Bundesamt
für Sicherheit in der
Informationstechnik

Überwindung von Medienbrüchen

BSI - TR 03138 RESISCAN

*** Magglinger Rechtsinformatikseminar 18. Mai 2015 ***

Astrid Schumacher, BSI

Agenda

- **Einleitung**

- **TR RESISCAN** – BSI-Richtlinie 03138 zum ersetzenden Scannen
  - Aufbau und Struktur
  - Rechtlicher Rahmen
  - Zertifizierung

- Ausblick

Bundesamt für Sicherheit in der Informationstechnik

Digitale Agenda für Deutschland

Grundsätze unserer Digitalpolitik	Digitale Infrastrukturen	Digitale Wirtschaft und digitales Arbeiten	Innovativer Staat
Handlungsfelder			
Digitale Lebenswelten in der Gesellschaft gestalten	Bildung, Forschung, Wissenschaft, Kultur und Medien	Sicherheit Schutz und Vertrauen für Gesellschaft und Wirtschaft	Europäische und digitale Dimension der digitalen Agenda

Bundesministerium für Wirtschaft und Energie

Bundesministerium des Innern

Bundesministerium für Verkehr und digitale Infrastruktur

Bundesamt
für Sicherheit in der
Informationstechnik

Digitale Verwaltung

Digitale Verwaltung 2020
www.bmi.bund.de

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

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

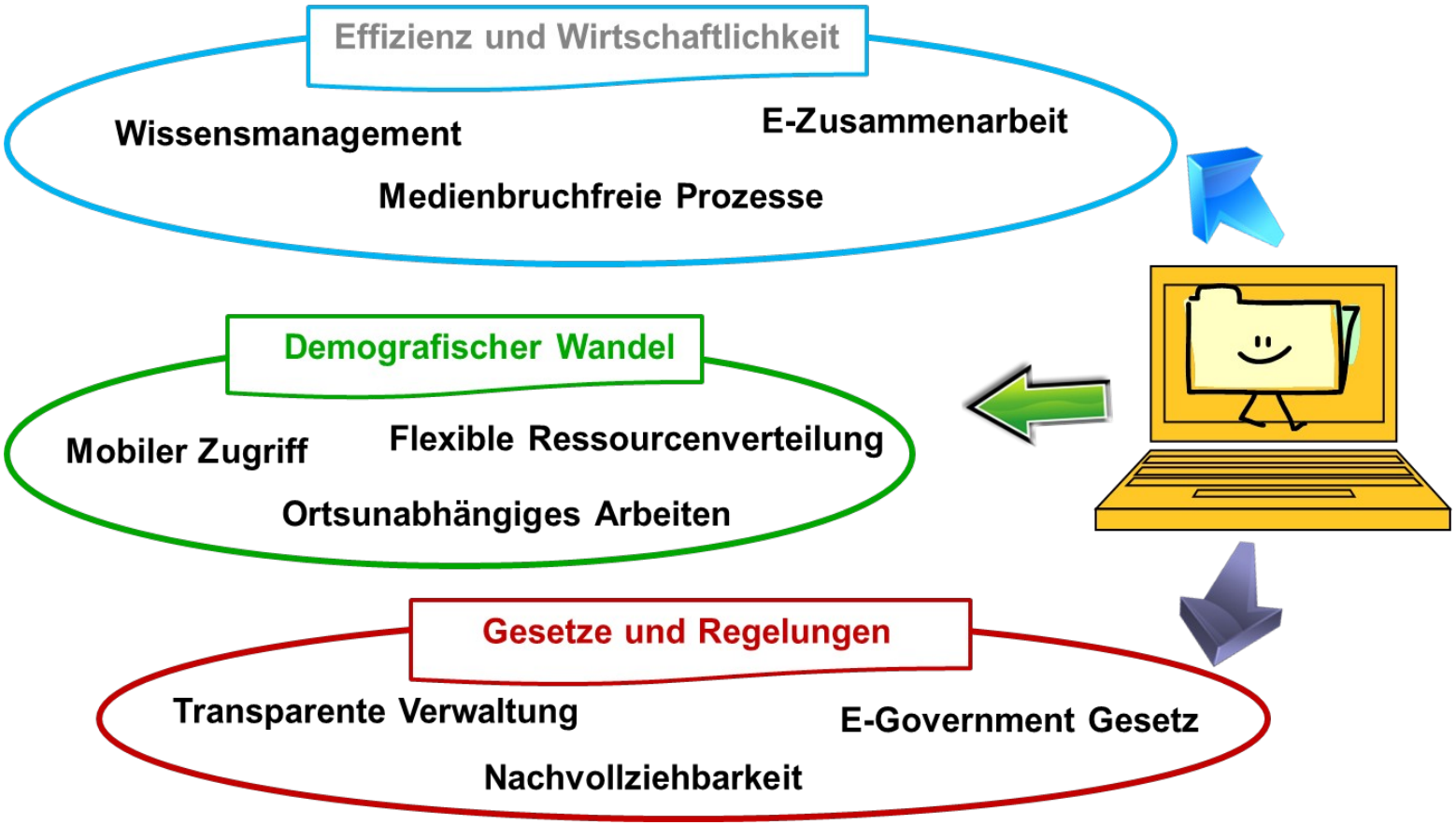
- *Gemeinsame IT des Bundes* zur Umsetzung EGovG notwendige Basisdienste für alle Bundesressorts (IT-Rahmenkonzept des Bundes), inkl. De-Mail-Gateway und zentraler eID-Service

