

# ArchiSafe

## Schutzbedarf für Archivierungssysteme

Dokumententitel: Schutzbedarf für Archivierungssysteme  
Dateiname: 2005-09-04\_Schutzbedarf ArchiSafe\_V10.doc  
Version: 1.0  
Anzahl Seiten: 22  
Status: Abgestimmte Version zur Vorlage für Nutzerbeirat

erstellt am: 04.09.2005 von: Christian Koob, Jobst Biester  
geprüft am: von:  
geändert am: von:  
Freigegeben am: von:

Standort:  
Verteiler:

## Inhalt

|          |   |           |
|----------|---|-----------|
| <b>0</b> | <b>Versionshistorie .....</b>   | <b>4</b>  |
| 0.1      | Dokumentverantwortlicher .....  | 4         |
| 0.2      | Verteilerliste.....   | 4         |
| <b>1</b> | <b>Zielsetzung des Dokumentes .....</b>                                       | <b>5</b>  |
| 1.1      | Zielsetzung .....   | 5         |
| 1.2      | Adressat.....   | 5         |
| 1.3      | Basis der Sicherheitsanforderungen .....                                      | 5         |
| 1.4      | Abgrenzung .....  | 6         |
| <b>2</b> | <b>Architektur .....</b>  | <b>8</b>  |
| <b>3</b> | <b>Sicherheitsanforderungen.....</b>  | <b>10</b> |
| 3.1      | <b>Zu archivierende Daten .....</b>   | <b>10</b> |
| 3.1.1    | <i>Authentizität .....</i>  | <i>10</i> |
| 3.1.2    | <i>Integrität.....</i>  | <i>11</i> |
| 3.1.3    | <i>Verfügbarkeit.....</i>   | <i>11</i> |
| 3.1.4    | <i>Vertraulichkeit (Schutz von Geheimnissen).....</i>                         | <i>12</i> |
| 3.2      | <b>Archivierte Daten .....</b>  | <b>12</b> |
| 3.2.1    | <i>Signaturerneuerung (Beweiskraft).....</i>                                  | <i>12</i> |
| 3.2.2    | <i>Authentizität .....</i>  | <i>14</i> |
| 3.2.3    | <i>Integrität.....</i>  | <i>15</i> |
| 3.2.4    | <i>Verfügbarkeit.....</i>   | <i>15</i> |
| 3.2.5    | <i>Vertraulichkeit (Schutz von Geheimnissen).....</i>                         | <i>15</i> |
| 3.2.6    | <i>Umfang der Archivierung.....</i>   | <i>16</i> |
| 3.2.7    | <i>Zeitpunkt der Archivierung.....</i>  | <i>16</i> |
| 3.2.8    | <i>Löschen von übertragenen Dokumenten im Vorgangsbearbeitungssystem.....</i> | <i>18</i> |
| 3.2.9    | <i>Dauer der Archivierung.....</i>  | <i>19</i> |
| 3.2.10   | <i>Löschen von Daten im Archivierungssystem.....</i>                          | <i>19</i> |
| 3.2.11   | <i>Abfrage von archivierten Dokumenten im Archivierungssystem.....</i>        | <i>19</i> |
| 3.2.12   | <i>Technisch-Organisatorische Anforderungen.....</i>                          | <i>19</i> |
| 3.3      | <b>Signaturerzeugung .....</b>  | <b>20</b> |



Schutzbedarf für  
Archivierungssysteme



|     |                            |    |
|-----|----------------------------|----|
| 3.4 | Signaturverifikation ..... | 21 |
| 4   | Literatur.....             | 23 |

## 0 Versionshistorie

| Version | Editor         | Datum      | Kommentar  |
|---------|----------------|------------|--|
| 0.1     | Christian Koob | 03.03.2005 | Dokument erstellt                                  |
| 0.2     | Christian Koob | 12.04.2005 | Abbildung und Erklärung der Architektur eingefügt. |
| 0.3     | Christian Koob | 27.04.2005 | Einarbeitung der ArchiSig-Anforderungen            |
| 0.4     | Jobst Biester  | 29.04.2005 | QS   |
| 0.5     | Jobst Biester  | 26.05.2005 | Überarbeitung anhand von Kommentaren               |
| 1.0     | Jobst Biester  | 04.09.2005 | Abgestimmte Version für Nutzerbeirat               |

### 0.1 Dokumentverantwortlicher

**Erläuterung:** Benennen Sie den zentralen Ansprechpartner für das vorliegende Dokument. Dieser *Dokumentverantwortliche* ist - unabhängig - von den bearbeitenden Autoren für die Koordination der Bearbeitungsmaßnahmen verantwortlich. Es gibt nur einen Dokumentverantwortlichen.

| Rolle                    | Name / OE      | Bemerkung |
|--------------------------|----------------|-----------|
| Dokumentverantwortlicher | Christian Koob |           |

### 0.2 Verteilerliste

**Erläuterung:** In dem Abschnitt „Verteilerliste“ wird die jeweilige Rolle mit der Person benannt, die das vorliegende Dokument benötigt.

| Rolle             | Name / OE                       | Bemerkung |
|-------------------|---------------------------------|-----------|
| Projektleiter PTB | Tobias Schäfer                  |           |
| CC VBPO           | Dr. Ulrike Rausch               |           |
| CAT               | Uwe Hanewald<br>Dr. Wolf Zimmer |           |
| CC DS             | Jobst Biester                   |           |

# 1 Zielsetzung des Dokumentes

## 1.1 Zielsetzung

Innerhalb der elektronischen Vorgangsbearbeitung und der Dokumentenverwaltung fallen Daten an - wie z. B. eingereichte Anträge oder ganze Vorgänge - die elektronisch archiviert werden müssen. Dabei müssen technische und organisatorische Rahmenbedingungen berücksichtigt werden, um eine langfristige Rechtsverbindlichkeit und Beweiskraft der archivierten Daten zu erreichen (rechtsverbindliche Langzeitarchivierung).

Beim Einsatz der elektronischen Signatur und insbesondere bei einer qualifizierten elektronischen Signatur entstehen Problemfelder, die so in der papiergebundenen Welt nicht vorhanden sind.

