Vertrauenswürdige E-Akte auf Basis von TR-RESISCAN / TR-ESOR

Jawad Ahmad[1] · Detlef Hühnlein[2] · Ulrike Korte[1]

[1]Bundesamt für Sicherheit in der Informationstechnik
{jawad.ahmad, ulrike.korte}@bsi.bund.de

[2]ecsec GmbH
detlef.huehnlein@ecsec.de

Zusammenfassung

Im Rahmen der Digitalisierungsstrategie der neuen deutschen Bundesregierung soll nun zügig die elektronische Vorgangsbearbeitung in der öffentlichen Verwaltung (E-Akte) eingeführt und somit der bereits im E-Government-Gesetz aus 2013 definierte rechtliche Rahmen praktisch ausgefüllt werden. In §6 [EGovG] (Elektronische Aktenführung) und §7 [EGovG] (Übertragen und Vernichten des Papieroriginals) wird der Einsatz von Sicherheitsmaßnahmen nach dem Stand der Technik gefordert, der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die „Beweiswerterhaltung kryptographisch signierter Dokumente“ in [BSI TR-03125] (TR-ESOR) und für das „Ersetzende Scannen“ in [BSI TR-03138] (TR-RESISCAN) dokumentiert wurde. Der vorliegende Beitrag stellt die wesentlichen Inhalte dieser beiden Richtlinien unter besonderer Berücksichtigung der jüngsten Änderungen vor und erläutert schließlich, welchen Beitrag diese beiden Richtlinien für eine vertrauenswürdige Digitalisierung der öffentlichen Verwaltung spielen können.

1 Einleitung

Durch die Digitalisierung von Geschäftsprozessen in Wirtschaft und Verwaltung können Kosten gesenkt sowie Fehlerquoten und Prozesslaufzeiten reduziert werden. Beispielsweise wird in Kapitel IV. Abschnitt 5 des Koalitionsvertrages der deutschen Bundesregierung vom 14.03.2018 [Bund18] zurecht festgestellt, dass *„die Digitalisierung […] große Chancen für unser Land und seine Menschen“*[1] bietet und die Bundesregierung deshalb unter anderem *„eine vollständig elektronische Vorgangsbearbeitung in der öffentlichen Verwaltung (E-Akte) zügig“*[2] einführen will. Liegen Daten und Dokumente erst einmal in elektronischer Form vor, so können die Abläufe unter Einsatz von elektronischen Signaturen, Siegeln, Zeitstempeln und sonstigen Vertrauensdiensten der eIDAS-Verordnung [eIDAS-VO] nicht nur effizient, sondern auch sehr sicher, vertrauenswürdig und nicht zuletzt rechtsverbindlich gestaltet werden.

Unglücklicher Weise werden viele Dokumente bislang noch nicht „digital geboren“, sondern häufig müssen papiergebundene Schriftstücke erst eingescannt und digitalisiert werden, bevor

[1] [Bund18], Zeile 1598 ff.

[2] [Bund18], Zeile 2028 ff.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 215-227.

sie elektronisch verarbeitet und in der E-Akte abgelegt werden können. Für diesen Fall spezifiziert die Technische Richtlinie 03138 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) *„Ersetzendes Scannen (RESISCAN)“* [BSI TR-03138], wie ein Scanprozess gestaltet werden sollte, damit die Rechtssicherheit auch dann noch möglichst weitgehend erhalten bleibt, wenn das papiergebundene Original nach der Digitalisierung vernichtet wird.

Eine weitere Herausforderung bei der Umsetzung der vollelektronischen Vorgangsbearbeitung auf Basis der E-Akte besteht darin, dass die Beweiskraft von signierten, gesiegelten oder mit einem Zeitstempel versehenen elektronischen Dokumenten im Laufe der Zeit schwinden kann, wenn die eingesetzten kryptographischen Algorithmen ihre Sicherheitseignung verlieren. Damit elektronische Unterschriften gewissermaßen nicht „verblassen“, fordert §15 [VDG] folgendes: *„Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen.“* Hierfür spezifiziert die Technische Richtlinie 03125 des BSI *„Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-ESOR)* auf der Grundlage bestehender rechtlicher Normen sowie nationaler und internationaler technischer Standards ein modular aufgebautes Gesamtkonzept für die beweiswerterhaltende Langzeitspeicherung.

Der vorliegende Beitrag stellt die aktuellen Versionen dieser beiden BSI-Richtlinien vor und erläutert die Rolle derselben bei der Einführung der E-Akte und der vertrauenswürdigen Digitalisierung der deutschen Verwaltung.

Der Rest des Beitrags ist folgendermaßen gegliedert: Abschnitt 2 liefert einen groben Überblick über den Anwendungsbereich der beiden BSI-Richtlinien und das Zusammenspiel derselben mit der E-Akte. Abschnitt 3 geht näher auf die in [BSI TR-03138] spezifizierten Anforderungen für das ordnungsgemäße ersetzende Scannen ein und Abschnitt 4 beleuchtet ausgewählte Aspekte der [BSI TR-03125]. Hierbei wird insbesondere auch auf die jeweiligen Änderungen in den kürzlich veröffentlichten Versionen 1.2 (TR-RESISCAN, siehe Abschnitt 3.3) bzw. 1.2.1 (TR-ESOR, siehe Abschnitt 4.4) eingegangen. In Abschnitt 5 wird schließlich skizziert, wie ein integriertes technisches System für die vertrauenswürdige Digitalisierung der deutschen Verwaltung aufgebaut sein könnte und ein Ausblick auf zukünftige Entwicklungen gewagt.

2 Zusammenspiel der BSI-Richtlinien mit der E-Akte

Die im Koalitionsvertrag [Bund18] genannte elektronische Verwaltungsarbeit auf Basis der E-Akte wird in Deutschland bereits seit geraumer Zeit thematisiert. Neben den rechtlichen Rahmenbedingungen durch das E-Government-Gesetz [EGovG] existiert bereits ein „Organisationskonzept elektronische Verwaltungsarbeit“ [Bund12] sowie eine vergleichsweise generische „Referenzarchitektur elektronische Verwaltungsarbeit“ [Bund13]. Auf dieser Basis wurde eine Anbieterbefragung [ÖfIT15] und schließlich ein Vergabeverfahren „Beschaffung des Basisdienstes E-Akte/DMS für die Bundesverwaltung“ durchgeführt und im November 2017 abgeschlossen [Faba17].