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

Schwerpunktthema im IT-PLR unter Vorsitz Bund 2014/2016 und Berliner Vorsitz 2015 (geplant)

IT-Planungsrat

Die E-Akte


Effizienz und Wirtschaftlichkeit
Wissensmanagement
E-Zusammenarbeit
Medienbruchfreie Prozesse
Demografischer Wandel
Mobiler Zugriff
Flexible Ressourcenverteilung
Ortsunabhängiges Arbeiten
Gesetze und Regelungen
Transparente Verwaltung
E-Government Gesetz
Nachvollziehbarkeit

Bundesamt
für Sicherheit in der
Informationstechnik

Elektronische Aktenführung

- §§ 6 und 7 EGovG fordern die elektronische Aktenführung inkl. Scannen und Langzeitaufbewahrung nach dem „Stand der Technik“ bis zum 1. Januar 2020

- Zudem: Beweisregelungen zugunsten nach Stand der Technik eingescannter Dokumente, z.B. §§ 371b, 298a ZPO

- Orientierungshilfen des BSI durch Technische Richtlinien

- Weitere Unterstützung bei der Konzeption von E-Government-Verwaltungsdienstleistungen und Geschäftsprozessen im E-Government durch BSI TR-3107 „Elektronische Identitäten und Vertrauensdienste im E-Government“

Agenda

- Einleitung
- **TR RESISCAN – BSI-Richtlinie 03138 zum ersetzenden Scannen**
  - **Aufbau und Struktur**
  - Rechtlicher Rahmen
  - Zertifizierung
- Ausblick

Ausgangslage

Rechtlich-technischer Rahmen:

- Mediumwechsel von analogen in elektronische Daten
- Rechtlich bedeutsam:
  die dem Papier immanenten Sicherheitsmerkmale zum Integritäts- und Authentizitätsschutz gehen verloren
- Gesetzliche Ausgestaltung des Scanprozesses nur vereinzelt, obwohl das Bedürfnis auch anwendungsübergreifend besteht

Wesentliche Fragen im Rahmen der TR:

→ (rechtliche und) *technisch-organisatorische Anforderungen an den Scanprozess und das Scanprodukt*

→ Erreichung eines möglichst hohen, dem Original angenäherten Beweiswert des Scanproduktes für ein Gerichtsverfahren

Bundesamt
für Sicherheit in der
Informationstechnik

Projekt TR 03138 RESISCAN – Team und Organisation –

- **Auftraggeber: BSI; Laufzeit: Mitte 2011 – Anfang 2013**
- **Auftragnehmer:**
  - ecsec GmbH