Ziel dieses Dokuments ist es, die Sicherheitsanforderungen an ein elektronisches Archivierungssystem hinsichtlich der Archivierung von Dokumenten mit qualifizierten elektronischen Signaturen zu erarbeiten.

## 1.2 Adressat

Die Sicherheitsanforderungen richten sich primär an

- a) alle Behörden, die beabsichtigen, ein Archivierungssystem im eigenen Hause oder im Ressort einzusetzen und für ihre speziellen Bedürfnisse eine Handreichung benötigen, um ihr konkretes Archivierungs-Einsatzszenario hinreichend abzusichern,
- b) Betreiber eines Archivierungssystems, die das Archivierungssystem im Sinne einer Dienstleistung anbieten und
- c) Hersteller von Archivierungssystemen und/oder Vorgangsbearbeitungssystemen.

## 1.3 Basis der Sicherheitsanforderungen

Die Sicherheitsanforderungen basieren unter anderem auf folgenden Informationen:

- DOMEA Organisationskonzept, Version 2.0 [OrgKonz20]
- ArchiSig, Version 2.0 [ArchiSig2002].

## 1.4 Abgrenzung

In diesem Dokument wird schwerpunktmäßig die Problematik der Langzeitarchivierung von Dokumenten mit qualifizierten elektronischen Signaturen erörtert. Die formulierten Sicherheitsanforderungen basieren u. a. auf der Annahme, dass allgemeine Anforderungen an eine elektronische Langzeitarchivierung von Dokumenten bereits durch das Archivierungssystem umgesetzt werden. Diese allgemeinen Anforderungen sind z.B.:

- Jedes Dokument muss zeitnah wiedergefunden werden können
- Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist
- Unterstützung verschiedener Indizierungs- und Recherchestrategien, um auf die gesuchte Information direkt zugreifen zu können
- Speicherung beliebiger Informationsobjekte, vom ASCII-Textdateien über gescannte Faksimile und PDF-Dateien bis hin zu komplexen XML-Strukturen, Listen oder ganzen Datenbankinhalten, wobei eine Beschränkung auf geeignete, langfristig stabile Formate erfolgen sollte.
- Standardisierte Schnittstellen, um elektronische Archive als Dienste in beliebige Anwendungen integrieren zu können.

Auf diese allgemeinen Anforderungen wird in diesem Papier nicht weiter eingegangen, es sei denn, sie stehen im unmittelbaren Zusammenhang mit der Archivierung von Dokumenten mit qualifizierten elektronischen Signaturen.

Elektronische Dokumente, elektronische Akten oder elektronische Vorgänge werden im Folgenden kurz als Daten bezeichnet.

Die Ergebnisse des Projekts ArchiSig [ArchiSig2002] werden in dem vorliegenden Dokument berücksichtigt. Die entsprechenden Anforderungen werden zitiert und ggf. weiter ausgeführt.

Zunächst werden Annahmen getroffen, die sich aus einer Betrachtung der Funktionalitäten von Vorgangsbearbeitungssystemen und Archivierungssystemen ableiten:

**Annahme:**

Ein Archivierungssystem kann den Schutzbedarf der zu archivierenden Daten nicht ermitteln, da es technisch dazu nicht ausgelegt ist.

Dies bedeutet insbesondere, dass der Schutzbedarf bezüglich Vertraulichkeit, Authentizität und Integrität der zu archivierenden Daten bereits vor Übertragung in das Archivierungssystem feststehen muss und durch entsprechende Maßnahmen im Vorgangsbearbeitungssystem umgesetzt ist.

Eine solche Maßnahme könnte für Daten, deren Schutzbedarf an die Vertraulichkeit als „sehr hoch“ eingestuft wurde (z.B. ein medizinisches Gutachten), eine verschlüsselte Speicherung im Vorgangsbearbeitungssystem erfordern. Dies wäre eine technische Maßnahme. Möglich wäre aber auch, dass die Vertraulichkeit durch eine Kombination von Zugangs- und Zugriffsschutz (z.B. Vier-Augen-Prinzip) zur Datenbank realisiert wird. Dies wäre eine Kombination aus baulicher und organisatorischer Maßnahme.

Bauliche oder organisatorische Maßnahmen, welche die Vertraulichkeit von Daten im Vorgangsbearbeitungssystem gewährleisten, sind unwirksam, sobald die Daten zum Archivierungssystem übertragen werden. Auch kann in der Regel nicht davon ausgegangen werden kann, dass beim Archivierungssystem dieselben baulichen und organisatorischen Maßnahmen wie beim Vorgangsbearbeitungssystem umgesetzt sind. Dies führt zu folgender Annahme:

**Annahme:**

Das Vorgangsbearbeitungssystem gewährleistet durch technische Maßnahmen (Verschlüsselung), dass die Vertraulichkeit der Daten während des Transports zum Archivierungssystem gesichert ist und informiert das Archivsystem über den Schutzbedarf der Daten.

Für besondere personenbezogene Daten wie rassische oder ethnische Herkunft, Gesundheit, Sexualleben, ... (vgl. [BDSG2003], §3 Abs. 9 BDSG) ist zwingend eine Verschlüsselung erforderlich, unabhängig davon, ob das Archivsystem durch bauliche und organisatorische Maßnahmen geschützt ist.

## 2 Architektur

Große Organisationen werden ihre eigenen Archive zentral in der Organisation aufbauen und betreiben. Für mittlere und kleinere Organisationen aber wird aufgrund der hohen Investitionskosten für die Anschaffung und der laufenden Kosten für den Betrieb eines Archivs die Nutzung von Archivierungs-Dienstleistungen externer Diensteanbieter immer mehr an Bedeutung gewinnen. Gegenstand einer solchen Dienstleistung ist es, einer Organisation eine Archivierungs-Infrastruktur inklusive der zugehörigen Service-Levels anzubieten.

