Bundesamt
für Sicherheit in der
Informationstechnik

Praxisgerechte Umsetzung der BSI TR-03138 (RESISCAN) für Kommunalverwaltungen

2. E-Government Konferenz Mecklenburg-Vorpommern

5. April 2017, Schwerin

Dr. Astrid Schumacher

Agenda

1. Einleitung
2. TR RESISCAN – BSI - Richtlinie 03138 zum ersetzenden Scannen
3. Praxisbeispiele erfolgreicher Anwendungen für Kommunen
4. Erteilte Zertifikate
5. Weitere Umsetzungsbeispiele und Ausblick

1. Einleitung

Digitale Verwaltung

Regierungsprogramm zur Verwaltungsmodernisierung der 18. LP: „*Digitale Verwaltung 2020*“

- ***Aktionsplan E-Akte*** zur Einführung der elektronischen Akte (organisatorische und fachliche Aspekte sowie technische Angebote)

- ***Gemeinsame IT des Bundes*** zur Umsetzung EGovG notwendige Basisdienste für alle Bundesressorts (IT-Rahmenkonzept des Bundes), inkl. De-Mail-Gateway und zentraler eID-Service

Bestandteil der **Digitalen Agenda** 2014-2017, Handlungsfeld „Innovativer Staat“

Elektronische Aktenführung - Digitalisierung

- **§§ 6 und 7 EGovG fordern die elektronische Aktenführung inkl. Scannen & Langzeitaufbewahrung nach dem „Stand der Technik“, Landesgesetze folgen**
- Beweisregelungen zugunsten nach Stand der Technik eingescannter Dokumente, z.B. §§ 371 b, 298a ZPO

→ ***Orientierungshilfen des BSI durch Technische Richtlinien***

Ausgangslage

Wesentliche Aspekte im Rahmen der TR:

- technisch-organisatorische Anforderungen an den Scanprozess und das Scanprodukt mit dem Ziel:

  → Erreichen eines **möglichst hohen, dem Original angenäherten Beweiswert des Scanproduktes** für ein Gerichtsverfahren durch standardisierte Vorgehensweise

- Zunehmender Bedarf an **verbindlicher** Digitalisierung von Verwaltungsprozessen mit dem Ziel der Effizienzsteigerung und des Bürokratieabbaus zur Umsetzung der rechtskonformen E-Akte

→ Lösungsansätze für das ordnungsgemäße ersetzende Scannen in Form von Empfehlungen

Gesetzliche Anforderungen

- **Weitgehende Einheitlichkeit hinsichtlich bestehender gesetzlicher Anforderungen an den Scanprozess und das Scanprodukt, z.B.:**

  - Bildliche und inhaltliche Übereinstimmung zwischen Papieroriginal und Scanprodukt
  - Übereinstimmungsnachweis
  - Schutz vor Informationsveränderungen und Informationsverlusten
  - Dauerhafte Datenträger

  - „*Stand der Technik*“

Aktuelle gesetzliche Referenzen

§ 7 EGovG: Übertragen und Vernichten des Papieroriginals:

Erlaubnis zum ersetzenden Scannen mit Verweis auf TR RESISCAN (in der Gesetzesbegründung) betr. Bundesbehörden

„*Die Behörden des Bundes sollen, soweit sie Akten elektronisch führen, an Stelle von Papierdokumenten deren elektronische Wiedergabe in der elektronischen Akte aufbewahren. Bei der Übertragung in elektronische Dokumente ist nach dem* ***Stand der Technik*** *sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.*“

„*Papierdokumente (...)* ***sollen*** *nach der Übertragung in elektronische Dokumente* ***vernichtet oder zurückgegeben*** *werden, sobald eine weitere Aufbewahrung nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvorgangs erforderlich ist.*“

- Länder-EGovernment-Gesetze folgen diesem Muster

Gesetzliche Referenzen

§ 298a ZPO: Elektronische Akte

(1) Die Prozessakten können elektronisch geführt werden. (...)

(2) *In Papierform eingereichte Schriftstücke und sonstige Unterlagen sollen* ***nach dem Stand der Technik*** *in ein elektronisches Dokument übertragen werden.* (...)

