

Technische Richtlinie für das ersetzende Scannen – Status und Ausblick

Dr. Astrid Schumacher
(Bundesamt für Sicherheit in der Informationstechnik)


Dr. Detlef Hühnlein (ecsec GmbH)

20. EDV-Gerichtstag 23.09.2011 Saarbrücken

Ausgangslage 1



Im **E-Government** und **elektronischen Rechtsverkehr** mehren sich Rechtsvorschriften, die die **elektronische Aktenführung** zulassen oder vorschreiben

Fortschreitende Digitalisierung der Verwaltungsvorgänge und zunehmender Einsatz von **eVorgangsbearbeitungssystemen**, gleichzeitig mittel- bis langfristig weiterhin **Papierdokumente** 



(Gesetzliche) **Dokumentations- und Aufbewahrungsvorschriften** verpflichten in vielen Fällen weiterhin zur Aufbewahrung des Originals



Verminderter Beweiswert bei Vernichtung des Originals berührt die Interessen der Beteiligten und führt zu Unsicherheit beim Anwender

Ausgangslage 2

- **Verwaltungsbereich:** eAkte idR nur Zweitakte („Duploakte“)
 - Besonderheit in der öff. Verwaltung: **Aktenführungspflicht** erfordert obj. Dokumentation; eAkte muss dem **Stand der Technik** genügen
- Hohe finanzielle & organisatorische **Belastung**
- Ersetzendes Scannen nur bei **ausdrücklicher gesetzlicher Ermächtigung** zulässig
- Bei den real existierenden **Erlaubnisnormen für das ersetzende Scannen**
 - fehlt es normativ an einer Konkretisierung der Anforderungen an das ersetzende Scannen
 - besteht daher Unsicherheit beim Anwender, der allg. formulierte Anforderungen in geeignete techn.org. Maßnahmen umsetzen muss
 - die Risiken bei der Nichterfüllung der Anforderungen variieren, umfassen aber stets eine Verringerung der Beweissicherheit



3

Zwei Beispiele aus dem wahren Leben







- **EAPatV: § 3 Vernichtung von Schriftstücken:**
„Werden Schriftstücke oder sonstige Unterlagen in ein elektronisches Dokument übertragen, **so dürfen sie nicht vernichtet werden, wenn in Betracht kommt, über ihr Vorhandensein oder ihre Beschaffenheit Beweis zu erheben.**“
- **OWiG: § 110b Abs. 4:**
„Enthält das nach Absatz 2 hergestellte elektronische Dokument zusätzlich zu dem Vermerk nach Absatz 2 Satz 2 einen **mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen Vermerk darüber,**
 1. dass die Wiedergabe auf dem Bildschirm mit der Urschrift **inhaltlich und bildlich übereinstimmt** sowie
 2. ob die **Urschrift** bei der Übertragung als Original oder in Abschrift vorgelegen hat, **kann die Urschrift bereits vor Abschluss des Verfahrens vernichtet werden.** **Dies gilt nicht für** in Verwahrung zu nehmende oder in anderer Weise sicherzustellende **Urschriften, die als Beweismittel von Bedeutung sind** oder der Einziehung oder dem Verfall unterliegen (§§ 22 bis 29a, 46 dieses Gesetzes in Verbindung mit §§ 94, 111b bis 111n der Strafprozessordnung).“

4

Verbesserungspotenzial

- Lösungen, die eine **Vernichtung des Originals unter maximal erreichbarer Wahrung der Rechts- und Beweissicherheit** ermöglichen

- **Vereinheitlichung** der heterogenen Prüf-Landschaft, u.a.:
 - DOMEA 
 - GoBS 
 - GDPdU 
 - IDW-FAIT 
 - TÜV-IT-Zertifizierung nach PK-DML (VOI)