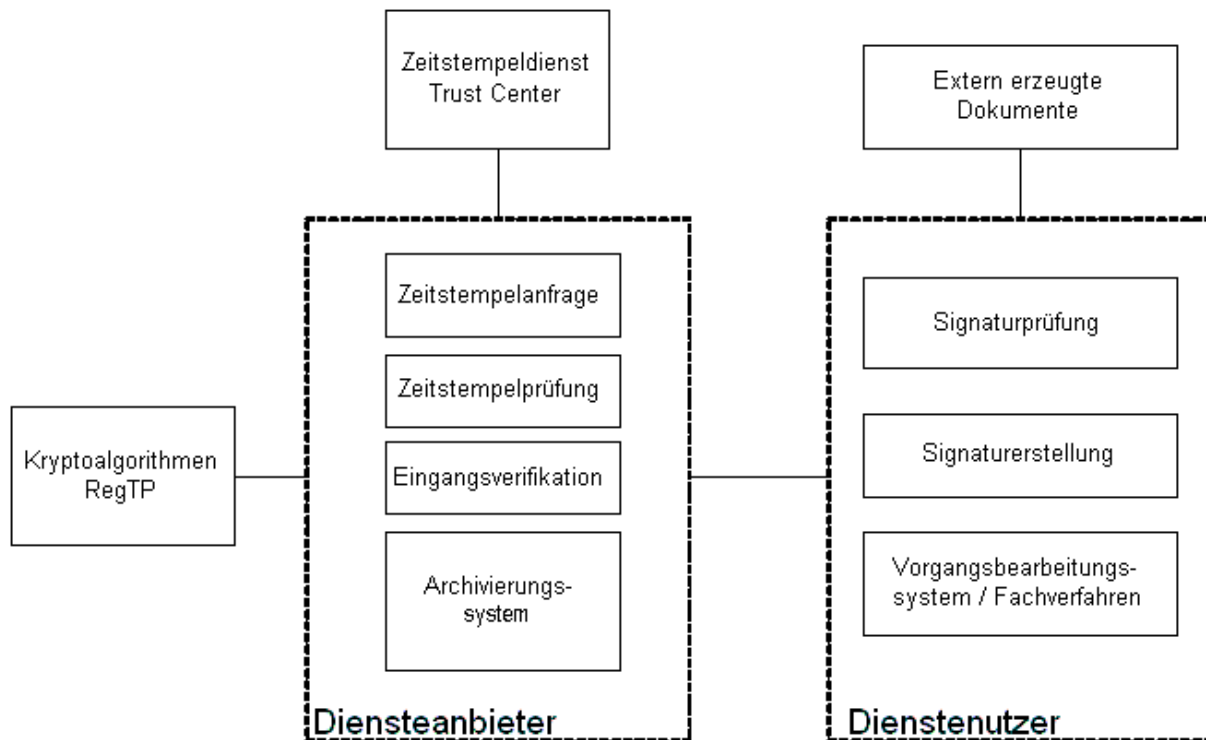
Die im Folgenden beschriebene diensteorientierten Architektur entspricht jedoch nicht nur den Interessen kleiner und mittlerer Organisationen an einer rechtsverbindlichen Langzeitarchivierung. Sie entspricht dem allgemeinen Architekturprinzip, dass für alle Bund-Online-Dienstleistungen gilt, und dient auch den Interessen große Organisationen.

Abbildung 1 zeigt eine solche Archivierungs-Infrastruktur mit den erforderlichen Komponenten, die im Weiteren kurz erläutert werden. Der Diensteanbieter hostet das Archiv. Darüber hinaus muss der Diensteanbieter in der Lage sein, für zu archivierende Daten einen qualifizierten Zeitstempel bei einem Zeitstempeldienst (i.d.R. bei einem Trust-Center) anzufordern (Komponente Zeitstempelanfrage) und dessen Authentizität anschließend zu prüfen (Komponente Zeitstempelprüfung), um die Beweiskraft der Daten, die in das Archiv eingestellt werden zu gewährleisten. Dies erfordert u.a., dass die als geeignet eingestuft Kryptoalgorithmen sowie deren Gültigkeitszeitraum<sup>1</sup> zu berücksichtigen sind. Zurzeit muss diese Information im System nachgehalten (konfiguriert) werden. Es wäre aber wünschenswert, dass die BNetzA diese Information für jedermann jederzeit elektronisch verfügbar/abrufbar hält.<sup>2</sup>

---

<sup>1</sup> Die Veröffentlichung der geeigneten Kryptoalgorithmen erfolgt durch die Bundesnetzagentur (BNetzA)

<sup>2</sup> Vgl. Frye, Pordesch, DUD, S. 73 ff.



**Abbildung 1: Architektur einer Archivierungs-Infrastruktur**

Ein Dienstenutzer empfängt Daten von außerhalb der Organisation (z.B. über die Virtuelle Poststelle des Bundes) und/oder erzeugt Daten innerhalb der Organisation im Rahmen einer Fachanwendung. Ein Mitarbeiter der Organisation prüft, ob die empfangenen Daten<sup>3</sup> qualifiziert elektronisch signiert sind. Falls ja, prüft er die qualifizierte elektronische Signatur (Komponente Signaturprüfung). Die im Rahmen einer Fachanwendung erzeugten Daten kann ein Mitarbeiter mit einer qualifizierten elektronischen Signatur versehen (Komponente Signaturerstellung).

Das vorliegende Dokument formuliert den Schutzbedarf anhand der in Abbildung 1 gezeigten verteilten ArchiSafe-Architektur. Die Architektur schließt nicht aus, dass die Rollen Diensteanbieter und Dienstenutzer zusammenfallen.

<sup>3</sup> Nicht zu verwechseln mit der OSCI-Transport-Signatur, die automatisch durch die Virtuelle Poststelle des Bundes geprüft wird.

## 3 Sicherheitsanforderungen

Die folgenden Sicherheitsanforderungen orientieren sich an den Grundwerten der IT-Sicherheit: Integrität, Authentizität, Vertraulichkeit und Verfügbarkeit.

### 3.1 Zu archivierende Daten

#### 3.1.1 Authentizität

**Anforderung:**

Ein muss sichergestellt werden, dass nur authentische Daten archiviert werden.