§ 371b ZPO: Beweiskraft gescannter öffentlicher Urkunden

„Wird eine öffentliche Urkunde nach dem ***Stand der Technik*** *von einer öffentlichen Behörde oder von einer mit öffentlichem Glauben versehenen Person in ein elektronisches Dokument übertragen und liegt die Bestätigung vor, dass das elektronische Dokument mit der Urschrift bildlich und inhaltlich übereinstimmt, finden auf das elektronische Dokument die* ***Vorschriften über die Beweiskraft öffentlicher Urkunden*** *entsprechende Anwendung.“*

Risikoanalyse hinsichtlich gerichtlicher Entscheidungen

- 2013 wurde eine ***Simulationsstudie*** durchgeführt, in der sachverständige Testpersonen (Anwälte, Richter, Gutachter) anhand nachgestellter Fälle (simulierte elektronische Akten im Rahmen simulierter Gerichtsprozesse) die **Beweisführung mit gescannten, transformierten, signierten und beglaubigten Dokumenten** erprobten. Die Arbeiten erfolgten an ihren Arbeitsplätzen unter wissenschaftlicher Beobachtung mittels Protokollen, Interviews, Beobachtung und Aktenauswertung.

- Wesentliches Ergebnis: die gescannten Dokumente werden grundsätzlich als Beweismittel akzeptiert. ***Das korrekte Scannen kann mittels Einhaltung der TR als Anforderungsprofil nachgewiesen werden. Die Zertifizierung verbessert die Beweissituation.*** Ein Zertifikat erspart eine umfangreiche Beweiserhebung.

→ Nachgewiesene Vorteile einer ***standardisierten Vorgehensweise*** für die Rechtssicherheit

2. TR RESISCAN – BSI - Richtlinie 03138 zum ersetzenden Scannen

Die Technische Richtlinie

- **Die BSI TR-03138 „Ersetzendes Scannen (RESISCAN)“ oder kurz TR RESISCAN – ist eine Technische Richtlinie des BSI, die Anwendern aus**
  Verwaltung, Justiz, Wirtschaft & Gesundheitswesen
  einen praxisorientierten **Handlungsleitfaden** zur sicheren Gestaltung ihrer Prozesse für das ersetzende Scannen bietet.

- Diese **Empfehlungen** erleichtern zudem Ausschreibungen und Beschaffungen.

→ Die TR zielt damit auf die Steigerung der Rechtssicherheit im Bereich des ersetzenden Scannens ab.

→ **ABER**: Die TR regelt nicht die Zulässigkeit oder die Rechtsverbindlichkeit des ersetzenden Scannens. Diese sind von jedem Anwender im jeweiligen Anwendungs- und Verantwortungsbereich, auf Grundlage der entsprechenden Rechtsvorschriften, zu prüfen.

Die Technische Richtlinie

- Die TR besteht aus dem ***Hauptdokument***, der Technischen *Richtlinie* 03138 und den ***Prüfspezifikationen*** für die Konformitätsprüfung (Anlage P)

- Darüber hinaus lediglich *informativ*:

  - Anlage A: Ergebnis der Risikoanalyse (Hintergrundinformation)
  - Anlage R: Rechtliche Erläuterungen zur Anwendung der TR
  - Anlage V: Exemplarische Verfahrensanweisung für Scanpersonal

Ziel

Die TR RESISCAN

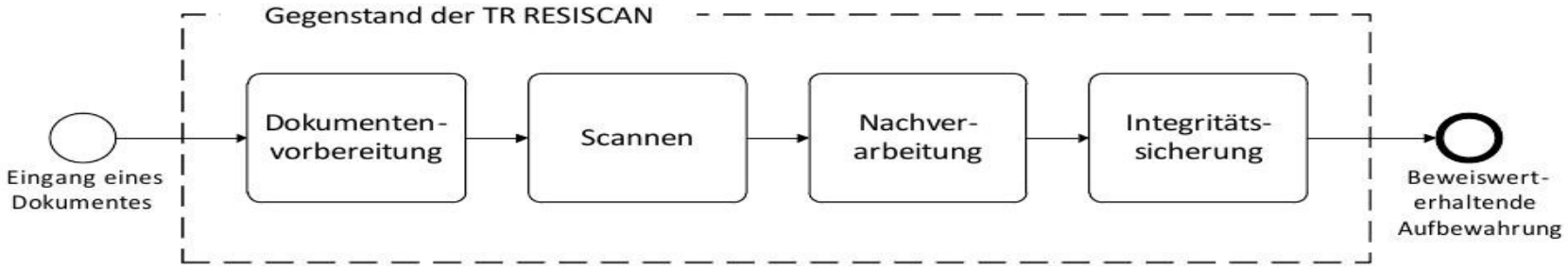
- soll als ***Handlungsleitfaden*** und ***Entscheidungshilfe*** dienen, wenn es darum geht, Papierdokumente nicht nur einzuscannen, sondern nach Erstellung des Scanproduktes auch zu vernichten;