5

Zukunftsorientierung - Die dritte Dimension

Synergie von Technik



und Recht

Technik

- Scanlösungen marktgängig, aber „Wildwuchs“
- Unsichere Entscheidungsgrundlage für Anwender
- Sicherheitsvorgaben zur Gewährleistung der wesentlichen Ziele der Informationssicherheit Integrität, Vertraulichkeit und Verfügbarkeit fehlen

Recht

- (Zu) weiter Auslegungsspielraum für technische Ausgestaltung
- Gesetzgebung uneinheitlich, verschiedene Ebenen und Vorgaben
- Zögerlichkeit hins. zukunftsorientierter Regelungen für eAkten

→ **Empfehlungen des BSI als Vertrauensanker**



6

Projektziele

→ Erhöhung von **Informationssicherheit & Rechtssicherheit** bei der eAkte, sowie darüber hinaus auch in der Wirtschaft; **Bürokratieabbau**

□ Technisch

- **Konformitätsbewertung** iRd Zertifizierung
 - Obj. Beurteilung durch unabhängige Prüfkriterien
 - Standardisierte Vorgehensweise beim ersetzenden Scannen:
Erhöhung der **Produktsicherheit** → **Mindeststandard** (§ 8 BSIG)
- **Empfehlungen** für Ausschreibung und Beschaffung
- **Spezifikationen** für Produkte und Lösungen



□ Rechtlich

- **Referenzierung** in zukünftigen Rechtsvorschriften („Stand der Technik“), z.B. EGovG
- Erleichterung der Schaffung von **Zulässigkeitstatbeständen** („Vernichtung des Originals ist (nur) dann zulässig, wenn nach der TR xxxxx des BSI eingescannt wurde“)
- **Einheitliche Auslegung** bei bestehenden Regelwerken

7

Zu regelnde Aspekte (1) - Auswahl

- Organisation der **Prozesse** (mit Arbeitsanweisungen)
- Anforderungen an die **Einsatzumgebung**
- Vorgaben für die **einzusetzende Technik**
- Insbes.: **Klassifizierung von Dokumenten** nach Schutzbedarf, insbesondere Beweisrisiko
 - davon abhängig Sicherungsmittel wie z.B. Einzelsichtprüfung mit anschließender Signatur, Batchsignaturen
- Beachtung der relevanten Schnittstellen zu DMS/VBS
- Ablage in einer für die **LZA** geeigneten Weise (TR-ESOR)

8

Zu regelnde Aspekte (2) - Auswahl

- ❑ **Scan-Strategien**
 - ❑ Zeitpunkt und Ort des Scannens
 - ❑ Art und Weise des Scannens: online/Stapel
 - ❑ Indizierung der Dokumente
- ❑ **Scan-Prozess**
 - ❑ Sichtung Posteingang
 - ❑ Vorbereitung und Sortierung des Schriftguts
 - ❑ Automatische oder manuelle Erst-Indizierung
 - ❑ OCR/Barcode
- ❑ **Qualitätssicherung**
- ❑ **Technische Aspekte Scanner**
 - ❑ Schnittstellen
 - ❑ Scanner-Arten
 - ❑ Auflösung und Bildverbesserungsfunktionen
 - ❑ Kompression: TIFF, JPEG, PDF

9

Herausforderungen des Projekts

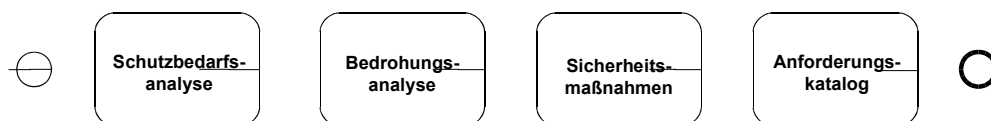
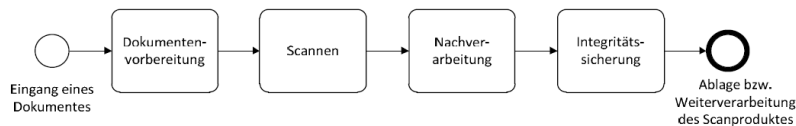