- **Unterauftragnehmer:**
  - secunet Security Networks AG

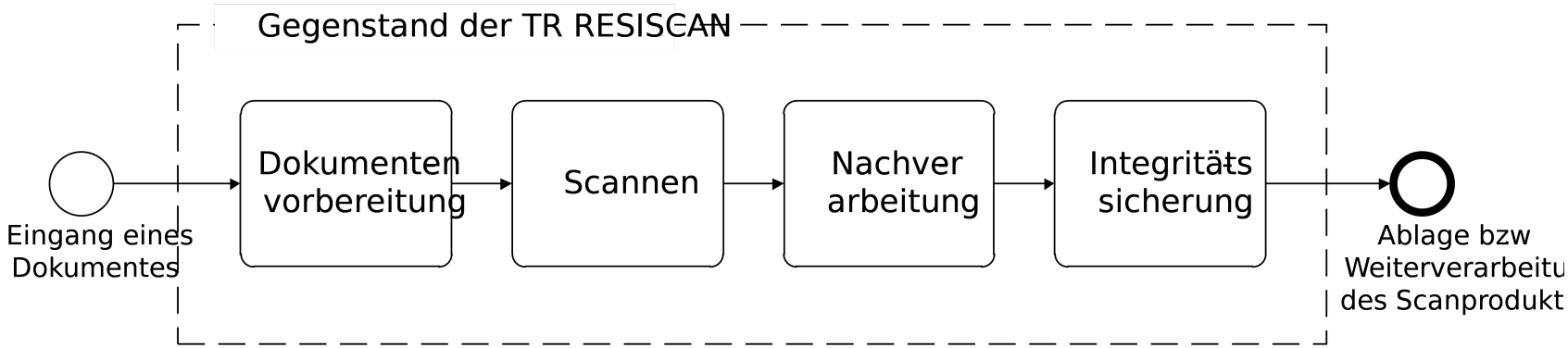
- **Rechtliche Begleitung**
  - provet

- **Projektbeirat**
  - Wirtschaftsvertreter, Unternehmen und Verbände, Verwaltung und Justiz, EDV-Gerichtstag, Versicherungswesen, Gesundheitswesen, Steuerberatungswesen, BMI, BMF, BfDI, Bundeskanzleramt, Datenverarbeitungszentrum M-V, etc.

Bundesamt
für Sicherheit in der
Informationstechnik

Der „generische Scanprozess“

- 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)



Bundesamt
für Sicherheit in der
Informationstechnik

Modularer Maßnahmenkatalog

Aufbaumodule mit zusätzlichen Sicherheitsmaßnahmen

Zusätzliche Maßnahmen bei Schutzbedarf **„sehr hoch“** bzgl. **Integrität**	Zusätzliche Maßnahmen bei Schutzbedarf **„sehr hoch“** bzgl. **Vertraulichkeit**	Zusätzliche Maßnahmen bei Schutzbedarf **„sehr hoch“** bzgl. **Verfügbarkeit**
Zusätzliche Maßnahmen bei Schutzbedarf **„hoch“** bzgl. **Integrität**	Zusätzliche Maßnahmen bei Schutzbedarf **„hoch“** bzgl. **Vertraulichkeit**	Zusätzliche Maßnahmen bei Schutzbedarf **„hoch“** bzgl. **Verfügbarkeit**

Generelle Maßnahmen bei der Verarbeitung von Dokumenten mit erhöhtem Schutzbedarf.