- soll die ***sicherheitsrelevanten Maßnahmen*** benennen, die beim ersetzenden Scannen zu berücksichtigen sind.

→ Es sind ***technische, organisatorische und personelle Anforderungen*** für Scanprozesse und -produkte zu erfüllen, damit Papierdokumente möglichst rechtssicher und gerichtsverwertbar digitalisiert und anschließend vernichtet werden können.

Der „generische Scanprozess“

- Der generische Scanprozess umfasst:
  - die Dokumentenvorbereitung
  - das Scannen
  - die Nachbereitung und
  - die Integritätssicherung



- Die Prozessschritte jenseits der Integritätssicherung wie z.B. Sachbearbeitung, Zwischenspeicherung, Aufbewahrung, Archivierung sind nicht Gegenstand der TR.

- Abgrenzung der TR durch klar definierte Schnittstellen.

Methodik

1. **Strukturanalyse**

   Erfassen der zu betrachtenden Objekte wie IT-Systeme, Netze, Anwendungen & Datenobjekte (Schriftgut, Scanprodukte, Sicherungsdaten, Protokolle).

2. **Schutzbedarfsanalyse**

   Erstellen einer Schutzbedarfsanalyse für die konkret zu verarbeitenden Dokumente

   - die Ergebnisse der exemplarischen Schutzbedarfsanalysen können dabei der Orientierung dienen

   Der Schutzbedarf der weiteren Datenobjekte ergibt sich aus dem Schutzbedarf der Papieroriginale

   - daher ist es ausreichend den Schutzbedarf (hinsichtlich der Grundwerte Integrität, Vertraulichkeit und Verfügbarkeit) derselben zu bestimmen

Methodik

Bedrohungsanalyse + Risikoanalyse

Bei der Erstellung der TR wurde eine Bedrohungs- und Risikoanalyse durchgeführt - daher können Anwender der Richtlinie auf diese Schritte **verzichten**. Es ist ausreichend, die dem ermittelten Schutzbedarf entsprechenden Sicherheitsmaßnahmen aus dem modularen Maßnahmenkatalog umzusetzen.