Die Authentizität eingehender Daten sollte geprüft (Signaturverifikation, vgl. Abschnitt 3.4) und das geprüfte Dokument im Vorgangsbearbeitungssystem abgelegt werden, so dass im Vorgangsbearbeitungssystem nur authentische Daten vorgehalten werden. In diesem Fall reduziert sich die o.g. Anforderung aus Sicht eines Archivierungssystems darauf, nur Daten bzw. Datensätze aus einem authentischen Vorgangsbearbeitungssystem entgegenzunehmen. Eine geeignete technische Umsetzung dieser Anforderung sollte eine gegenseitige Authentisierung zwischen Vorgangsbearbeitungssystem und Archivierungssystem erzwingen. Zu berücksichtigen sind hierbei die Fragen, ob das Vorgangsbearbeitungssystem und Archivierungssystem lokal oder global angebunden sind und ob die Verbindung zwischen Vorgangsbearbeitungssystem und Archivierungssystem permanent oder temporär ist.

Sofern das Archivierungssystem nicht davon ausgehen kann, dass eine Signaturverifikation bereits stattgefunden hat, z.B. bei Signaturen, die innerhalb einer Organisation erzeugt wurden, muss eine automatisierte vollständige Signaturverifikation (Eingangsprüfung) erfolgen.<sup>4</sup>

<sup>4</sup> Siehe ArchiSig-Anforderung A21 (vgl. [ArchiSig2002], Seite 87)

### 3.1.2 Integrität

Die Integrität zu archivierender Daten kann vorsätzlich oder zufällig verletzt werden.

**Anforderung:**

Ein Archivierungssystem muss die Integrität übertragener Daten prüfen können.

Verläuft die in Abschnitt 3.1.1 durchgeführte Prüfung der Authentizität eingehender Daten erfolgreich, ist somit implizit auch die Integrität der Daten im Vorgangsbearbeitungssystem geprüft. Erfolgt nun die Übertragung in das Archiv, ist zwischen dem Vorgangsbearbeitungssystem und dem Archivierungssystem ein Mechanismus zu etablieren, der sicherstellt, dass im Falle eines Integritätsverlusts die zugehörigen Daten bzw. Datensätze erneut übertragen werden.

### 3.1.3 Verfügbarkeit

Die Verfügbarkeit zu archivierender Daten hängt von der Verfügbarkeit des Vorgangsbearbeitungssystems ab. D.h., Daten können für die Dauer der Nichtverfügbarkeit eines Vorgangsbearbeitungssystems nicht archiviert werden.

Auf die langfristige Lesbarkeit<sup>5</sup> von archivierten Daten ist bereits bei ihrer Erzeugung Rücksicht zu nehmen, da jede Änderung der Daten dazu führen würde, dass die Signaturen nicht mehr gültig sind. Es dürfen daher nur langfristig stabile Nutzdatenformate verwendet werden, von denen auch nach 30 oder mehr Jahren davon auszugehen ist, dass ihre Lesbarkeit gewährleistet ist. Darüber hinaus muss auch die eindeutige Anzeige der Daten (Präsentation) gewährleistet werden.<sup>6</sup>

Es sind die Nutzdatenformate zu bevorzugen, die durch geprüfte und bestätigte Signaturanwendungskomponenten gemäß SigG ([SigG]) eindeutig angezeigt werden können. Zurzeit sind Signaturanwendungskomponenten verfügbar, die Nutzdatenformate wie TIFF, TXT und Bitmap (16 Graustufen) eindeutig anzeigen. Adobe hat beim Bundesamt für

<sup>5</sup> Ein Aspekt der Verfügbarkeit

<sup>6</sup> Siehe ArchiSig-Anforderung A1 (vgl. [ArchiSig2002], Seite 84)

Sicherheit in der Informationstechnik die Bestätigung für den Acrobat Reader 7 beantragt. Sobald die Bestätigung vorliegt, gehört PDF damit zu den zu bevorzugenden Nutzdatenformaten.

Sofern Daten nicht bereits bei der Erzeugung in einem geeigneten Format vorliegen, sollten sie vor der Signierung in ein geeignetes Format konvertiert werden oder nach einer Konvertierung zur erneuten Signatur vorgelegt werden.<sup>7</sup> Dies sollte allerdings die Ausnahme bleiben, da jede Konvertierung mit einem erhöhten Aufwand verbunden ist. Deshalb sollte darauf geachtet werden, dass zu archivierende Daten, die innerhalb der Organisation erzeugt werden, bereits in einem geeigneten Nutzdatenformat vorliegen. Eine Organisation sollte Dritten mitteilen, welche Nutzdatenformate von ihr akzeptiert werden. Sie kann z.B. auch durch Verwendung der Basiskomponente Formularserver erreichen, dass Nutzdaten in einem geeigneten Format eingehen.

### **3.1.4 Vertraulichkeit (Schutz von Geheimnissen)**

Die Vertraulichkeit zu archivierender Daten ist bereits im Vorgangsbearbeitungssystem über eine technische Maßnahme zu gewährleisten (vgl. Abschnitt 1.4), sofern dies aufgrund von Vorgaben des Datenschutzes und/oder behördeninternen Vorgaben erforderlich ist. Eine solche Maßnahme ist auf hohem Sicherheitsniveau durchzusetzen. Da aber auch in diesem Fall nicht ausgeschlossen werden kann, dass Daten mit einem entsprechenden Schutzbedarf unverschlüsselt im Vorgangsbearbeitungssystem gespeichert sind (Sachbearbeiter hat vergessen zu verschlüsseln!), müssen sie i.d.R. jedenfalls für die Dauer des Transports zwischen dem Vorgangsbearbeitungssystem und dem Archivierungssystem verschlüsselt werden. Eine Verschlüsselung hat jedenfalls dann zu erfolgen, wenn der Transport über öffentliche Netzwerke erfolgt.

## **3.2 Archivierte Daten**

### **3.2.1 Signaturneuerung (Beweiskraft)**

---

<sup>7</sup> Siehe ArchiSig-Anforderung A2 (vgl. [ArchiSig2002], Seite 84)

**Anforderung:**

Ein Archivierungssystem muss die Beweiskraft qualifizierter elektronischer Signaturen langfristig sichern.