Basismodul

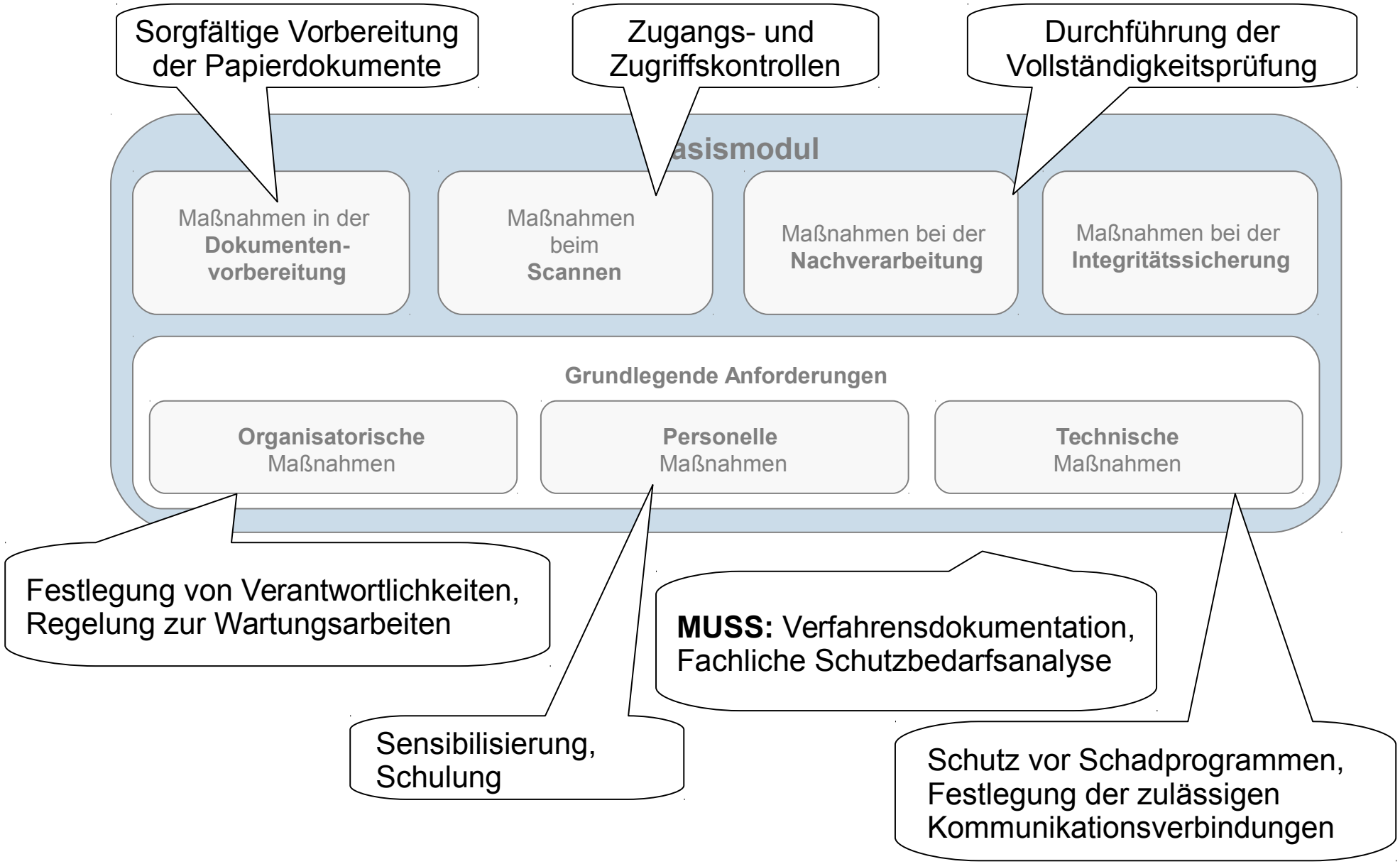
Maßnahmen in der **Dokumenten-vorbereitung**	Maßnahmen beim **Scannen**	Maßnahmen bei der **Nachverarbeitung**	Maßnahmen bei der **Integritätssicherung**

Grundlegende Anforderungen

Organisatorische Maßnahmen	**Personelle** Maßnahmen	**Technische** Maßnahmen

Bundesamt
für Sicherheit in der
Informationstechnik

Das Basismodul (für alle) – Beispiele



Bundesamt
für Sicherheit in der
Informationstechnik

Aufbaumodul – Beispiele

Agenda

- Einleitung
- **TR RESISCAN – BSI-Richtlinie 03138 zum ersetzenden Scannen**
  - Aufbau und Struktur
  - **Rechtlicher Rahmen**
  - Zertifizierung
- Ausblick

Rechtliche Betrachtung

Scannen von Papierdokumenten und Vernichtung der Originale

Rechtsfragen

Zulässigkeit
Dokumentations-, Aktenführungs- und Aufbewahrungspflichten

Teilweise Regelungen zum ersetzenden Scannen im jeweiligen Fachrecht (tlw. Homogenität der Regelungen)