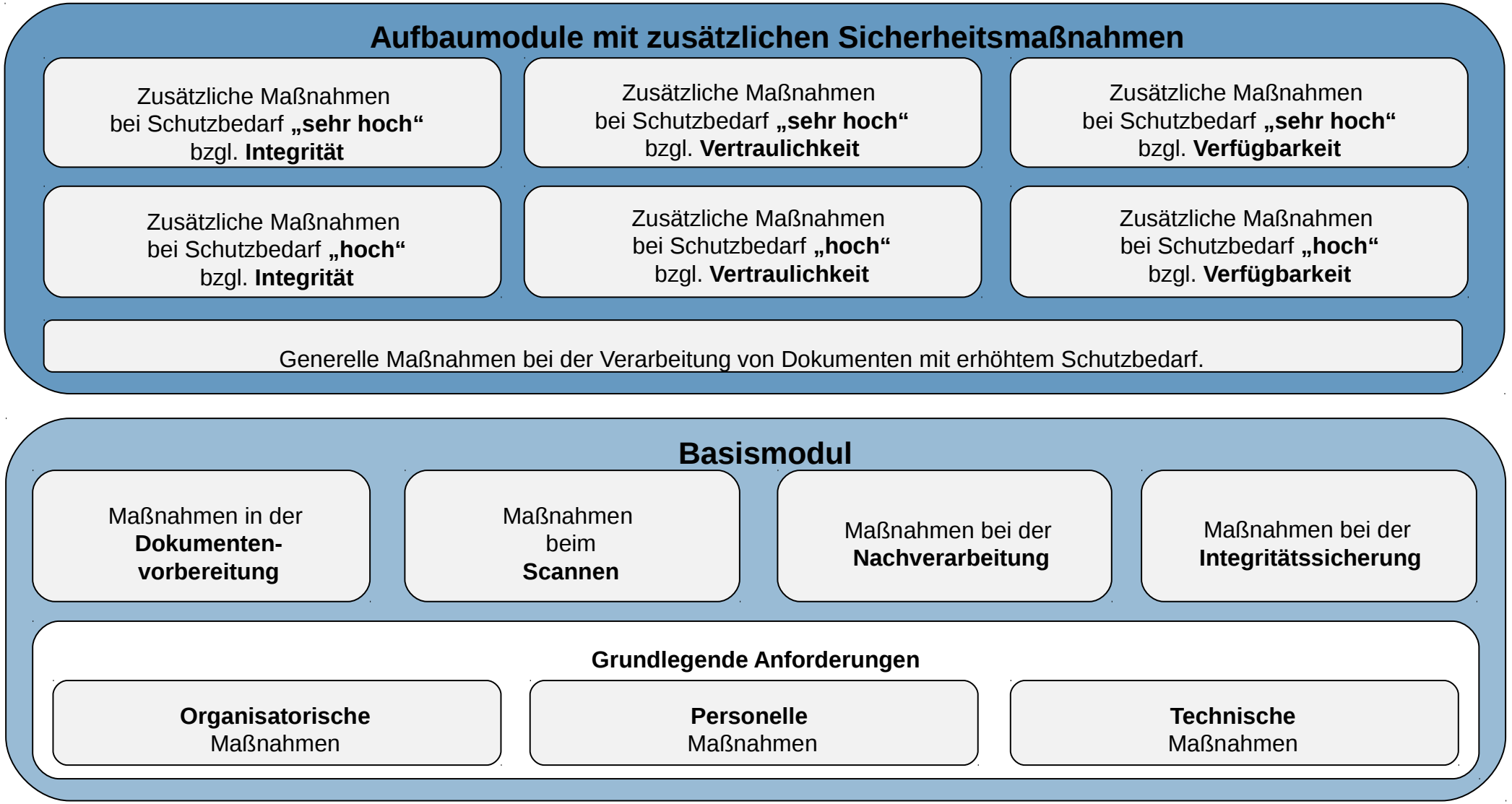
3. Sicherheitsmaßnahmen

Erfassen der zu betrachtenden Objekte wie IT-Systeme, Netze, Anwendungen & Datenobjekte (Schriftgut, Scanprodukte, Sicherungsdaten, Protokolle).

Spezifizierte Anforderungen

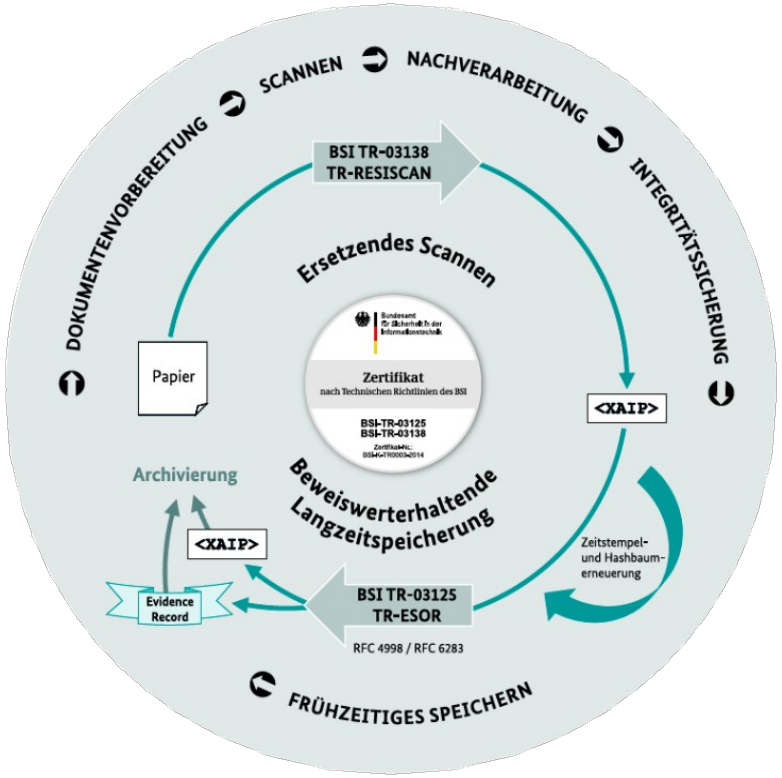
Modularer Anforderungskatalog /Maßnahmenkatalog

Modularer Maßnahmenkatalog



Einheitliches System der Digitalisierung und Beweiswerterhaltung

TR RESISCAN: Beweiserhaltende Digitalisierung mit dem Ziel der Vernichtung des Papieroriginals.