Die Eignung von Kryptoalgorithmen zur Erzeugung qualifizierter elektronischer Signaturen ist zeitlich begrenzt. Endet das Zeitintervall für die Eignung von Kryptoalgorithmen, verliert ein Dokument, dessen qualifizierte elektronische Signatur mit einem solchen Kryptoalgorithmus erzeugt wurde, die angestrebte hohe Beweiskraft. Vor Ablauf der Sicherheitseignung der bei elektronischen Signaturen verwendeten Signatur- oder Hash-Algorithmen müssen die signierten Datensätze rechtzeitig erneut signiert werden (Signaturerneuerung).<sup>8</sup> Die erneute Signatur hat dabei mit zum Zeitpunkt der Erneuerung geeigneten Algorithmen zu erfolgen.

Das Archivierungssystem hat auf Anforderung – durch eine berechtigte Rolle oder automatisch – eine Signaturerneuerung für die von einem Verlust der Sicherheitseignung der Algorithmen betroffenen Daten durchzuführen. Das Verfahren sollte vorzugsweise automatisiert ablaufen. Um die Signaturerneuerung automatisch initiieren zu können, sollte im Archivierungssystem regelmäßig eine Aktualisierung der als geeignet eingestuften Kryptoalgorithmen erfolgen, die durch die BNetzA veröffentlicht werden.<sup>9</sup>

Da die erneute qualifizierte elektronische Signatur keine Willenserklärung darstellt, sondern ein Sicherungsmittel ist, ist keine persönliche Signatur, z. B. die eines Archivars, erforderlich. Stattdessen genügt auch ein qualifizierter Zeitstempel. Darüber hinaus kann von den in Abschnitt 5.2 der „Verwaltungsrechtlichen Rahmenbedingungen“ [VerwR2005] beschriebenen Vereinfachungen Gebrauch gemacht werden.<sup>10</sup>

Alle Vorgänge im Zusammenhang mit der Signaturerneuerung sollten protokolliert werden.<sup>11</sup>

<sup>8</sup> Siehe ArchiSig-Anforderung A33 (vgl. [ArchiSig2002], Seite 89)

<sup>9</sup> Siehe ArchiSig-Anforderung A34 (vgl. [ArchiSig2002], Seite 89)

<sup>10</sup> Siehe ArchiSig-Anforderung A35 (vgl. [ArchiSig2002], Seite 89)

<sup>11</sup> Siehe ArchiSig-Anforderung A36 (vgl. [ArchiSig2002], Seite 90)

Es sollte konfigurierbar sein, nach welcher Strategie Daten für eine gemeinsame Zeitstempelung (Archivzeitstempel) zusammengefasst werden, um verschiedenen Anforderungen der Verwaltung genügen zu können.<sup>12</sup> Sofern sich ein Archivzeitstempel auf mehrere Daten bezieht, müssen aus Datenschutzgründen einzelne Daten gelöscht werden können, ohne die Beweiskraft der Signatur des Archivzeitstempels zu gefährden.<sup>13</sup>

Für den Fall, dass Algorithmen ihre Eignung verloren haben, ohne dass die BNetzA zuvor darauf hingewiesen hätte (nachträglich erkannte Sicherheitslücken), sollte die Signaturerneuerung vorsorglich durch parallele Verwendung mehrerer Hash- und Signatur-Algorithmen erfolgen.<sup>14</sup>

Die erneute elektronische Signatur muss mindestens die gleiche Signaturstufe aufweisen wie die Ausgangssignatur, um deren ursprüngliche Qualität zu erhalten. Für die Signaturerneuerung qualifizierter elektronischer Signaturen mit Anbieter-Akkreditierung muss der Zertifizierungsdiensteanbieter, der den qualifizierten Zeitstempel zur Signaturerneuerung erzeugt, deshalb akkreditiert sein. Für die Signaturerneuerung sollte einheitlich immer die höchste Signaturstufe verwendet werden.<sup>15</sup>

Falls das Archivsystem bei der automatisierten Signaturerneuerung einen Fehler erkennt, ist ein Archivadministrator zu informieren, der geeignete Maßnahmen ergreift.<sup>16</sup>

Die erneute Signatur, die alle früheren Signaturen einschließen muss, ist so zu speichern, dass eine fehlerfreie Zuordnung zu Daten und Signaturen gewährleistet ist.<sup>17</sup>

### 3.2.2 Authentizität

Die Authentizität der archivierten Daten wird durch die Signaturerneuerung gewährleistet.

---

<sup>12</sup> Siehe ArchiSig-Anforderung A37 (vgl. [ArchiSig2002], Seite 90)

<sup>13</sup> Siehe ArchiSig-Anforderung A38 (vgl. [ArchiSig2002], Seite 90)

<sup>14</sup> Siehe ArchiSig-Anforderung A39 (vgl. [ArchiSig2002], Seite 90)

<sup>15</sup> Siehe ArchiSig-Anforderung A40 (vgl. [ArchiSig2002], Seite 90)

<sup>16</sup> Siehe ArchiSig-Anforderung A41 (vgl. [ArchiSig2002], Seite 90)

<sup>17</sup> Siehe ArchiSig-Anforderung A42 (vgl. [ArchiSig2002], Seite 90)

### 3.2.3 Integrität

Es bestehen keine zusätzlichen Anforderungen.

### 3.2.4 Verfügbarkeit

Bitfehler führen dazu, dass signierte Daten nicht mehr verifiziert werden können. Es sind daher eine mehrfach redundante Speicherung oder fehlerkorrigierende Codes vorzusehen.<sup>18</sup>

### 3.2.5 Vertraulichkeit (Schutz von Geheimnissen)

Die Vertraulichkeit archivierter Daten kann durch technische und/oder organisatorische Maßnahmen sichergestellt werden. Diese Maßnahmen sollen verhindern, dass Nichtberechtigte Zugang zu und Zugriff auf Daten erhalten können. Als technische Maßnahme zum Schutz der Vertraulichkeit dient die Verschlüsselung der archivierten Daten (vgl. Abschnitt 3.1.4).