Aktuell wird der Basisdienst E-Akte realisiert und die Pilotierung der E-Akte bei ausgewählten Bundesbehörden[3] vorbereitet (vgl. [BMI17a], [BMI17b] und [BMI18]). Hierbei kann der Basisdienst E-Akte über geeignete Schnittstellen, wie z.B. [CMIS], angesprochen und mit entsprechenden Client-Systemen, Scansystemen, Fachverfahren und sonstigen IT-Systemen des Bundes, wie z.B. der auf der Open Source Plattform Nextcloud[4] basierten „Bundescloud“ (vgl. [Beut18] und [Grün18]) oder dem „Digitalen Zwischenarchiv des Bundes“ [DZAB] integriert werden. Die aktuelle Zeitplanung zur Einführung der E-Akte Bund in der deutschen Bundesverwaltung (Stand: Juli 2018) ist in [BMI18] dargestellt. Ein Überblick über entsprechende Aktivitäten auf Ebene der Bundesländer findet sich beispielsweise in [Zaho15].

Wie bereits eingangs erwähnt, spezifiziert die *TR-RESISCAN* Anforderungen für eine ordnungsgemäße und Risiko-minimierende Gestaltung des Scanprozesses für die Transformation eines papiergebundenen Originals in ein elektronisches Abbild und adressiert somit eine *frühe Phase* des Lebenszyklus eines elektronischen Dokumentes.

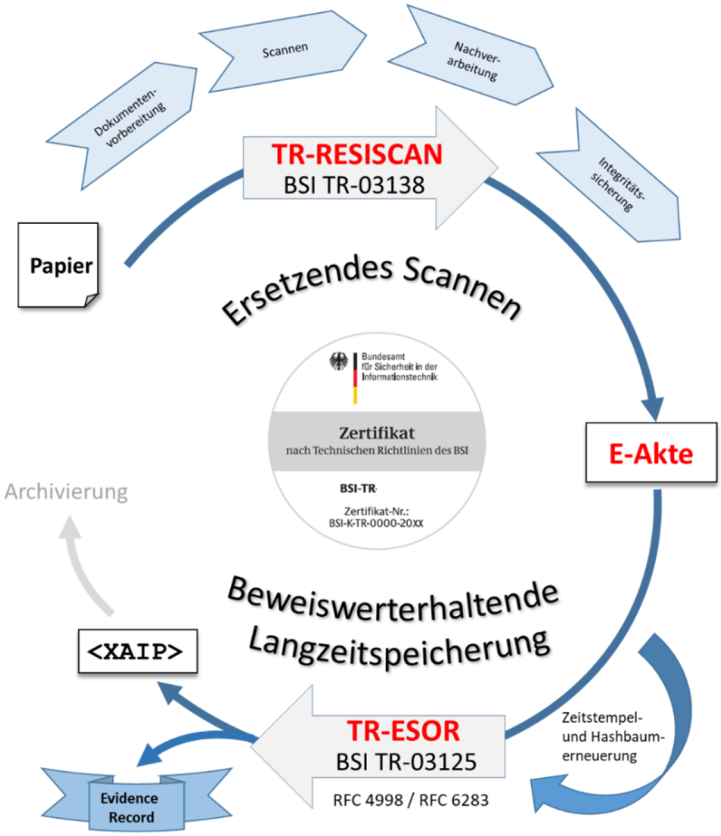

Abb. 1: Zusammenspiel von TR-RESISCAN, E-Akte und TR-ESOR

Die *TR-ESOR* sorgt hingegen für den Beweiswerterhalt kryptographisch signierter Dokumente bei der langfristigen Aufbewahrung bis hin zur Archivierung und adressiert somit eher eine *späte Phase* des Lebenszyklus eines elektronischen Dokumentes.

---

[3] Neben dem führenden Pilotprojekt beim Bundesamt für Justiz (BfJ) sind weitere Pilotprojekte beim Bundesministerium der Finanzen (BMF), bei der Bundeszentrale für politische Bildung (BbP), beim Bundesministerium der Justiz und für Verbraucherschutz (BMJV) und beim Statistischen Bundesamt (StBA) vorgesehen, bevor die E-Akte in der Bundesverwaltung eingeführt wird.

[4] Siehe https://nextcloud.com

Wie in Abbildung 1 skizziert, ist das verbindende Element zwischen den beiden von den TRs adressierten frühen und späten Phasen die *E-Akte*, durch die eine vollständige elektronische Aktenführung ermöglicht werden soll.

Um einen vertrauenswürdigen Gesamtprozess für die digitale Vorgangsbearbeitung zu erhalten, müssen also die verschiedenen Aspekte der TR-RESISCAN, E-Akte und TR-ESOR in einem integrierten und ganzheitlichen Ansatz zusammen betrachtet werden.

Hierbei können beispielsweise die vorbereitenden Maßnahmen, wie die für die TR-RESISCAN notwendige Schutzbedarfsanalyse und Verfahrensdokumentation mit den Checklisten und Leitfäden zur Einführung der E-Akte organisatorisch integriert werden. In ähnlicher Weise kann durch die technische Integration des E-Akte Basisdienstes mit TR-RESISCAN-konformen Scan- und Signatursystemen einerseits und TR-ESOR-basierten Ablagesystemen andererseits ein vertrauenswürdiges Ablagesystem für die vollständig elektronische Vorgangsbearbeitung geschaffen werden.

3 BSI TR-03138 (TR-RESISCAN)

Wie in [SGHJ12] und [HüKS12] und näher erläutert, wurde für die Entwicklung der TR-RESISCAN eine Markt-, Struktur-, Schutzbedarfs-, Bedrohungs- und Risikoanalyse für ein „typisches Scansystem“ und für den „generischen Scanprozess“ durchgeführt, der die Schritte „Dokumentenvorbereitung“, das eigentliche „Scannen“, die „Nachverarbeitung“ und schließlich die „Integritätssicherung“ umfasst (vgl. Abbildung 1).