<XAIP>
XML-basiertes selbsttragendes Archivdatenobjekt inklusive Nutz- und Metadaten sowie beweiserhaltende Daten und Evidence Records.

TR ESOR: Beweiserhaltung kryptographisch gesicherter Dokumente und Daten.

Bundesamt
für Sicherheit in der
Informationstechnik

3. Praxisbeispiele erfolgreicher Anwendungen für Kommunen

Fragen aus der Praxis

Soll das Papierdokument (überhaupt) gescannt werden? (Beurteilung der **Sinnhaftigkeit**)				Aktenrelevanz?
Kann das Papierdokument **ersetzend** gescannt werden? (Beurteilung der **Zulässigkeit und Eignung**)				Gesetzliche Regelungen?
Welcher fachliche **Schutzbedarf** besteht? Gibt es gesetzliche oder sonstige Vorgaben?				Normal, hoch, sehr hoch?
Welche **fachliche Scanstrategie** ergibt sich aus Zulässigkeit, Eignung und Schutzbedarf?				
Ersetzend Scannen gem. definierter Standards	Ersetzend Scannen gem. definierter **höherer** Standards (technisch und/oder organisatorisch)	Kopierend scannen, Original gemäß der Aufbewahrungsfristen aufbewahren	Kopierend scannen und Rückgabe/Weiterleitung Original	Nicht scannen, Original gem. der Aufbewahrungsfristen aufbewahren
Wann und wo bzw. von wem soll gescannt werden? (Festlegung der **organisatorischen Scanstrategie**)				
Zeitpunkt/ Ort	**früh**	**parallel**	**spät**	
zentral	**x**			Zentrale Poststelle?
dezentral		**x**	**x**	Arbeitsplatz, Fachbereich?
Welche **flankierenden organisatorischen Maßnahmen** sind weiterhin notwendig?				Scannen beim externen Dienstleister?

(Quelle: KGSt/VITAKO)

Erfolgreiche jüngste Kooperation

Nationaler IT-Gipfel /Plattform 5/Digitale Verwaltung und Öffentliche IT → *UAG Rechtskonforme E-Akte* unter der Leitung des LR Amt Breisgau-Hochschwarzwald), April 2016

- Beteiligte: Vertreter des Bundes, der Justiz, kommunale Praktiker, öffentliche IT-Dienstleister, private Unternehmen

- Verweis auf Notwendigkeit praxisbezogener Regelungen

- Bildung von **2 Arbeitsgruppen** mit kommunalen Praktikern
  → Erarbeitung von Handlungsleitfäden auf Grundlage der TR RESISCAN
  1. Exemplarische Schutzbedarfsanalyse (KGSt)
  2. Musterverfahrensbeschreibung (VITAKO)

  → *Veröffentlichung 2. Q/2017*

KGSt-Analyse zum Schutzbedarf kommunaler Dokumente

- Gleicher Dokumentenbestand in allen Kommunen und gleiche Gesetze für alle.
- Schutzbedarf „normal“ ist der Regelfall.
- Beim Scanprozess sind die organisatorischen und technischen Anforderungen der Stufe „normal“ (Basismodul) i.d.R. ausreichend.
  Nur wenn aufgrund geltender Vorschriften ein erweiterter Schutz notwendig ist, werden besondere organisatorische und/oder technische Standards empfohlen.
- Die Einstufung Schutzbedarf „sehr hoch“ wurde in keinem Fall erreicht.