Sofern eine Verschlüsselung der Daten nicht zwingend durch Gesetze oder Verfahrensanweisungen gefordert wird, kann ein angemessener Schutz auch durch organisatorische Maßnahmen sichergestellt werden. Als organisatorische Maßnahmen sind die Zutritts-, die Zugangs- und die Zugriffskontrolle zu nennen.

Eine Zutrittskontrolle verwehrt Unbefugten den Zutritt zum Archiv. Eine Zutrittskontrolle kann z.B. durch Schlüsselausgabe oder eine kartenbasierte Zutrittskontrollanlage umgesetzt werden. Eine Zugangskontrolle verhindert, dass Unbefugte das Archiv nutzen. Eine Zugangskontrolle kann durch Benutzername/Passwort oder chipkartenbasiert mit Unterstützung des Betriebssystems oder der entsprechenden Fachanwendung umgesetzt werden. Eine Zugriffskontrolle gewährleistet, dass Berechtigte ausschließlich auf Grundlage der ihrer Zugriffsberechtigung unterliegenden Daten auf Archivdaten zugreifen können. Eine entsprechende Zugriffskontrollpolitik ist zu etablieren. Die Zugriffskontrollpolitik erfordert die

---

<sup>18</sup> Siehe ArchiSig-Anforderung A30 (vgl. [ArchiSig2002], Seite 89)

Definition von Rollen (Sachbearbeiter, Revision,...) und den zugehörigen Zugriffsrechten (lesen, archivieren, löschen, ändern,...).

### 3.2.6 Umfang der Archivierung

**Anforderung:**

Das Archivierungssystem muss sicherstellen, dass die verwendeten Datenformate zur Langzeitarchivierung elektronisch signierter Dokumente geeignet sind.

Das für die Archivierung verwendete Datenformat muss gewährleisten, dass in den zu archivierenden Daten folgende Informationen enthalten sind oder dort abgelegt werden können:<sup>19</sup>

- Dokument (das signierte Dokument)
- Elektronische Signatur
- X.509 Zertifikate des oder (bei Mehrfachsignaturen) der Erzeuger der Signaturen und der Dienste (Zeitstempel, OCSP), oder eine Referenz auf diese, falls die Zertifikate an anderer Stelle archiviert werden
- Ausstellerzertifikate für o.g. Zertifikate (Zertifikatskette), oder Referenz auf diese, falls die Zertifikate an anderer Stelle archiviert werden
- Attributzertifikate, oder Referenz auf diese, falls die Zertifikate an anderer Stelle archiviert werden
- Zertifikatsstatus zum Zeitpunkt der Erzeugung (Annahme) der Signatur (OCSP Information)<sup>20</sup>
- Qualifizierte und/oder akkreditierte Zeitstempel.

### 3.2.7 Zeitpunkt der Archivierung

Der in Abschnitt 3.2.1 dargelegte Fall des Ablaufs der Sicherheitseignung der verwendeten Algorithmen kann bereits dann auftreten, wenn sich die Dokumente noch im

<sup>19</sup> Siehe ArchiSig-Anforderung A13 (vgl. [ArchiSig2002], Seite 86) und ArchiSig-Anforderung A22 (vgl. [ArchiSig2002], Seite 87)

<sup>20</sup> Zertifikatsstatus muss bei Annahme über OCSP ermittelt werden

Vorgangsbearbeitungssystem befinden. In diesem Fall müssten die Dokumente bereits im Vorgangsbearbeitungssystem erneut signiert werden. Um eine Signaturerneuerung im Vorgangsbearbeitungssystem zu vermeiden wird folgende Anforderung erhoben.

**Anforderung:**

Von archivierungsbedürftigen Daten, die einem Vorgangsbearbeitungssystem zugeführt werden, muss eine weitere Instanz<sup>21</sup> erzeugt und diese – ggf. mit einem akkreditierten Zeitstempel versehen – an das Archivsystem übertragen werden.

Es obliegt dem zuständigen Mitarbeiter, zu prüfen, ob die eingehenden Daten signiert sein müssen oder nicht, d.h. nur in signierter Form als Eingang gewertet werden können. Nach erfolgreicher Prüfung der qualifizierten elektronischen Signatur sind die Daten zu archivieren. Zum Umfang der Archivierung vgl. Abschnitt 3.2.6. Durch den akkreditierten Zeitstempel kann der Zeitpunkt dokumentiert werden, zu dem die Daten zur Prüfung vorgelegen haben. Wird ein Dokument später zu Beweis Zwecken benötigt, so ist die Instanz, die im Archivierungssystem abgelegt ist, als Beweismittel heranzuziehen.

Bei qualifiziert elektronisch signierten Daten, die einem Dienstenutzer (z.B. Behörde) bereits qualifiziert zeitgestempelt vorgelegt werden (z.B. per E-Mail, OSCI, ...), kann die Gültigkeit der qualifizierten elektronischen Signatur anhand des im qualifizierten Zeitstempel enthaltenen Zeitpunkts geprüft werden. Dieser Zeitpunkt ist der vermutete Signaturzeitpunkt. Ist das Zertifikat des Signaturschlüsselinhabers zum Zeitpunkt der Prüfung im zuständigen Verzeichnis vorhanden und nicht gesperrt, kann der Signaturschlüsselinhaber später (z.B. vor Gericht) nicht glaubhaft behaupten, die vorliegende qualifizierte elektronische Signatur nicht erzeugt zu haben. Der qualifizierte Zeitstempel gewährleistet demnach die Nichtabstreitbarkeit.