- ❑ **Technisch-organisatorische Komplexität**
 - **Signaturen:**
in welchen Prozessschritten für welche Arten von Dokumenten
 - Unterschiedliche Sicherheitsniveaus nach **Modulsystem** (Schutzbedarfsanalyse nach bereichsspezifischen Anforderungen, Bedrohungen und Angriffsrisiken sowie Gegenmaßnahmen)
 - **Prüfkriterien**
 - Ökonomische **Effizienz:** Kosten-Nutzen-Analyse
- ❑ **Aktives Adressieren aller Betroffener**
 - Projektbeirat
 - Öffentliche Kommentierung unter Einbeziehung von Österreich und der Schweiz

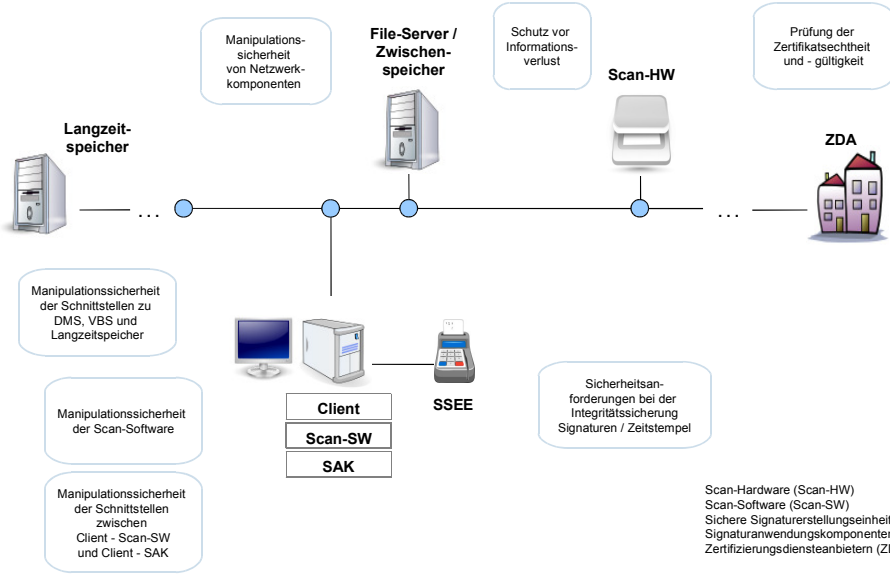


10

- Bedrohungs- und Risikoanalyse orientiert sich am „generischen Scanprozess“
- Abgrenzung der TR durch klar definierte Schnittstellen
- Zuständigkeit der TR beginnt beim Eingang des Dokuments und endet an der Schnittstelle zu einem DMS, VBS oder Langzeitspeicher (z.B. TR-ESOR)



Sicherheitsanforderungen für den Scanprozess



Entscheidungsmatrix (Entwurf)

Module / Schutzziele	Technische Module							Organisatorische Module	
	Sichere Netz-anbindung	Raum-zugangs-kontrolle	Signatur für ge-scann-ten Stapel	Signatur für einzelne Dokumente	Verfi-zierung durch Einzel-sicht-prüfung	Überein-stimm-ungs-vermerk „Beglau-bigung“	Langzeit-archivier-ungs-sicheres Speicher-format	Arbeits-anweisung	
Phase 1: Vorbereitung des Originaldokuments									
räumliche Sicherheit der Scanstelle		X						X	
Phase 2: Funktionalen Anforderungen an den technischen Scanvorgang selbst									
Schutz vor Datenverlust	X						X		
Phase 3: Gewährleistung der Echtheit des Scanprodukts									
Basis-Integritätsschutz	X		X						
Hoher Integritätsschutz	X			X	X		X		
Sehr hoher Integritätsschutz	X			X	X	X	X		



Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Dr. Astrid Schumacher
Leiterin des Referats B 25
Mindeststandards und Produktsicherheit

astrid.schumacher@bsi.bund.de

Tel. 0228-95825371