Beweiswert

Gegenstand des Augenscheins (§ 371 Abs. 1 S. 2 ZPO); Vernichtung des Originals führt zu einer Verschlechterung der Beweissituation

Anlage R

„Unverbindliche rechtliche Erläuterungen zur Anwendung der TR RESISCAN“

Ziel:

- Erläuterung der Zusammenhänge zwischen Recht und TR RESISCAN
- Darstellung der aktuellen Rechtslage
- Hilfestellung für den Anwender bei der Einordnung und Beantwortung rechtlicher Fragen und Probleme

Aufbau:

- Sicherheitsziele und exemplarische Schutzbedarfsanalysen

- Rechtliche Fragen im Zusammenhang mit ersetzendem Scannen

Gesetzliche Referenzen: elektronische Aktenführung

- **§ 7 EGovG: Übertragen und Vernichten des Papieroriginals**

  Erlaubnis zum ersetzenden Scannen mit Verweis auf TR Resiscan, umfasst Teilbereich der 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 ein weitere Aufbewahrung nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvorgangs erforderlich ist."

→ *als Beispiel für den Stand der Technik kann die TR-Resiscan des BSI herangezogen werden.*

Gesetzliche Referenzen: elektronische Aktenführung & Beweisregelung

- **§ 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.“*

→ ***Simulationsstudie !***

Agenda

- Einleitung
- **TR RESISCAN – BSI-Richtlinie 03138 zum ersetzenden Scannen**
  - Aufbau und Struktur
  - Rechtlicher Rahmen
  - **Zertifizierung**
- Ausblick

Bundesamt
für Sicherheit in der
Informationstechnik

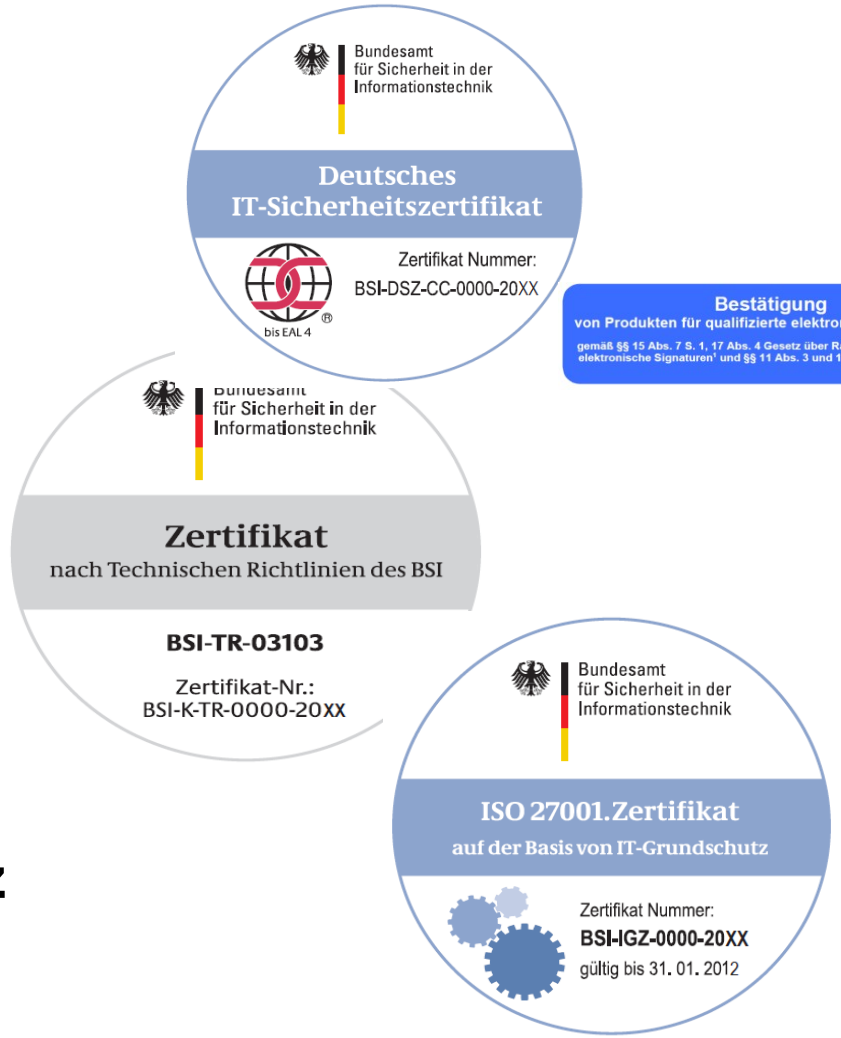
Zertifizierung und Konformitätsprüfung im BSI

1) Zertifizierung nach **CC** und ITSEC
(+ ggf. Bestätigung nach SigG)

2) Zertifizierung nach **TR**

3) Zertifizierung nach **IT-Grundschutz**

4) Neu: **Mindeststandard** nach § 8 I BSIG



Bundesamt
für Sicherheit in der
Informationstechnik

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

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

Bundesamt
für Sicherheit in der
Informationstechnik

Aktuelle Prüfspezifikationen

BSI Technische Richtlinie 03138
Ersetzendes Scannen

Anlage P: Prüfspezifikation

Bezeichnung
RESISCAN – Ersetzendes Scannen
Kürzel
BSI TR RESISCAN – 03138-P
Version **1.1**
(beinhaltet Test Cases TR-RESISCAN, Version 1.2)

Datum
04.12.14

Bundesamt
für Sicherheit in der
Informationstechnik

Aktuelle Prüfspezifikationen

Aktuelle Prüfspezifikationen

- Reduzierter Prüfumfang
- Im Testfall A.T.1 max. fünf Grundschutz-Bausteine zu prüfen
- Wiederverwendung von Prüfergebnissen für Bausteine möglich

  → Prüfumfang der 5 Bausteine ggf. reduzieren
- Abstimmung von Prüfumfang bzw. Bausteinauswahl vor dem Audit mit dem BSI

Prüfgegenstand I

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.

Bundesamt
für Sicherheit in der
Informationstechnik

Ersetzendes Scannen für DATEV Unternehmen online nach TR-RESISCAN

- Referenzimplementierung eines Scanprozesses bei der DATEV eG
- Digitalisierung der für den Prozess erforderlichen Belege
- Einstufung des Schutzbedarfs: normal

Prüfgegenstand II

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifikat

nach Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

BSI-K-TR-0196-2014

Scanprozess gemäß TR-RESISCAN

Scanprozess im De-Mail Accountmanagement der Deutschen Telekom AG

der	Vivento Customer Services GmbH
Konformität zu:	**BSI TR-03138** – Technische Richtlinie Ersetzendes Scannen (TR-RESISCAN)
gültig bis:	04. Dezember 2017

Die Konformität des Prüfgegenstands 'Scanprozess im De-Mail Accountmanagement der Deutschen Telekom AG' 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

BSI TR-03138 – Technische Richtlinie Ersetzendes Scannen
Anlage P: Prüfspezifikation, Version 1.2

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

Bundesamt
für Sicherheit in der
Informationstechnik

Scanprozess im De-Mail Accountmanagement der Deutschen Telekom AG

- Digitalisierung der für Eröffnung eines De-Mail Kontos notwendigen Dokumente
- Versendung an Auftraggeber T-Systems International GmbH
- Einstufung des Schutzbedarfs:
  - Integrität: hoch
  - Verfügbarkeit: normal
  - Vertraulichkeit: hoch

Prüfgegenstand III

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifikat

nach Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

BSI-K-TR-0169-2014

Scan-Prozess

Scan-Station
Scanprozess im De-Mail Accountmanagement

der	Mentana Claimsoft GmbH
Konformität zu:	**BSI TR-03138** – Technische Richtlinie Ersetzendes Scannen (TR-RESISCAN)
gültig bis:	14. Mai 2017

Die Konformität des Prüfgegenstands 'Scan-Station (Scanprozess) im De-Mail Accountmanagement' 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

BSI TR-03138 – Technische Richtlinie Ersetzendes Scannen
Anlage P: Prüfspezifikation, Version 1.0

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

Scan-Station bei der Mentana Claimsoft GmbH

- Scan der für Eröffnung eines De-Mail Kontos notwendigen Dokumente
- Ablage im Archiv
- Einstufung des Schutzbedarfs: hoch

Aktuelle Ergänzung der TR

Auswahl geeigneter Kompressionsverfahren

- Bei der Umsetzung der TR-RESISCAN ist hinsichtlich der Auswahl geeigneter Kompressionsverfahren folgende Regelung zu beachten:
  - Beim Scannen MUSS auf die Auswahl geeigneter Bildkompressionsverfahren geachtet werden.
  - verlustfreie als auch verlustbehaftete Verfahren grundsätzlich geeignet
  - Verfahren, die zur Bildkompression die sog. „Pattern Matching & Substitution“ - Vorgehensweise nutzen, DÜRFEN NICHT eingesetzt werden. Auch das verwandte Soft Pattern Matching DARF NICHT eingesetzt werden.

- Bei ungenauem oder fehlerhaft implementiertem Pattern Matching besteht die Gefahr, dass sich das Scanergebnis semantisch (z. B. durch Vertauschung von Zeichen) vom Original unterscheidet. Selbst bei korrekter Implementierung kann die notwendige Rechtssicherheit aufgrund einer nicht sicher bestimmbaren inhaltlichen und bildlichen Übereinstimmung nicht gewährleistet werden.

Umsetzungsbeispiele

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“

Organisationskonzept elektronische Verwaltungarbeit (OeV, Nachfolge DOMEA): Module zum Scannen und zur Langzeitaufbewahrung

Bund-Länder-Kommission für Informationstechnik in der Justiz: Organisatorisch-technische Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften

Agenda

- Einleitung
- **TR RESISCAN** – BSI-Richtlinie 03138 zum ersetzenden Scannen
  - Aufbau und Struktur
  - Rechtlicher Rahmen
  - Zertifizierung
- **Ausblick**

Perspektive

Technisch-Organisatorisch

- **Orientierungshilfen**
- **Konformitätsbewertung, u.a.** iRe Zertifizierung
  - Obj. Beurteilung durch unabhängige Prüfkriterien
  - *Standardisierte Vorgehensweise*:
    Erhöhung der Produktsicherheit
- **Empfehlungen** für Ausschreibung und Beschaffung
- **Spezifikationen** für Produkte und Lösungen

Rechtlich

- Erleichterung der **Beweiswürdigung** durch die Gerichte: Nachweis durch Simulationsstudie erbracht (ArchiSig/Resiscan)
- **Referenzierung** in Rechtsvorschriften sowie Erleichterung der Schaffung neuer **Zulässigkeitstatbestände: eGovG, ERV-G**
- **Einheitliche Auslegung** nach bestehenden und zukünftigen Regelwerken erleichtert die tatsächliche und rechtliche Interpretation

Nächste Schritte

- **Weitere Zertifizierungsverfahren** nach TR Resiscan laufen
- Erweiterung mit Bezug auf **Hard- und Software?**
- **TR-Evaluierung**
  - Anpassung der Prüfspezifikation, insbes. IT-GS-Anforderungen
  - Aktualisierung und Anpassung der TR bis Mitte 2015
    - u.a. Integration der Empfehlung zu Kompressionsverfahren

Zusammenfassung

- Zunehmend elektronische Datenverarbeitung in allen Branchen (eAkte)
- Unterschiedlicher Schutzbedarf der verarbeiteten Dokumente

- Herausforderungen im Bereich
  a) dem dokumentenersetzenden Scannen
  b) der Beweiswerterhaltung kryptographisch signierter Dokumente

- BSI stellt Technische Richtlinien für diese Themen bereit:

a) **TR-RESISCAN**

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html

b) **TR-ESOR**

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Dr. Astrid Schumacher
Godesberger Allee 185
53175 Bonn

astrid.schumacher@bsi.bund.de

www.bsi.bund.de
www.bsi-fuer-buerger.de