Anders verhält es sich, wenn qualifiziert elektronisch signierte Daten ohne qualifizierten Zeitstempel geprüft werden. Der vermutete Signaturzeitpunkt ist, falls kein anderer Zeitpunkt zuverlässig bestimmbar ist, der aktuelle Prüfzeitpunkt. Werden nun die qualifiziert

---

<sup>21</sup> Die Bezeichnung Instanz wird bewusst gewählt, da bei elektronischen Daten im Gegensatz zu papiergebundenen Dokumenten die eine Unterscheidung von „Original“ und „Kopie“ nicht möglich ist.

elektronisch signierten Daten zunächst ohne Zeitstempel im Archiv abgelegt und lässt der Signaturschlüsselinhaber nach der Signaturprüfung sein Signaturschlüsselzertifikat sperren, bevor ein Archivzeitstempel gebildet wurde, so kann er später (z.B. nach einem Jahr vor Gericht) behaupten, die Signatur nicht erzeugt zu haben. Entscheidend ist, dass in diesem Fall nicht eindeutig bestimmt werden kann, dass sich die Prüfung auf einen Zeitpunkt zu beziehen hat, zu dem Signaturschlüsselzertifikat noch gültig war. (Nicht eindeutiger Prüfzeitpunkt). Der Signaturschlüsselinhaber kann z.B. behaupten, dass die Signatur erzeugt wurde, nachdem er sein Zertifikat hat sperren lassen. Widerlegt werden kann ihm dies ohne qualifizierten Zeitstempel i.d.R. nicht!

Aus diesen Überlegungen kann sich die o.g. Anforderung ergeben, zeitlich vor einem Archivzeitstempel einen weiteren akkreditierten Zeitstempel einzuholen. Dabei ist zu beachten: Je mehr Zeit zwischen der Prüfung einer qualifizierten elektronischen Signatur und der Anforderung eines Archivzeitstempels verstreicht, desto wahrscheinlicher ist der Erfolg des o.g. Angriffs.

### **3.2.8 Löschen von übertragenen Dokumenten im Vorgangsbearbeitungssystem**

Anforderung:

Zwischen einem Archivierungssystem und einem Vorgangsbearbeitungssystem muss ein Quittungs-Mechanismus etabliert sein.

In diesem Dokument werden zwei Möglichkeiten der Archivierung unterschieden, die ein Archivierungssystem bzw. Vorgangsbearbeitungssystem unterstützen sollte: Die erste Möglichkeit besteht darin, Daten zu archivieren, aber weiterhin auch im aktiven Bestand des Vorgangsbearbeitungssystems zu halten. Die zweite Möglichkeit besteht darin Daten zu archivieren und diese anschließend aus dem aktiven Bestand des Vorgangsbearbeitungssystems zu löschen. Für beide Möglichkeiten ist es erforderlich, dass ein Archivierungssystem dem übertragenden Vorgangsbearbeitungssystem den erfolgreichen Datenimport quittiert. Ein Vorgangsbearbeitungssystem darf erst nach Erhalt dieser Quittung die Daten löschen. Ein entsprechender Quittungs-Mechanismus muss etabliert werden.

### **3.2.9 Dauer der Archivierung**

Die Dauer der Archivierung ergibt sich aus gesetzlichen Anforderungen. Für diese Dauer müssen Verifikationsdaten in beweiskräftiger Form beschaffbar sein oder vorab beschafft und archiviert werden.<sup>22</sup>

### **3.2.10 Löschen von Daten im Archivierungssystem**

Die Notwendigkeit des Löschens von archivierten Daten kann sich bei Zweckerreichung bzw. auf Anforderung eines Betroffenen aus Datenschutzgründen ergeben.<sup>23</sup> Daten im Archivierungssystem müssen daher jederzeit gelöscht werden können.

Das Löschen von Daten im Archivsystem muss protokolliert werden können.<sup>24</sup>

### **3.2.11 Abfrage von archivierten Dokumenten im Archivierungssystem**

Es muss sichergestellt werden, dass nur autorisierte Benutzer einen Dokumentenabruf durchführen können. Die Abfrage von archivierten Dokumenten im Archivierungssystem kann z.B. durch eine Zugangs- und Zugriffskontrolle gesichert werden (vgl. Abschnitt 3.2.5).

Der Dokumentabruf muss jederzeit möglich sein, wobei die Dokumente in verkehrsfähiger Form mit allen notwendigen Verifikationsdaten ausgeliefert werden können.<sup>25</sup>

### **3.2.12 Technisch-Organisatorische Anforderungen**

Das Archivsystem muss über eine geeignete Managementkomponente verfügen, die der Steuerung und Überwachung der Signaturneuerung dient.<sup>26</sup>

---

<sup>22</sup> Siehe ArchiSig-Anforderung A22 (vgl. [ArchiSig2002], Seite 87)

<sup>23</sup> Anforderungen hinsichtlich des Löschens von archivierten Daten sind in [Roß2004], Abschnitt 4.3, beschrieben

<sup>24</sup> Siehe ArchiSig-Anforderung A32 (vgl. [ArchiSig2002], Seite 89)

<sup>25</sup> Siehe ArchiSig-Anforderungen A48 und A49 (vgl. [ArchiSig2002], Seite 92)

<sup>26</sup> Siehe ArchiSig-Anforderung A28 (vgl. [ArchiSig2002], Seite 88)

Das Archivsystem muss für alle verwendeten Signatur- und Datenformate, eine geeignete Signaturanwendungskomponente verfügbar halten, die bei Bedarf auch Dritten zur Verfügung gestellt werden kann.<sup>27</sup>

### 3.3 Signaturerzeugung

Innerhalb einer Organisation sind zur Signaturerzeugung sichere Signaturerstellungseinheiten und geeignete Signaturanwendungskomponenten zu verwenden, die die Anforderungen des Signaturgesetzes sowie der Signaturverordnung erfüllen.<sup>28</sup> Auch bei eingehenden Daten sollte dies gefordert werden. Es wird aber i.d.R. nicht möglich sein, zu prüfen, ob dieser Forderung tatsächlich nachgekommen wurde. Da die Gültigkeit der Signatur nicht davon abhängig ist, dass sie mit einer geeigneten Signaturanwendungskomponente erstellt wurde, kann auf eine solche Prüfung verzichtet werden.

Es sollten ausschließlich langfristig stabile Signaturdatenformate verwendet werden.<sup>29</sup>

Innerhalb einer Organisation sollten ausschließlich akkreditierte Signaturen<sup>30</sup> verwendet werden.<sup>31</sup>

Der Nachweis eines möglichst authentischen Signaturzeitpunktes kann von der Organisation durch zeitnahe Einholung eines akkreditierten Zeitstempels<sup>32</sup> gewährleistet werden (vgl. dazu auch Abschnitt 3.2.7).<sup>33</sup>

---

<sup>27</sup> Siehe ArchiSig-Anforderung A29 (vgl. [ArchiSig2002], Seite 88) und ArchiSig-Anforderung A50 (vgl. [ArchiSig2002], Seite 92)

<sup>28</sup> Siehe ArchiSig-Anforderung A3 (vgl. [ArchiSig2002], Seite 84)

<sup>29</sup> Siehe ArchiSig-Anforderung A4 (vgl. [ArchiSig2002], Seite 84)

<sup>30</sup> Eine akkreditierte Signatur ist eine qualifizierte elektronische Signatur mit Anbieterakkreditierung (vgl. §15 SigG).

<sup>31</sup> Siehe ArchiSig-Anforderung A5 (vgl. [ArchiSig2002], Seite 85)

<sup>32</sup> Ein akkreditierter Zeitstempel ist ein qualifizierter Zeitstempel mit Anbieterakkreditierung.

<sup>33</sup> Siehe ArchiSig-Anforderung A6 (vgl. [ArchiSig2002], Seite 85)

### 3.4 Signaturverifikation

Für eingehende Dokumente ist zu prüfen, ob sie elektronisch signiert sein müssen. Falls ja, ist zu prüfen, ob die Signatur die erforderliche Qualität (qualifiziert bzw. qualifiziert mit Anbieterakkreditierung) aufweist. Außerdem ist eine umfassende und vollständige Gültigkeitsprüfung durchzuführen.<sup>34</sup>

Gemäß ISIS-MTT muss eine Prüfung der Zertifikatskette nach dem Schalenmodell und, falls diese nicht erfolgreich ist, nach dem Kettenmodell erfolgen. Allgemein sollten auch alternative Gültigkeitsprüfungen durchgeführt werden können.<sup>35</sup>

Bei der Verifikation sollte der Signaturzeitpunkt vorgegeben werden können (z.B. Zeitangabe aus Zeitstempel oder andere authentische Zeitangaben).<sup>36</sup>

Die Verifikation muss automatisch erfolgen. Dies gilt auch für Zeitstempelfolgen im Archiv. Die Ergebnisse der Verifikation müssen den Nutzer in übersichtlicher Form angezeigt und bei Bedarf jederzeit zur Verfügung gestellt werden können.<sup>37</sup>

Eine Organisation sollte sich auf Nutzdatenformate beschränken, welche durch eine evaluierte und bestätigte Signaturanwendungskomponente eindeutig angezeigt werden können und bei denen die für die Präsentation erforderlichen Daten (z.B. Zeichensätze) im Dokument verankert sind.<sup>38</sup> Es sollte gefordert werden, dass alle signierten Daten, die intern erzeugt werden oder eingehen diesem Nutzdatenformat entsprechen<sup>39</sup>.

Für das Archiv muss ein sicherer Speicher der Wurzelzertifikate vorgesehen werden, der zentral administrierbar ist.<sup>40</sup>

---

<sup>34</sup> Siehe ArchiSig-Anforderung A10 (vgl. [ArchiSig2002], Seite 86)

<sup>35</sup> Siehe ArchiSig-Anforderung A11 (vgl. [ArchiSig2002], Seite 86)

<sup>36</sup> Siehe ArchiSig-Anforderung A12 (vgl. [ArchiSig2002], Seite 86)

<sup>37</sup> Siehe ArchiSig-Anforderungen A14 und A15 (vgl. [ArchiSig2002], Seite 86) und ArchiSig-Anforderung A19 (vgl. [ArchiSig2002], Seite 87)

<sup>38</sup> Siehe ArchiSig-Anforderung A17 (vgl. [ArchiSig2002], Seite 87)

<sup>39</sup> Die Einschränkung auf bestimmte Nutzdatenformate ist gängige Praxis. Vgl. dazu z.B. [http://www.regtp.de/reg\\_tele/start/fs\\_05.html](http://www.regtp.de/reg_tele/start/fs_05.html).

<sup>40</sup> Siehe ArchiSig-Anforderung A18 (vgl. [ArchiSig2002], Seite 87)

Im Falle einer automatisierten Signaturverifikation vor dem Speichern im Archiv sind folgende Fehlerfälle zu berücksichtigen:<sup>41</sup>

- Für die Langzeitspeicherung ungeeignete Nutzdatenformate
- Ungeeignete Signaturdatenformate
- Verifikation nicht erfolgreich
- Verifikationsdaten nicht vorhanden

---

<sup>41</sup> Siehe ArchiSig-Anforderung A27 (vgl. [ArchiSig2002], Seite 88)

## 4 Literatur

- [ArchiSig2002] ArchiSig: Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente, Anforderungskatalog, Version 2.0, Dezember 2002.
- [BDSG2003] Bundesdatenschutzgesetz in der Fassung der Neubekanntmachung vom 14. Januar 2003.
- [OrgKonz20] Erweiterungsmodul zum Organisationskonzept 2.0, Technische Aspekte der Archivierung elektronischer Akten, Oktober 2004.
- [Roß2004] Signaturgesetzkonformität des Standardisierungsvorschlags „Long-Term Conservation of Electronic Signatures“ für die ISIS-MTT Spezifikation vom 30.6.2004, Prof. Dr. Alexander Rossnagel.
- [SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG), Bundesgesetzblatt Jahrgang 2001 Teil I Nr. 22, ausgegeben zu Bonn am 21. Mai 2001  
in der Fassung des 1. Gesetzes zur Änderung des Signaturgesetzes vom 04. Januar 2005, Bundesgesetzblatt Jahrgang 2005 Teil I Nr. 1, ausgegeben zu Bonn am 10. Januar 2005
- [VerwR2005] ArchiSafe: Verwaltungsrechtliche Rahmenbedingungen