(Quelle: KGSt)

KGSt-Aktenplan mit Scanstrategie, Negativliste + Zweifelsfälle

		Schutzbedarf *					
Az.	**Dokumentenart**	Verfügbarkeit	Vertraulichkeit	Integrität	**Scan-Strategie**	**Grundlage der Ausnahme**	**Bemerkung**
11.20	**Personalmanagement**						
11.21	**Personalangelenheiten der Mitarbeiter**						
	Ärztliche Gutachten		x		Ersetzend scannen mit erhöhtem organisatorischen Standard	Datenschutz	z.B. Dezentral scannen oder scannen nur durch ausgewähltes Personal (Tr 4.3.4)
	Prüfungsaufgaben der Studieninstitute		x		Nicht Scannen		Prüfungaufgaben dürfen von Dritten nicht eingesehen werden. Bei entsprechender Adressierung wird der Umschlag nicht geöffnet.
	Familienkasse (z.B. Kindergeld)		x	x	Ersetzend scannen mit erhöhtem organisatorischen und technischen Standard	DA-KG (Dienstanweisung zunm Kindergeld nach dem EStG (O2.73)	1. Qualifizierte elektronische Signatur (rechtliche Regelung sollte überarbeitet werden) 2. Die Familienkasse muss für die Kindergeldakten eine organisatorische Ablage- bzw. Speicherform wählen, die die Wahrung des Steuergeheimnisses (§ 30 AO) sicherstellt. Sollte das Scannen der Dokumente durch Dritte erfolgen, so sind diese Personen zur Wahrung des Steuergeheimnisses gem. § 30 AO förmlich zu verpflichten (vgl. O 2.7 Abs. 3)

Vitako-Projektgruppe ersetzendes Scannen

- Vorgaben der TR RESISCAN für das ersetzende Scannen auf kommunale Praxis übertragen
- Interpretation der TR RESISCAN und fachlich-inhaltliche Diskussion im Kreis kommunaler Praktiker (25 beteiligte Institutionen)
- Erarbeitung einer Musterverfahrensbeschreibung für alle Kommunen mit Begleitung des BSI

(Quelle: VITAKO)

VITAKO
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V.

Bundesamt für Sicherheit in der Informationstechnik

Musterverfahrensbeschreibung der VITAKO

- Verfahrensbeschreibung dokumentiert Maßnahmen und Verfahrensschritte, die für behördeninterne Scanprozesse inkl. der Vernichtung der originären Papierbelege gelten
- Anwendung der Anlage V (TR RESISCAN) auf kommunaler Ebene
- Beibehaltung der Original-Gliederungspunkte
- Modularer Aufbau, Verweis auf mitgeltende Unterlagen
  Gliederungsplan der Behörde, AGA, verwendete Hard- und Software beim Scannen, verantwortliches Scanpersonal, Verantwortliche für IT-Sicherheit, Qualifizierungsmaßnahmen etc.

(Quelle: VITAKO)

VITAKO
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V.

4. Erteilte Zertifikate

Erteilte Zertifikate

DATEV eG (BSI-K-TR-0202-2015)
Deutsche Telekom AG Placement Services Business Projects (BSI-K-TR-0233-2016)
DMI GmbH & Co. KG (BSI-K-TR-0246-2016)
DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (BSI-K-TR-0153-2015)
Enteos GmbH (BSI-K-TR-0230-2016)
Mentana Claimsoft GmbH (BSI-K-TR-0169-2014)
Satz-Rechen-Zentrum Hartmann + Heenemann GmbH & Co. KG [SRZ-Berlin] (BSI-K-TR-0178-2016)
Universal Investment GmbH (BSI-K-TR-0235-2016)
Vivento Customer Services GmbH (BSI-K-TR-0196-2014)

9 insgesamt (davon 1 Re-Zertifizierung)

(Stand 04/2017)

Zertifikat- Beispiel

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifikat

nach Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

BSI-K-TR-0202-2015

Scan-Prozess

Ersetzendes Scannen für DATEV Unternehmen online nach TR-RESISCAN bei der DATEV eG

der	DATEV eG
Konformität zu:	**BSI TR-03138** – Technische Richtlinie Ersetzendes Scannen (TR-RESISCAN)
gültig bis:	19. März 2018

Die Konformität des Prüfgegenstands 'Ersetzendes Scannen für DATEV Unternehmen online nach TR-RESISCAN bei der DATEV eG' zur Technischen Richtlinie BSI TR-03138 wurde von dem vom BSI zertifizierten Auditor für ISO 27001 Audits auf der Basis von IT-Grundschutz, Herrn Martin Steger, intersoft certification services GmbH, überprüft und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt.