Hieraus wurde ein modularer Anforderungs- und Maßnahmenkatalog (vgl. Abbildung 2 und Abschnitt 3.2) entwickelt. Die Einhaltung der dort formulierten Anforderungen kann durch anerkannte Auditoren geprüft und objektiv bestätigt werden (Zertifizierung). Aktuell (April 2018) existieren zwölf gemäß BSI TR-03138 zertifizierte Scanprozesse[5].

3.1 Methodik der Analyse

Die bei der Entwicklung der TR-RESISCAN genutzte Methodik ist in informeller Weise an die internationalen Standards [ISO27001], [ISO27005] und die IT-Grundschutz-Vorgehensweise (siehe [BSI-200-2]) des BSI angelehnt und umfasste die in [HüKS12] und [SGHJ12] näher beschriebenen Schritte zur:

- Strukturanalyse,
- Schutzbedarfsanalyse,
- Bedrohungsanalyse und
- Risikoanalyse.

Das Ergebnis dieses elaborierten Prozesses ist in der informativen [BSI TR-03138-A] niedergelegt, welche lediglich informativen und historischen Charakter besitzt.

3.2 Modularer Anforderungs- und Maßnahmenkatalog

Um diesen Risiken zu minimieren, wurden entsprechende technische und organisatorische Sicherheitsmaßnahmen festgelegt, die den identifizierten Gefährdungen entgegenwirken. Aus

[5] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/Zertifizierung nachTR/ZertifizierteProdukte/TR-RESISCAN/TR-RESISCAN_node.html

diesen Sicherheitsmaßnahmen wurden Anforderungen abgeleitet, die bei der richtlinienkonformen Ausgestaltung des Scanprozesses berücksichtigt werden müssen, sollen oder können. Um ein für den jeweiligen Anwendungsfall und damit für das konkrete Fachverfahren angemessenes Sicherheitsniveau erreichen zu können, wurde der Maßnahmenkatalog in einer modularen Weise aufgebaut. Bei der Entwicklung der TR-RESISCAN wurde bewusst dieser Weg gewählt, damit der Anwender die für seinen konkreten Einsatzbereich angemessene Sicherheitsstufe wählen und dadurch die in betriebswirtschaftlicher Hinsicht effizienteste Lösung realisieren kann.

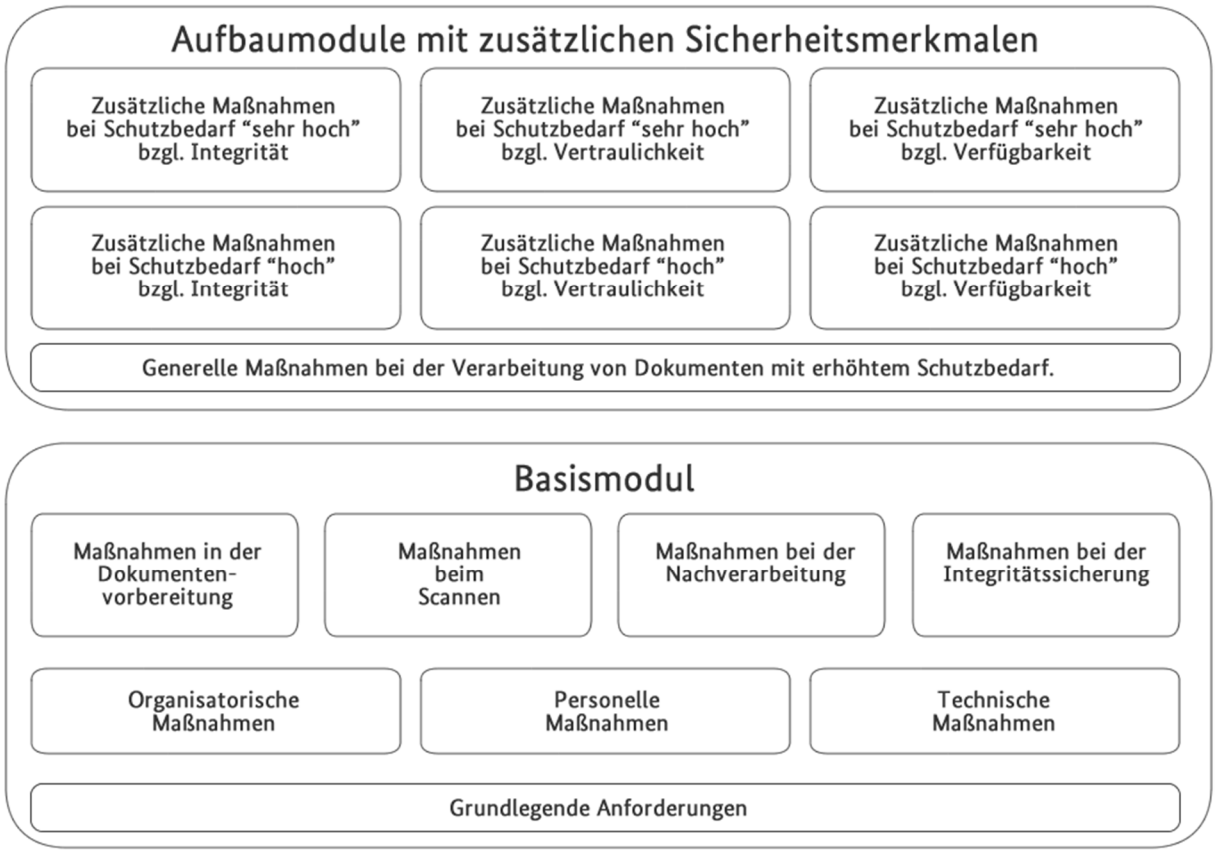

Abb. 2: Der modulare Maßnahmenkatalog der TR-RESISCAN im Überblick

Der in Abbildung 2 dargestellte Maßnahmenkatalog (vgl. [BSI TR-03138], Abbildung 3) sieht im *Basismodul* zunächst *grundlegende Anforderungen* vor, die für eine richtlinienkonforme Ausgestaltung des Scanprozesses umzusetzen sind. Diese umfassen übergreifende und somit in allen Phasen des Scanprozesses wirksame *organisatorische Maßnahmen*, wie z. B. Festlegung von Verantwortlichkeiten und Funktionstrennung, sowie *personelle Maßnahmen*, wie z. B. Verpflichtung zur Einhaltung von Gesetzen, Sensibilisierung und Schulung der Mitarbeiter und *technische Maßnahmen*, wie z. B. die geeignete Netztrennung bei Einsatz von netzwerkfähigen Scannern. Darüber hinaus sieht die Richtlinie spezifische Maßnahmen für die verschiedenen Phasen des Scanprozesses (Dokumentenvorbereitung, Scannen, Nachverarbeitung, Integritätssicherung) vor.

Für den hohen und sehr hohen Schutzbedarf existieren zudem Aufbaumodule zur angemessenen Steigerung der Integrität, Vertraulichkeit und Verfügbarkeit.

3.3 Änderungen in Version 1.2 der TR-RESISCAN

Wie in der aktuellen Version 1.2 der [BSI TR-03138] klargestellt wurde, empfiehlt sich beispielsweise bei hohem Schutzbedarf hinsichtlich der Integrität[6] der Einsatz von fortgeschrittenen elektronischen Signaturen oder fortgeschrittenen elektronischen Siegeln und/oder elektronischen Zeitstempeln gemäß [eIDAS-VO].

Sofern Datenobjekte (a) mit einem Schutzbedarf von „sehr hoch" bezüglich der Integrität verarbeitet werden, (b) die Verkehrsfähigkeit gefordert ist und (c) die im Rahmen des Scanprozesses entstandenen Datenobjekte (Scanprodukt, Transfervermerk, Index- und Metadaten, Protokolldaten) voraussichtlich als Beweismittel genutzt werden, sollen[7] für die Integritätssicherung des Scanproduktes bzw. des Transfervermerkes qualifizierte elektronische Signaturen, qualifizierte elektronische Siegel und qualifizierte Zeitstempel gemäß der [eIDAS-VO] eingesetzt werden.

Im Transfervermerk[8] werden

1. der Ersteller des Scanproduktes,
2. das technische und organisatorische Umfeld des Erfassungsvorganges,
3. etwaige Auffälligkeiten während des Scanprozesses,
4. der Zeitpunkt der Erfassung,
5. das Ergebnis der Qualitätssicherung und nicht zuletzt
6. die Tatsache, dass es sich um ein Scanprodukt handelt, das bildlich und inhaltlich mit dem Papierdokument übereinstimmt, dokumentiert.

Zu den wesentlichen Änderungen, die mit Version 1.2 der TR eingeführt wurden, zählt die maßgeblich überarbeitete und aktualisierte [BSI TR-03138-R] mit rechtlichen Hinweisen sowie die neu geschaffene [BSI TR-03138-F], in der häufig gestellte Fragen zur TR-RESISCAN beantwortet werden.

Aktuell wird an einer Profilierung der TR-RESISCAN für das Gesundheitswesen gearbeitet, die den spezifischen Anforderungen in diesem Bereich Rechnung trägt und welche die Anwendung der TR in diesem wichtigen Anwendungsbereich erleichtern soll.

4 BSI TR-03125 (TR-ESOR)

Die Übertragung von Papierdokumenten in die elektronische Form induziert zusätzliche Risiken bezüglich der Authentizität und Integrität der Daten, denen oft durch Einsatz elektronischer Signaturen bzw. Siegel begegnet wird. Auf der anderen Seite ist die Sicherheitseignung der eingesetzten kryptographischen Algorithmen selbst eine Funktion der Zeit, so dass bei der langfristigen Aufbewahrung signierter Dokumente zusätzliche Maßnahmen für den Erhalt der Beweiskraft notwendig sind.

Für diesen Zweck hat das BSI die Technische Richtlinie 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente" (TR-ESOR) auf Basis des Evidence Record Syntax (ERS)

---

[6] Vgl. A.AM.IN.H.1 (Einsatz kryptographischer Mechanismen zum Integritätsschutz) in [BSI TR-03138], Abschnitt 4.3.2.1.

[7] Vgl. A.AM.IN.SH.2 (Einsatz qualifizierter elektronischer Signaturen oder Siegel und Zeitstempel) in [BSI TR-03138], Abschnitt 4.3.3.2.

[8] Siehe A.NB.4 in [BSI TR-03138], Abschnitt 4.2.7.4. Ein Praxisbeispiel für die Umsetzung des Transfervermerks, der von der Deutschen Rentenversicherung bereitgestellt wurde, findet sich unter https://resiscan.de.

Standards (vgl. [RFC4998] und [RFC6283]) und der Ergebnisse der vorausgegangenen Projekte ArchiSig [RoSc06] und ArchiSafe [ArchiSafe] entwickelt. Hierdurch kann insbesondere die Integrität und Authentizität archivierter Daten und Dokumente bis zum Ende der gesetzlich vorgeschriebenen Aufbewahrungspflicht unter Wahrung des rechtswirksamen Beweiswertes erhalten werden. Die Einhaltung der Anforderungen an die ordnungsgemäße Aufbewahrung wird dabei vorausgesetzt.

Thematisch behandelt die Technische Richtlinie dabei:

- Daten- und Dokumentenformate,
- Austauschformate für Archivdatenobjekte und Beweisdaten,
- Empfehlungen zu einer Referenzarchitektur, ihrer Prozesse, Module und Schnittstellen als Konzept einer Middleware,
- Konformitätsregeln für die Konformitätsstufe 1 „logisch-funktional“ und die Konformitätsstufe 2 „technisch-interoperabel“ sowie
- zusätzliche Anforderungen für Bundesbehörden.

Aus den für den Erhalt des Beweiswerts notwendigen funktionalen Anforderungen wurde eine modulare Referenzarchitektur abgeleitet, die in Abschnitt 4.1 kurz vorgestellt wird. Die Erfüllung dieser Anforderungen kann im Rahmen eines TR-spezifischen Zertifizierungsverfahrens nachgewiesen werden (siehe Abschnitt 4.3).

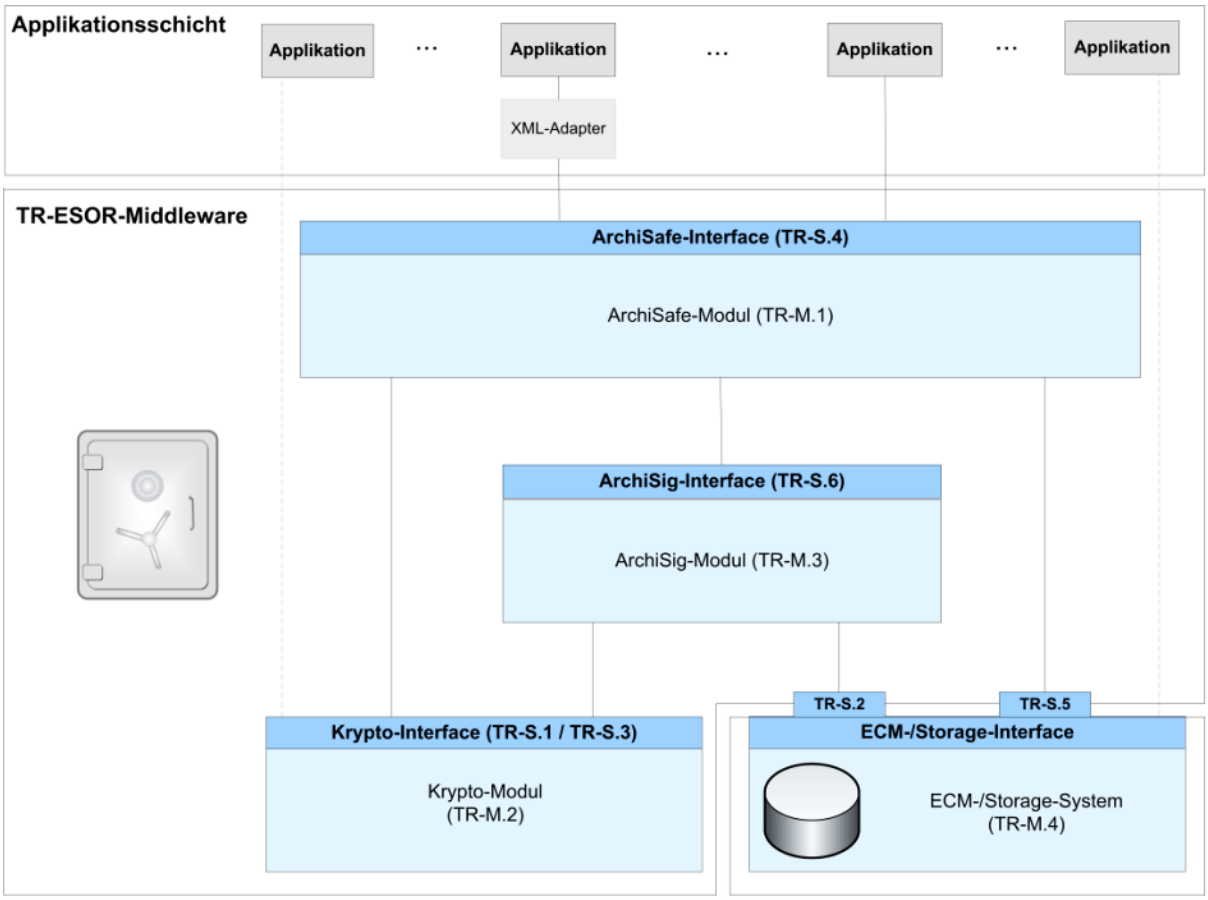

Abb. 3: TR-ESOR Referenzarchitektur

4.1 TR-ESOR Referenzarchitektur

Die in der TR-ESOR für Zwecke des Beweiswerterhalts kryptographisch signierter Daten entwickelte Referenzarchitektur (siehe Abbildung 3) besteht aus den folgenden funktionalen und logischen Einheiten:

- *„ArchiSafe-Interface“* (TR-S. 4) bildet die Eingangs-Schnittstelle zur TR-ESOR-Middleware und bettet diese in die bestehende IT- und Infrastrukturlandschaft ein.
- Das *„ArchiSafe-Modul“* (TR-M.1) regelt den Informationsfluss in der Middleware, sorgt dafür, dass die Sicherheitsanforderungen an die Schnittstellen zu den IT-Anwendungen umgesetzt werden und gewährleistet eine Entkopplung von Anwendungssystemen und Enterprise Content Management (ECM)/Langzeitspeicher.
- Das *„Krypto-Modul“* (TR-M.2) mit den Eingangsschnittstellen TR-S.1 und TR-S.3 stellt die kryptographischen Funktionen bereit, welche für den Beweiswerterhalt kryptographisch signierter Dokumente wesentlich sind.
- Das *„ArchiSig-Modul“* (TR-M.3) mit der Schnittstelle TR-S. 6 stellt die erforderlichen Funktionen für die Beweiswerterhaltung der digital signierten Unterlagen gemäß [RoSc06] zur Verfügung. Auf diese Weise wird gewährleistet, dass die in §15 [VDG] geforderte Signaturerneuerung einerseits gesetzeskonform und anderseits performant und wirtschaftlich durchgeführt werden kann und somit dauerhafte Beweissicherheit gegeben ist.
- Das *ECM*- bzw. das *Langzeitspeicher-System* mit den Schnittstellen TR-S.2 und TR-S.5, das nicht mehr Teil der Technischen Richtlinie 03125 TR-ESOR ist, sorgt für die physische Archivierung/Aufbewahrung.

Die in Abbildung 3 dargestellte IT-Referenzarchitektur orientiert sich an der ArchiSafe-Referenzarchitektur [ArchiSafe] und soll die funktionale Konformität und technische Interoperabilität von TR-ESOR-Produkten unterstützen bzw. ermöglichen (siehe auch [BSI TR-03125-C.1] und [BSI TR-03125-C.2]).

Diese strikt plattform-, produkt-, und herstellerunabhängige Technische Richtlinie [BSI TR-03125] hat einen modularen Aufbau und besteht aus einem Hauptdokument und Anlagen, die die funktionalen und sicherheitstechnischen Anforderungen an die einzelnen Module, Schnittstellen und Formate der TR-ESOR-Middleware beschreiben.

4.2 Formate

Für die Langzeitspeicherung ist es erforderlich, dass nur langfristig verfügbare und verkehrsfähige Datenformate wie z. B. ASCII, TIFF, PDF/A und XML für die zu archivierenden Dokumente zum Einsatz kommen.

Aufbauend auf den Grundlagen aus den Projekten ArchiSig [RoSc06], ArchiSafe [ArchiSafe] sowie XFDU [XFDU] werden zudem die zu archivierenden Daten in ein selbsterklärendes Archivdatenobjekt als Austauschformat auf der Basis von XML (kurz „XAIP“ für „XML Archival Information Package“ genannt) eingebettet und so dem Langzeitspeicher zur Archivierung übergeben [BSI TR-03125-F]. Das XAIP enthält neben einem „Inhaltsverzeichnis“ und Metadaten die Originaldaten sowie Beweisdaten (z. B. Signaturen, Zeitstempel, sog. Evidence Records), so dass insbesondere auch die Verkehrsfähigkeit gegeben ist.

4.3 Konformität und Interoperabilität

Für die Technische Richtlinie 03125 TR-ESOR sind drei Stufen für die Konformitätsprüfung von Produkten und Systemen vorgesehen:

- Konformitätsstufe 1 – Funktionale Konformität gemäß [BSI TR-03125-C.1]
- Konformitätsstufe 2 – Technische Konformität gemäß [BSI TR-03125-C.2]
- Konformitätsstufe 3 – Technische Konformität gemäß der Profilierung für Bundesbehörden [BSI TR-03125-B]

Diese drei Konformitätsstufen unterscheiden sich in technischen Detailspezifikationen der Schnittstellen und Formate und sind in [BSI TR-03125] (Abschnitt 9) und [HüKS12] (Abschnitt 4.3) näher beschrieben.

Derzeit (April 2018) sind fünf Produkte[9] gemäß der ersten Stufe der Konformität (Level 1 – Functional Conformity gemäß [BSI TR-03125-C.1]), aber noch keine Produkte gemäß der zweiten Stufe der Konformität (Level 2 – Technical Conformity gemäß [BSI TR-03125-C.2]), zertifiziert.

4.4 Änderungen in Version 1.2.1 der TR-ESOR

Die wesentlichen Änderungen in Version 1.2.1 der TR-ESOR gehen letztlich auf die seit Juli 2016 in ganz Europa anwendbare [eIDAS-VO] zurück. Hierdurch können neben elektronischen Signaturen nun insbesondere auch elektronische Siegel eingesetzt werden, die bei der Beweiswerterhaltung berücksichtigt werden müssen. Darüber hinaus ist bei der optionalen Signaturerzeugung in der TR-ESOR-Middleware nun auch die Möglichkeit der „Fernsignatur“ erwähnt, bei der die Erstellung von elektronischen Signaturen und Siegeln durch einen spezialisierten Vertrauensdiensteanbieter erfolgen kann. Außerdem wird nach der Aktualisierung von [BSI TR-03125-F] nun auf die in [2015/1506/EU] referenzierten AdES-Formate für fortgeschrittene elektronische Signaturen und Siegel verwiesen.

Um die technische Konformität und Interoperabilität zwischen den verschiedenen TR-konformen Produkten zu verbessern, wurden entsprechende Prüfwerkzeuge für Evidence Records gemäß [RFC4998] und XAIP-Container gemäß [BSI TR-03125-F] entwickelt und validiert. Außerdem wurde ein technischer Workshop mit Herstellern von TR-ESOR-Middleware-Produkten durchgeführt, dessen Ergebnisse in die nächste Version der TR-ESOR (Version 1.3) einfließen werden.

Im Einklang mit den aktuell bei ETSI ESI laufenden Standardisierungsarbeiten für Bewahrungsdienste gemäß [eIDAS-VO] soll diese TR-ESOR-Version voraussichtlich beispielsweise auch effizientere ASiC-basierte Container-Formate und JSON-basierte REST-Schnittstellen enthalten.

5 Integriertes technisches System und Ausblick

Ein integriertes technisches System für die vertrauenswürdige Digitalisierung der Bundesverwaltung könnte etwa wie Abbildung 4 dargestellt aufgebaut sein.

[9] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/Zertifizierung nachTR/ZertifizierteProdukte/TR-ESOR/TR-ESOR_node.html

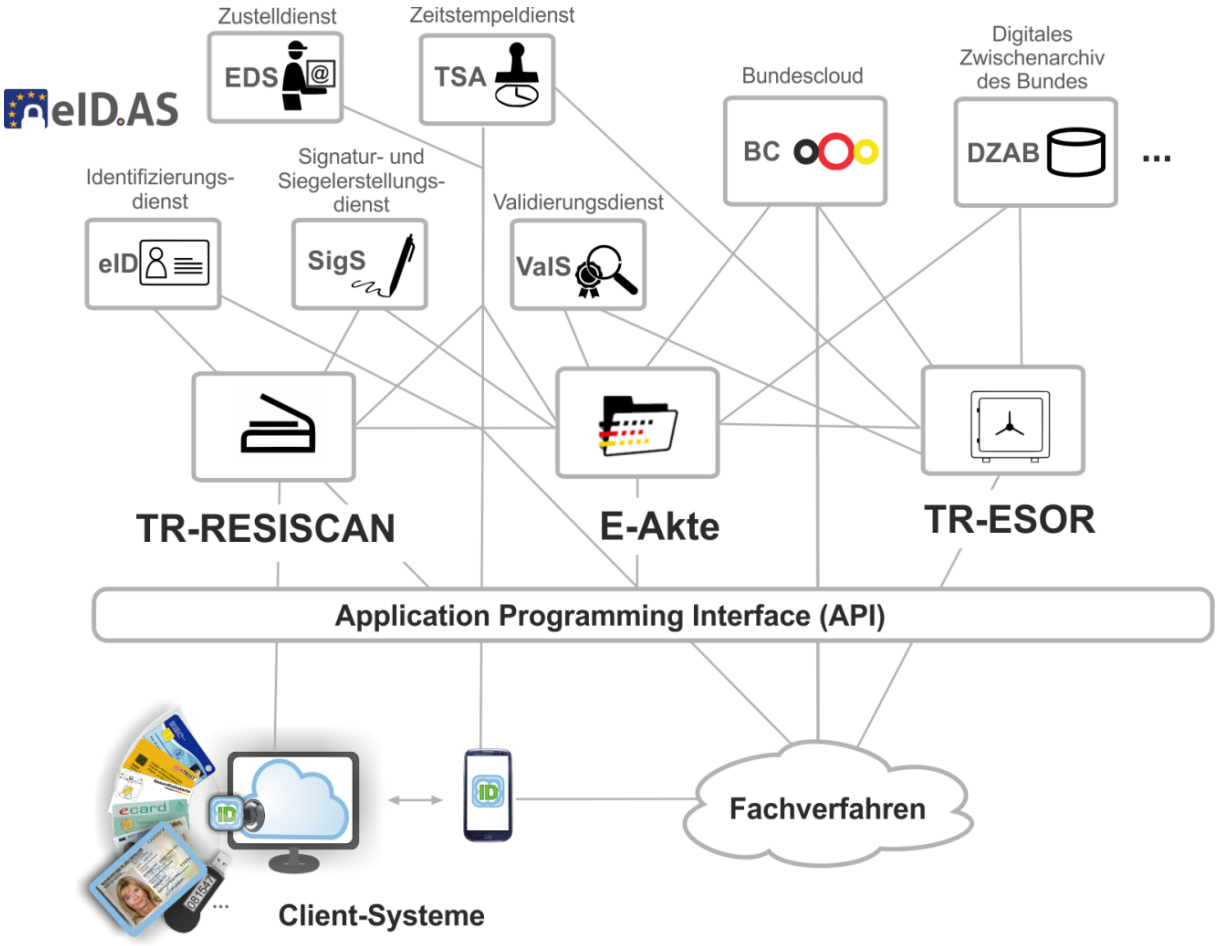

Abb. 4: Integriertes System zur vertrauenswürdigen Digitalisierung der deutschen Verwaltung

Hierbei würden Fachverfahren und Client-Systeme über entsprechend gesicherte Programmierschnittstellen (API) mit Scankomponenten (TR-RESISCAN), dem E-Akte Basisdienst und Systemen für die beweiswerterhaltende Aufbewahrung signierter Dokumente (TR-ESOR) kommunizieren. Diese zentralen Bausteine stützen sich wiederum auf generische Basisdienste gemäß der eIDAS-Verordnung [eIDAS-VO] (eID, SigS, EDS, TSA, ValS) und nutzen weitere Anwendungen und Dienste des Bundes, wie z.B. die „Bundescloud“ oder das digitale Zwischenarchiv des Bundes (DZAB).

Nur durch ein Service-orientiertes System, das sich nahtlos in eine tragfähige Digitalisierungsstrategie und „Digitale Gesamtarchitektur“ (vgl. [Scha18]) einfügt, über offene und möglichst international standardisierte Schnittstellen verfügt, konsequent Sicherheitsaspekte berücksichtigt, stets entsprechende Sicherheitsmaßnahmen nach dem jeweiligen Stand der Technik umsetzt und nach Möglichkeit, wie bereits die „Bundescloud“, als Open Source verfügbar ist, kann die vertrauenswürdige Digitalisierung der deutschen Verwaltung sowohl beim Bund, als auch in den Ländern und bei den Kommunen gelingen und E-Government in Deutschland nachhaltig erfolgreich sein.

Es gibt viel zu tun – packen wir’s an!

Literatur

[2015/1506/EU] Durchführungsbeschluss (EU) 2015/1506 der Kommission vom 8. 9. 2015 zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel http://data.europa.eu/eli/dec_impl/2015/1506/oj

[ArchiSafe] Physikalisch-Technische Bundesanstalt: vgl. http://www.archisafe.de

[Beut18] P. Beuth: Open-Source-Lösung – Deutsche Firma baut Dropbox für den Bund, 17.04.2018, http://www.spiegel.de/netzwelt/web/open-source-software-nextcloud- baut-die-bundescloud-a-1203261.html

[BSI-200-2] BSI: BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise

[BSI-GSKat] BSI: IT-Grundschutz-Kataloge, 15. Ergänzungslieferung, 2016

[BSI TR-03125] BSI: Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), Technische Richtlinie (TR) 03125, Version 1.2.1, 15.03.2018, http://tr-esor.de[BSI TR-03125-B] BSI: Anlage B zu [BSI TR-03125], Profilierung für Bundesbehörden, Version 1.2.1, 2018

[BSI TR-03125-C.1] BSI: Anlage C.1 zu [BSI TR-03125], Conformity Test Specification (Level 1 – Functional Conformity), Version 1.2.1, 2018

[BSI TR-03125-C.2] BSI: Anlage C.2 zu [BSI TR-03125], Conformity Test Specification (Level 2 – Technical Conformity), Version 1.2.1, 2018

[BSI TR-03125-E] BSI: Anlage E zu [BSI TR-03125]: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks, Version 1.2.1, 2018

[BSI TR-03125-F] BSI: Anlage F zu [BSI TR-03125], Formate und Protokolle, Version 1.2.1, 2018

[BSI TR-03138] BSI: Ersetzendes Scannen (RESISCAN), Version 1.2 vom 30.04.2018, http://resiscan.de

[BSI TR-03138-A] BSI: Anwendungshinweis A zu [BSI TR-03138], Ergebnis der Risikoanalyse, Version 1.2, 2018

[BSI TR-03138-F] BSI: Anwendungshinweis F zu [BSI TR-03138], Häufig gestellte Fragen, Version 1.2, 2018

[BSI TR-03138-P] BSI: Anlage P zu [BSI TR-03138], Prüfspezifikation, Version 1.3, 2018

[BSI TR-03138-R] BSI: Anwendungshinweis R zu [BSI TR-03138], Unverbindliche rechtliche Hinweise, Version 1.2, 2018

[BSI TR-03138-V] BSI: Anwendungshinweis V zu [BSI TR-03138], Exemplarische Verfahrensanweisung, Version 1.2, 2018

[BMI17a] BMI / L. Tsintsifa: E-Akte mit einem einheitlichen Basisdienst: Organisatorische Vorbereitung, Standardisierung, 10.01.2017, https://www.bundesarchiv. de/imperia/ md/content/abteilungen/abtb/b1b/dr_lydia_tsintsifa_vortrag.pdf

[BMI17b] BMI / L. Tsintsifa: Einführung der E-Akte in der Bundesverwaltung – Wie gelingt die Informationssicherheit?, 04.07.2017, https://www.bsi.bund.de/Shared Docs/

Downloads/ DE/ BSI/ Veranstaltungen/ Grundschutz/ 3GS-Tag_2017/ Sicherheitssensibilisierung_der_E-Akte.pdf?__blob=publicationFile&v=3

[BMI18] BMI / M. Reisener, L. Tsintsifa: Die E-Akte Bund – Einfach. Digital. Verwalten, Vortrag im Rahmen des 6. Zukunftskongress Staat & Verwaltung, Berlin, 18.-20. Juni 2018

[Bund12] Bundesregierung: Organisationskonzept elektronische Verwaltungsarbeit, 2012, https:// www. verwaltung-innovativ.de/ DE/ E_Government/orgkonzept_everwaltung/ orgkonzept_everwaltung_artikel.html

[Bund13] Die Beauftragte der Bundesregierung für Informationstechnik: Referenzarchitektur elektronische Verwaltungsarbeit, 2013, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/referenzarchitektur.pdf?__blob=publicationFile

[Bund18] Bundesregierung: Ein neuer Aufbruch für Europa, Eine neue Dynamik für Deutschland, Ein neuer Zusammenhalt für unser Land, Koalitionsvertrag vom 14. März 2018 zwischen CDU, CSU und SPD, 19. Legislaturperiode, https:// www. bundesregierung. de/ Content/ DE/ _Anlagen/ 2018/ 03/ 2018- 03- 14-koalitionsvertrag. pdf

[CMIS] F. Müller, R. McVeigh, J. Hübel (Ed.): Content Management Interoperability Services (CMIS), Version 1.1, OASIS Standard, 23 May 2013, http://docs.oasis-open.org/cmis/CMIS/v1.1/os/CMIS-v1.1-os.pdf

[DZAB] Bundesarchiv: Digitales Zwischenarchiv des Bundes (DZAB), 2018, http://www.bundesarchiv.de/DE/Content/Artikel/Anbieten/Behoerden/Zwischenarchive/digitales-zwischenarchiv.html

[EGovG] Gesetz zur Förderung der elektronischen Verwaltung, http://www.gesetze-im-internet.de/egovg/

[eIDAS-VO] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG vom 23.07.2014, https://eid.as

[Faba17] Fabasoft: Fabasoft erhält Zuschlag im Vergabeverfahren „Beschaffung des Basisdienstes E-Akte/DMS für die Bundesverwaltung“ – Deutschland (Corporate News), 23.11.2017, https:// www. fabasoft. com/ de/ news/ presse/pressemitteilungen/fabasoft-erhaelt-zuschlag-im-vergabeverfahren-beschaffung-des

[Grün18] S. Grüner: Bundescloud – Bundesverwaltung setzt auf Nextcloud, 17.04.2018, https:// www. golem. de/ news/ bundescloud- bundesverwaltung- setzt- auf-nextcloud- 1804-133892.html

[HFG+09] D. Hühnlein, S. Fischer-Dieskau, U. Gnaida, U. Korte, P. Rehäußer, W. Zimmer: Langfristig beweiskräftige Signaturen mit dem eCard-API-Framework, DACH Security 2009, http://www.ecsec.de/pub/2009_DACH-eCard-API.pdf

[HüKS12] D. Hühnlein, U. Korte, A. Schumacher: Die BSI-Richtlinien TR-ESOR und TR-RESISCAN, DACH Security 2012, http:// www. ecsec. de/ pub/ 2012_ DACH_ TRs.pdf

[ISO27001] ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements, International Standard, 2005

[ISO27005] ISO/IEC 27005: Information technology – Security techniques – Information security risk management, International Standard, 2008

[ÖfIT15] Kompetenzzentrum Öffentliche IT: Die elektronische Akte (E-Akte) Anbieterbefragung, August 2015, http://www.oeffentliche-it.de/eakte

[RFC4998] T. Gondrom, R. Brandner, U. Pordesch: Evidence Record Syntax (ERS), IETF RFC 4998, http://www.ietf.org/rfc/rfc4998.txt, August 2007

[RFC6283] A. J. Blazic, S. Saljic, T. Gondrom: Extensible Markup Language Evi-dence Record Syntax (XMLERS), IETF RFC 6283, http://www.ietf.org/rfc/rfc6283.txt, Juli 2011.

[RoSc06] A. Rossnagel, P. Schmücker (Hrsg.): Beweiskräftige elektronische Archi-vierung. Ergebnisse des Forschungsprojektes „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“, Eco-nomica Verlag, 2006

[Scha18] M. Schallbruch: Schwacher Staat im Netz – Wie die Digitalisierung den Staat in Frage stellt, Springer-Verlag, 2018

[SGHJ12] A. Schumacher, O. Grigorjew, D. Hühnlein, S. Jandt: Die Entwicklung der BSI-Richtlinie für das rechtssichere ersetzende Scannen, in Tagungsband FTVI 2012, GI, LNI, 2012, https://subs.emis.de/LNI/Proceedings/Proceedings197/127.pdf

[VDG] Vertrauensdienstegesetz, https://www.gesetze-im-internet.de/vdg/

[XFDU] The Consultative Committee for Space Data Systems: XML FORMATTED DATA UNIT (XFDU), CCSDS 661.0-B-1, September 2008, http://public. ccsds. org/publications/archive/661x0b1.pdf

[Zaho15] I. Zahorsky: eAkte: Stand der Einführung in den Bundesländern, 12.03.2015, https:/ /www. egovernment-computing. de/ eakte-stand-der-einfuehrung-in-den-bundeslaendern-a-481282/