielle Funktion).*  *Alternativ: Eine Löschung von Zwischenergebnissen erfolgt am Ende eines jeden Arbeitstages.* |

## 4.4 Zusätzliche Maßnahmen bei hohen Verfügbarkeitsanforderungen

### 4.4.1 Erweiterte Qualitätssicherung

Siehe Abschnitt 3.5.8 „Qualitätssicherung der Scanprodukte“

### 4.4.2 Fehlertolerante Protokolle und redundante Datenhaltung

Die Verwendung eines fehlertoleranten Übertragungsprotokolls sowie eine redundante Datenhaltung werden empfohlen.

|  |
| --- |
| **Fehlertolerante Protokolle und redundante Datenhaltung** |
| […]  *Beispiel: Es werden fehlertolerante Übertragungsprotokolle verwendet, bei denen nicht unbemerkt eine Übertragung fehlschlagen kann (z. B. SFTP/SMB/HTTPS).*  *Im Falle des Verlustes des Scanproduktes ist die Originalurkunde noch vorhanden und kann erneut eingescannt werden. Nach dem zentralen Archivieren des Scanprodukts in der elektronischen Urkundensammlung ist das Elektronische Urkundenarchiv für die Datenhaltung zuständig. Bei der zentralen Archivierung in der elektronischen Urkundensammlung stellt die Bundesnotarkammer die Nutzung fehlertoleranter Protokolle sicher*. |

# Anlagenverzeichnis

Folgende Anlagen sind Bestandteil dieser Muster-Verfahrensdokumentation:

* Anlage 1 „Zuständigkeiten“
* Anlage 2 „Anforderungen an Scan-Systeme zum Einsatz mit dem Elektronischen Urkundenarchiv“
* Anlage 3 „Rechtliche Rahmenbedingungen“

1. Sofern nicht anders ausgewiesen, beziehen sich Zitate von Vorschriften auf die am 1. Januar 2022 geltende Fassung. [↑](#footnote-ref-2)
2. Das ist die im Streitfall identifizierbare natürliche Person, die die Erstellung des Scanprodukts verantwortet, also die Notarin / der Notar. [↑](#footnote-ref-3)
3. Es spricht nichts dagegen, alle Mitarbeitenden des Notarbüros auch für den Scanprozess zu benennen. Sie sind nach § 26 BNotO besonders verpflichtet und werden in der Regel ohnehin mit den Urkunden umgehen, die auch Gegenstand des Scanprozesses sind. Wenn alle Mitarbeiterinnen und Mitarbeiter in Anlage 1 als für den Scanprozess zuständige Mitarbeiter aufgenommen sind, dürfen auch alle Zugriff auf den Scan-Ordner haben. [↑](#footnote-ref-4)