Als Prüfgrundlage für die Konformitätsprüfung dienten:

BSI TR-03138 – Technische Richtlinie Ersetzendes Scannen
Version 1.0 vom 20. März 2013

BSI TR-03138 – Technische Richtlinie Ersetzendes Scannen
Anlage P: Prüfspezifikation, Version 1.1 vom 04. Dezember 2014

Der Prüfgegenstand erfüllt die Anforderungen der Technischen Richtlinie BSI TR-03138.

Personenzertifizierung RESISCAN Auditor

- Antragsverfahren: auditor@bsi.bund.de (Referat D 25)
- Antrag auf Personenzertifizierung als RESISCAN Auditor ab Ende April 2017 möglich
- Kompetenzfeststellung im Rahmen des Verfahrens

Grds. Zertifizierungsverfahren (TR)

Verfahrensablauf

- Konformitätsprüfung durch zertifizierte IT-Grundschutz Auditoren
- Zertifikatsgültigkeit: 3 Jahre
- Kosten:
  - Zertifizierungsgebühren BSI (Erst-Zertifizierung) [2600,- € pauschal] + Kosten der Konformitätsprüfung

- Alternativen zur Zertifizierung durch BSI
  - Auditor-Testat
  - Konformitätserklärung als Eigenerklärung

Weitere Informationen, Antragsformular, … unter: www.bsi.bund.de/zertifizierungtr

Bundesamt für Sicherheit in der Informationstechnik

4. Weitere Umsetzungsbeispiele und Ausblick

Weitere Umsetzungsbeispiele

BMI: Muster-Hausanordnung „Ersetzendes Scannen“ - Dieses Muster legt fest, wie mit eingescannten Papierdokumenten zu verfahren ist. (04/2016)

BÄK/KBV: „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“

Deutsche Steuerberaterverband e.V.: „Gemeinsame Muster-Verfahrensdokumentation (...) zur Digitalisierung und elektronischen Aufbewahrung von Belegen inkl. Vernichtung der Papierbelege“

Bundesversicherungsamt für Sozialversicherungsträger: Leitfaden „Elektronische Kommunikation und Langzeitspeicherung elektronischer Daten“

Organisationskonzept elektronische Verwaltungsarbeit: Module zum Scannen & zur Langzeitaufbewahrung

Bund-Länder-Kommission für Informationstechnik in der Justiz: „Organisatorisch-technische Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften“, Beschluss des E-Justice-Rats auf Grundlage eines BLK-Beschlusses, Muster-Rechtsverordnung

Fazit

- **Rechtssichere Digitalisierung ist insbesondere für die rechtskonforme E-Akte relevant**
- Nutzung von Einspareffekten, **Effizienzsteigerung** von Verwaltungsprozessen und -dienstleistungen
- **Unterschiedlicher Schutzbedarf** der verarbeiteten Dokumente, branchen- und fachverfahrens-/ bereichsspezifisch
  - ➔ Auswahl der geeigneten, d.h. angemessenen Maßnahmen zur Realisierung von Informations- und Rechtssicherheit
  - ➔ Klassifizierung von Dokumentengruppen für analoge Bereiche
- Erstellung von **Blaupausen** schafft Synergieeffekte und spürbaren Mehrwert
- BSI TR-RESISCAN unterstützt durch standardisierten Prozess und ermöglicht den Nachweis der Ordnungsgemäßheit: **Digitalisierung sicher und einfach**

Ausblick

- **Weiterentwicklung** der TR RESISCAN bis Ende 2017
  - ➔ Integration der eIDAS-VO und des VDG („SigG-neu“)
  - ➔ Weitere Detailschärfungen
  - ➔ Kontinuierliche Einbindung der kommunalen Perspektive und weiterer Praxiserfahrungen

- **Unterstützung der verschiedenen Branchen** bei generischen Verfahrensanweisungen für große Anwendergruppen,

  u.a. Finanzdienstleistungen und Gesundheitswesen

- **Fortführung des konstruktiven Dialogs** und Erfahrungsaustauschs mit der Praxis, insbesondere mit den Kommunen

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Dr. Astrid Schumacher
Referatsleiterin
astrid.schumacher@bsi.bund.de
Tel. +49 (0) 228 99 9585 5371
Fax +49 (0) 228 99 10 9585 5371

Bundesamt für Sicherheit in der Informationstechnik
Referat D 11 eID-Anwendungen im E-Government
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik