Die BSI-Richtlinien TR-ESOR und TR-RESISCAN

Detlef Hühnlein[1] · Ulrike Korte[2] · Astrid Schumacher[2]

[1] ecsec GmbH, Sudetenstraße 16, 96247 Michelau,
detlef.huehnlein@ecsec.de

[2] Bundesamt für Sicherheit in der Informationstechnik,
{ulrike.korte, astrid.schumacher}@bsi.bund.de

Zusammenfassung

In der öffentlichen Verwaltung werden Geschäftsprozesse zunehmend digitalisiert. Hierfür werden ursprünglich Papier-gebundene Schriftstücke gescannt und elektronische Daten und Dokumente oft auf Grund von Formvorschriften bzw. aus Sicherheitsgründen mit elektronischen Signaturen versehen. Besondere Herausforderungen existieren in diesem Umfeld bei der rechtssicheren Gestaltung des Scanvorganges sowie beim dauerhaften Erhalt der Beweiskraft der elektronisch signierten Dokumente. Vor diesem Hintergrund entwickelt das Bundesamt für Sicherheit in der Informationstechnik (BSI) entsprechende Technische Richtlinien mit Lösungsansätzen und Empfehlungen für diese beiden Problembereiche, die voraussichtlich auch in § 6 EGovG (Elektronische Aktenführung) und § 7 EGovG (Übertragen und Vernichten des Papieroriginals) ihren Niederschlag finden werden (siehe [EGovG-RE]). Der vorliegende Beitrag stellt die wesentlichen Inhalte und das mögliche Zusammenspiel dieser beiden Richtlinien TR-ESOR [BSI-TR-03125] und TR-RESISCAN [BSI-TR-RESISCAN] in kompakter Weise vor.

1 Einleitung

Durch die elektronische und weitgehend automatisierte Abwicklung von Geschäftsprozessen lassen sich Kosten senken, sowie Fehlerquoten und Prozesslaufzeiten reduzieren. Auf der anderen Seite geht die Nutzung elektronischer Dokumente mit zusätzlichen Herausforderungen einher: Elektronische Dokumente können ohne Hilfsmittel weder wahrgenommen noch gelesen werden. Sie liefern aus sich heraus auch weder Anhaltspunkte für ihre Integrität und Authentizität noch einen Nachweis der Ordnungsmäßigkeit im elektronischen Rechts- und Geschäftsverkehr. Diese Eigenschaften müssen vielmehr, beispielsweise bei der Transformation Papier-gebundener Dokumente in die elektronische Form und bei der längerfristigen Aufbewahrung elektronischer Dokumente, durch zusätzliche organisatorische und technische Maßnahmen sichergestellt und dauerhaft erhalten werden. Vor diesem Hintergrund entwickelt das Bundesamt für Sicherheit in der Informationstechnik (BSI) entsprechende Technische Richtlinien mit Lösungsansätzen und Empfehlungen für diese beiden Problembereiche, die voraussichtlich auch in § 6 EGovG (Elektronische Aktenführung) und § 7 EGovG (Übertragen und Vernichten des Papieroriginals) ihren Niederschlag finden werden (siehe [EGovG-RE]).

N. N • N. N (Hrsg.) · DACH Security 2012 · syssec (2012) pp-pp.

Dieser Beitrag beleuchtet die wesentlichen Inhalte und das Zusammenspiel dieser beiden BSI-Richtlinien und ist folgendermaßen gegliedert: Abschnitt 2 beleuchtet den Regelungsgegenstand und Anwendungsbereich dieser beiden Richtlinien. Abschnitt 3 bietet einen Überblick über die in TR-RESISCAN spezifizierten Anforderungen für das ordnungsgemäße ersetzende Scannen. Abschnitt 4 beleuchtet ausgewählte Aspekte der TR-ESOR, die auf der Grundlage bestehender rechtlicher Normen sowie nationaler und internationaler technischer Standards ein modular aufgebautes Gesamtkonzept für die beweiswerterhaltende Langzeitspeicherung bereitstellt. Abschnitt 5 fasst die wesentlichen Ergebnisse des Beitrags kurz zusammen und liefert einen Ausblick auf zukünftige Entwicklungen.

2 Zusammenwirken der beiden Richtlinien

Während die TR-RESISCAN Anforderungen für eine ordnungsgemäße und Risiko-minimierende Gestaltung des Scanprozesses für die Transformation eines papiergebundenen Originals in ein elektronisches Abbild definiert, adressiert die TR-ESOR insbesondere den Beweiswerterhalt kryptographisch signierter Dokumente unter Verwendung von qualifizierten Zeitstempeln, wie dies in § 17 SigV für die langfristige Aufbewahrung von qualifiziert signierten Daten gefordert ist.

Wie in Abb. 1 dargestellt, kann mit einem Aufbewahrungssystem gemäß [BSI-TR-03125] insbesondere auch die in [BSI-TR-RESISCAN] geforderte Integritätssicherung erfolgen.

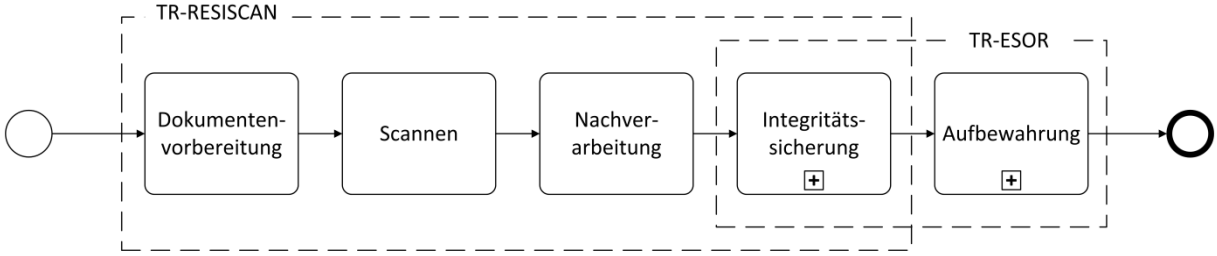

Abb. 1: Zusammenwirken der TR-RESISCAN und TR-ESOR

Auf der anderen Seite ist die Anwendung der in [BSI-TR-03125] spezifizierten Mechanismen für die ordnungsgemäße Integritätssicherung von Dokumenten gemäß [BSI-TR-RESISCAN] nicht in jedem Fall notwendig und wirtschaftlich sinnvoll. Wie im beispielhaften Entscheidungsprozess in Abb. 2 erkennbar, können im Kontext des ersetzenden Scannens gemäß TR-RESISCAN auch alternative Mechanismen zur Integritätssicherung und Aufbewahrung eingesetzt werden. Ist der Schutzbedarf hinsichtlich der Integrität nicht sehr hoch und wird kein verkehrsfähiger Integritätsnachweis benötigt, müssen die aufzubewahrenden Dokumente nicht mit einer qualifizierten elektronischen Signatur versehen werden.

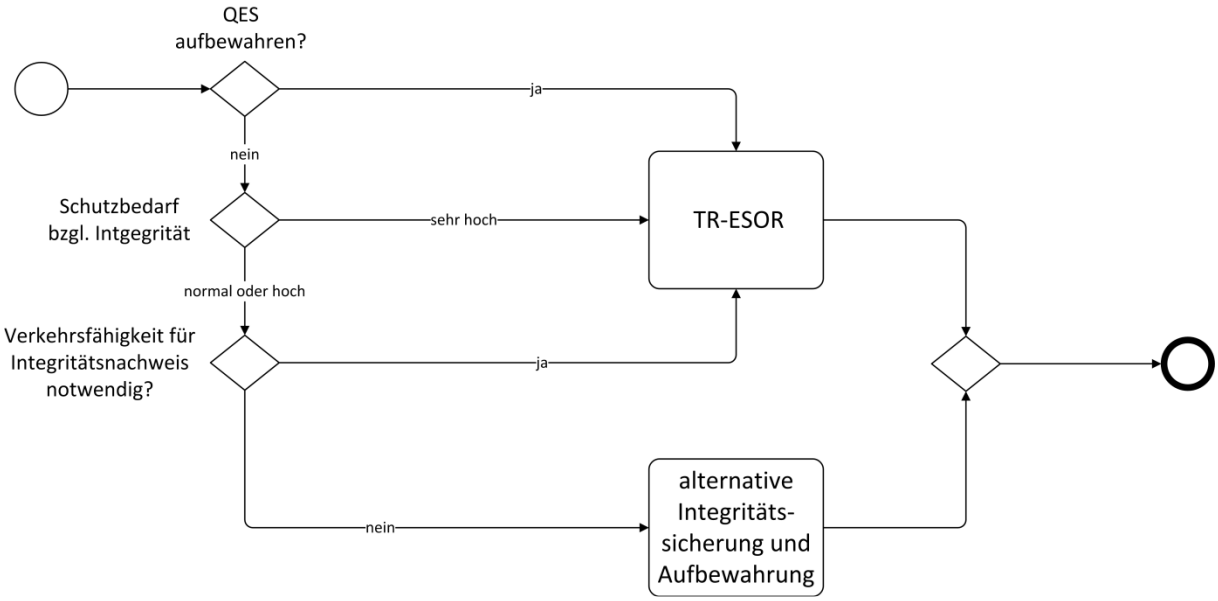

Abb. 2: Möglicher Entscheidungsprozess für die Anwendung von TR-ESOR

3 Technische Richtlinie TR-RESISCAN

Für die Entwicklung der TR-RESISCAN wurde eine Markt-, Struktur-, Schutzbedarfs- und Bedrohungsanalyse 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. Abb. 1 und Abschnitt 3.1).

Hieraus wurde ein modularer Anforderungs- und Maßnahmenkatalog (vgl. Abb. 3 und Abschnitt 3.2) entwickelt. Die Einhaltung der dort formulierten Anforderungen kann durch eine neutrale Stelle geprüft und objektiv bestätigt werden (Zertifizierung).

3.1 Struktur-, Schutzbedarfs- und Bedrohungsanalyse

Die bei der Entwicklung der TR-RESISCAN genutzte Methodik ist in informeller Weise an die internationalen Standards [ISO27001], [ISO27005], das IT-Sicherheitshandbuch [BSI-IT-SiHB] und die IT-Grundschutz-Vorgehensweise (siehe [BSI-100-2], [BSI-100-3]) des BSI angelehnt und umfasst die im Folgenden kurz erläuterten Aufgaben.

Auf Basis des durch Abstraktion aus der Praxis abgeleiteten „generischen Scanprozesses“ (siehe Abb. 1) und des „typischen Scansystemes“ wurden die im weiteren Verlauf zu betrachtenden Objekte identifiziert. Hierbei wurden insbesondere die relevanten Datenobjekte (Schriftgut, Scanprodukte, Sicherungsmittel, Protokolle etc.), IT-Systeme, Netze und Anwendungen betrachtet.

Für diese identifizierten Objekte wurde in zwei Schritten eine detaillierte fachliche und technische Schutzbedarfsanalyse durchgeführt.

Im Rahmen der fachlichen Schutzbedarfsanalyse (siehe z.B. [SGHJ12] für Gerichtsakten) wurde zunächst ausgehend von den rechtlichen Anforderungen der Schutzbedarf der Datenobjekte ermittelt, wobei die differenzierten Sicherheitsziele „Integrität“, „Authentizität“, „Vollständigkeit“, „Nach-vollziehbarkeit“, „Verfügbarkeit“, „Lesbarkeit“, „Verkehrsfähigkeit“, „Vertraulichkeit“ und „Löschbarkeit“ betrachtet wurden.

Danach wurde in der technischen Schutzbedarfsanalyse der Schutzbedarf der IT-Systeme, Anwendungen und Kommunikationsbeziehungen hinsichtlich der Grundwerte „Integrität“, „Verfügbarkeit“ und „Vertraulichkeit“ bestimmt.

Um die einfache Wiederverwendbarkeit der Ergebnisse im IT-Grundschutz-Kontext [BSI-100-2] zu gewährleisten, wurde der jeweilige Schutzbedarf in Abhängigkeit des Schutzbedarfs des ursprünglichen Papierdokumentes ausgedrückt und die differenzierten Sicherheitsziele wurden den oben genannten Grundwerten zugeordnet.

Bei der Bedrohungsanalyse wurden für die einzelnen Datenobjekte, IT-Systeme, Anwendungen und Kommunikationsverbindungen entsprechende Gefährdungen und Schwachstellen ermittelt. Hierbei wurden entlang des „generischen Scanprozesses“ etwaige Bedrohungen ermittelt und geeignete Gegenmaßnahmen vorgeschlagen, die den identifizierten Gefährdungen entgegenwirken können. Dabei wurde auf anwendbare IT-Grundschutz-Bausteine [BSI-GSKat] aufgebaut und bei Bedarf eine entsprechende Präzisierung und Ergänzung vorgenommen. Hierdurch ist ein für das ersetzende Scannen spezifischer Maßnahmenkatalog entstanden, der neben den generischen Gefährdungen und Maßnahmen aus dem IT-Grundschutzhandbuch auch eine Vielzahl von zusätzlichen anwendungsspezifischen Bedrohungen und Maßnahmen enthält.

Unter den spezifischen Bedrohungen in der Dokumentenvorbereitung finden sich beispielsweise die Manipulation oder die Vernichtung des Originals sowie das versehentliche Umdrehen einzelner Blätter in einem Scan-Stapel.

Beim Scannen könnten beispielsweise Fehler bei der Erfassung des Scangutes oder gezielte Manipulationen der Scan-Workstation oder des Scanners auftreten.

Bei der Nachverarbeitung könnte beispielsweise eine falsche Zuordnung der Index- und Metadaten erfolgen, wodurch das zukünftige Auffinden der Scanprodukte erschwert oder gar unmöglich gemacht werden würde.

Die Integritätssicherung könnte schließlich gar nicht oder mit ungeeigneten Sicherungsmitteln erfolgen und die eingesetzten kryptographischen Mechanismen könnten im Laufe der Zeit ihre Sicherheitseignung verlieren. Aus all diesen Gefährdungen ergibt sich ein mehr oder weniger großes Risiko, das den Beweiswert des Scanproduktes schmälern kann.

3.2 Modularer Anforderungs- und Maßnahmenkatalog

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

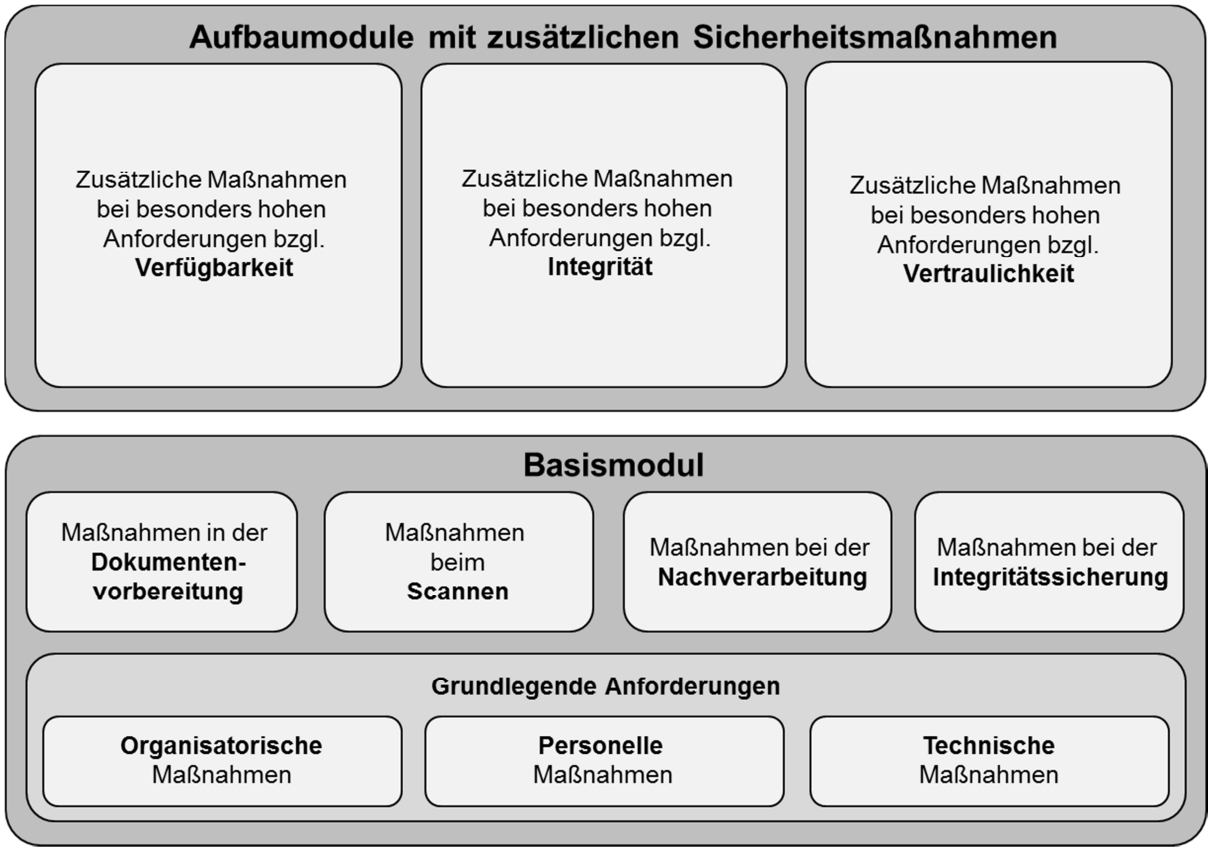

Abb. 3: Der modulare Maßnahmenkatalog der TR-RESISCAN im Überblick

Der in Abb. 3 im Überblick dargestellte Maßnahmenkatalog sieht 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 in den verschiedenen Phasen des Scanprozesses vor. Dies umfasst beispielsweise:

- *Sicherheitsmaßnahmen in der Dokumentenvorbereitung*, wie die sorgfältige Vorbereitung der Papierdokumente, die Kennzeichnung der Dokumente bzgl. Sensitivität oder die Beschränkung des Zugriffs auf sensible Papierdokumente;
- *Sicherheitsmaßnahmen beim Scannen*, wie das sorgfältige Scannen, die Verwendung geeigneter Scan-Einstellungen, die Nutzung von Metainformationen aus der Dokumentenvorbereitung, die Durchführung geeigneter Schritte zur Qualitätssicherung sowie verschiedene Maßnahmen für Drucker, Kopierer, Scanner und Multifunktionsgeräte, wie z.B.
  - die Definition von Kriterien für die Beschaffung und die geeignete Auswahl,
  - die geeignete Aufstellung und Inbetriebnahme,
  - die Änderung voreingestellter Passwörter,
  - die sorgfältige Durchführung von Konfigurationsänderungen,

  - die Beschränkung des Zugriffs und die Verwendung von sicheren Zugriffsmechanismen bei Fernadministration,
  - die geeignete Protokollierung und Auswertung und schließlich
  - die sichere Außerbetriebnahme.
- *Sicherheitsmaßnahmen bei der Nachbereitung*, wie die Durchführung von geeigneten Maßnahmen zur Qualitätssicherung und Nachbearbeitung und schließlich
- *Sicherheitsmaßnahmen zur Integritätssicherung*, wie die Nutzung geeigneter Dienste und Systeme für den Integritätsschutz. Während die oben erläuterten Maßnahmen für ein grundlegendes Schutzniveau sorgen, können in bestimmten Anwendungsszenarien zusätzliche Sicherheitsmaßnahmen zum Schutz der Verfügbarkeit, Integrität und Vertraulichkeit empfehlenswert oder unmittelbar notwendig sein.

Beispielsweise empfiehlt sich für Sozialversicherungsträger (vgl. § 110d SGB IV) oder beim Scannen besonders schützenswerter Dokumente der Einsatz qualifizierter elektronischer Signaturen für die Integritätssicherung. In entsprechender Weise kann ein besonders hohes Maß an Vertraulichkeit durch Einsatz von geeigneten Verschlüsselungsmechanismen erreicht werden. In den beiden genannten Fällen sind darüber hinaus zusätzliche Maßnahmen für das Schlüsselmanagement, die Auswahl geeigneter kryptographischer Produkte und nicht zuletzt Aspekte der Nachsignatur bzw. der Umschlüsselung zu beachten.

4 Technische Richtlinie TR-ESOR (TR 03125)

Die Übertragung von Papierdokumenten in die elektronische Form induziert zusätzliche Risiken bezüglich der Authentizität und Integrität der Daten, denen oft durch Einsatz elektronischer Signaturen 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) 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 5.1 kurz vorgestellt wird. Die Erfüllung dieser Anforderungen kann im Rahmen eines TR-spezifischen Zertifizierungsverfahrens nachgewiesen werden. Abschnitt 5.2 stellt den aktuellen Stand zur Konformitätsprüfung gemäß TR-ESOR vor.

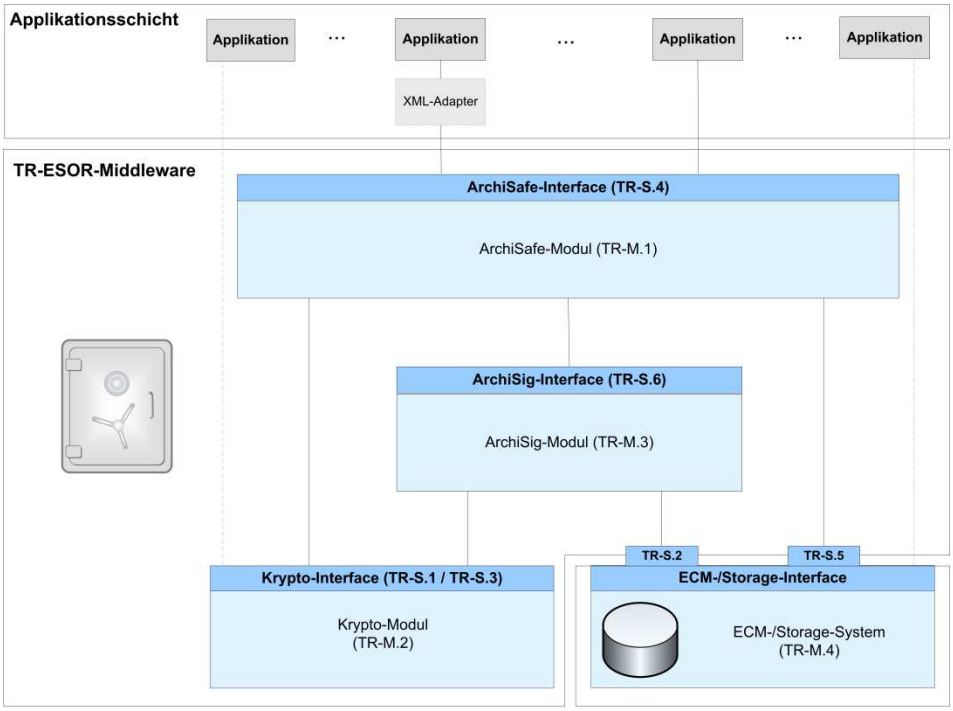

Abb. 4: TR-ESOR Referenzarchitektur

4.1 TR-ESOR Referenzarchitektur

Die in der TR-ESOR für Zwecke des Beweiswerterhalts kryptographisch signierter Daten entwickelte Referenzarchitektur (siehe Abb. 4) besteht aus den folgenden funktionalen und logischen Einheiten:

- Das *„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. Die Sicherheitsanforderungen dieses Moduls sind im „Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Legally compliant Long-Term Preservation of Electronic Documents (ACM_PP)“ [BSI-PP-0049] definiert.
- 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 Krypto-Modul stellt Funktionen zur Erstellung (optional) und Prüfung elektronischer Signaturen, zur Nachprüfung

elektronischer Zertifikate und zum Einholen qualifizierter Zeitstempel für die Middleware zur Verfügung. Das Krypto-Modul muss die Anforderungen des Gesetzes über Rahmenbedingungen für elektronische Signaturen (SigG) und der Verordnung zur elektronischen Signatur (SigV) erfüllen. Die Aufrufschnittstellen des Krypto-Moduls sollen nach dem eCard-API-Framework (vgl. [BSI-TR-03112], [OASIS-DSS] und [BSI-TR-03125-E]) gestaltet sein, um die Integration und Austauschbarkeit kryptographischer Funktionen zu erleichtern.

- 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 § 17 SigV 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 Abb. 4 dargestellte IT-Referenzarchitektur orientiert sich an der ArchiSafe-Referenzarchitektur [ArchiSafe] und soll die logische (funktionale) Interoperabilität künftiger Produkte mit den Zielen und Anforderungen der Technischen Richtlinie ermöglichen und unterstützen (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.

Produkte und Systeme, die gemäß der Technischen Richtlinie 03125 TR-ESOR zertifiziert werden möchten, haben ihre Konformität zu den vorliegenden Spezifikationen nachzuweisen.

Die drei Konformitätsstufen bauen aufeinander auf. Um entsprechend der angestrebten Konformitätsstufe zertifiziert zu werden, muss ein Produkt oder System alle Konformitätskriterien (Testfälle) für diese Konformitätsstufe und für alle tieferen Konformitätsstufen erfüllen.

4.3.1 Funktionale Konformität

Ein System oder eine Komponente ist „funktional konform“ zu [BSI-TR-03125], wenn das System oder die Komponente funktional auf die in dieser Richtlinie beschriebene Systemkomposition oder auf einzelne (auch mehrere) Module dieser Systemkomposition abgebildet werden kann und die Übereinstimmung zu den Anforderungen an das Gesamtsystem oder an einzelne Module festgestellt wird.

Funktional konform im Sinne der [BSI-TR-03125] bedeutet, dass die Komponenten die in der TR-ESOR definierten funktionalen und sicherheitstechnischen Anforderungen erfüllen, die logische Abbildung der funktionalen Anforderungen nachvollziehbar dargestellt wird und die Komponenten zweckmäßig auf der Basis der in der TR-ESOR aufgeführten Ziele und Standards miteinander arbeiten können.

Funktional konform im Sinne der TR-ESOR bedeutet nicht, dass die Schnittstellen der Komponente bzw. des Systems den ASN.1- oder XML- Spezifikationen exakt entsprechen müssen.

Wesentliches Ziel dieser Konformitätsprüfung ist der Nachweis, dass das Modul bzw. das Gesamtsystem den entsprechenden Anteil für die Beweiswerterhaltung funktional umsetzt.

Aktuell wird der Anhang [BSI-TR-03125-C.1] erstellt, der im Herbst 2012 fertiggestellt sein soll.

Dieses Dokument spezifiziert die funktionalen Konformitätskriterien (Testfälle), die aus den bereits veröffentlichten Anforderungen in [BSI-TR-03125] abgeleitet wurden. Zusätzlich werden die vorliegenden Anforderungen und die daraus resultierenden Testfälle der entsprechenden Konformitätsstufe zugeordnet.

Die Testfall-Spezifikation wird so erstellt, dass dieses Dokument als Muster für die Dokumentation der Testdurchführung und Testergebnisse dienen kann.

4.3.2 Technische Konformität

Ein System oder eine Komponente ist „technisch konform“ zu [BSI-TR-03125], wenn zusätzlich zum Nachweis der funktionalen Konformität auch alle bzw. die betreffenden Schnittstel-

len auf Basis der eCard-API [BSI-TR-03112], wie in [BSI-TR-03125-E] beschrieben, umgesetzt sind und ein definiertes XML-Datenformat (z.B. für selbsterklärende Archivdatenobjekte „XML Archiving Information Package“ (XAIP) gemäß [BSI-TR-03125-F]) für die Kommunikation und das Speichern verwendet wird.

Außerdem wird in der Technischen Richtlinie TR-ESOR festgelegt, dass ein Richtlinienkonformes ArchiSig-Modul auf Anforderung Evidence Records gemäß [RFC4998] bzw. [RFC6283] erzeugen können muss.

Die Prüfung der technischen Konformität umfasst dabei insbesondere:

1. die Prüfung der in [BSI-TR-03125-E] spezifizierten Webservice-Schnittstellen (vgl. Abb. 4),
2. die Prüfung der syntaktischen und semantischen Korrektheit der Evidence Records gemäß [RFC4998] bzw. [RFC6283] und
3. die Prüfung der syntaktischen und semantischen Korrektheit der XAIP-Container.

Als XML-Datenformat soll XAIP aus [BSI-TR-03125-F] verwendet werden. Abweichungen im verwendeten XML-Datenformat sind zulässig, allerdings muss dann erläutert werden, dass gleichwertige Funktionalität unterstützt wird. Insbesondere ist zu erläutern, wie eine Transformation in das XAIP Format aus [BSI-TR-03125-F] erfolgen kann.

Außerdem wird derzeit für die automatisierte Durchführung von technischen Konformitätsprüfungen eine erweiterbare Testumgebung geschaffen, die möglichst auf bereits beim BSI existierende Testumgebungen aufbaut, so dass Webservice-Schnittstellen und Signaturspezifische Funktionen und Datenobjekte in einer einheitlichen Umgebung getestet werden können.

5 Zusammenfassung und Ausblick

Zur weiteren Steigerung der Effizienz in der öffentlichen Verwaltung sollen Akten zukünftig elektronisch geführt werden und Papier-gebundene Schriftstücke zu diesem Zweck bei Bedarf eingescannt und das Original möglichst vernichtet werden. Um die hierbei im Vergleich zur Papier-gebundenen Verwaltungstätigkeit entstehenden Risiken kompensieren zu können, müssen entsprechende Sicherheitsmaßnahmen nach dem Stand der Technik eingesetzt werden. Gemäß des derzeitigen Entwurfs des Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – EGovG, siehe [EGovG-RE]) wird die Einhaltung des Standes der Technik vermutet, wenn beim ersetzenden Scannen die in der TR-RESISCAN spezifizierten Anforderungen erfüllt werden (siehe § 7 EGovG (Übertragen und Vernichten des Papieroriginals)) und die langfristige Aufbewahrung qualifiziert signierter Dokumente mit einem TR-ESOR-konformen System (siehe § 6 EGovG (Elektronische Aktenführung)) erfolgt. Vor diesem Hintergrund können interessierte Parteien ab Herbst 2012 in den Prozess der Konformitätsprüfung gemäß [BSI-TR-03125] bzw. [BSI-TR-RESISCAN] eintreten.

Literatur

[ArchiSafe] Physikalisch-Technische Bundesanstalt: *ArchiSafe-Webseite,* siehe unter http://www.archisafe.de

[BSI-100-2] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-2: *IT-Grundschutz-Vorgehensweise*

[BSI-100-3] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-3: *Risikoanalyse auf der Basis von IT-Grundschutz*

[BSI-GSKat] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Kataloge*, 2011

[BSI-IT-SiHB] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik*, 1992

[BSI-PP-0049] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents (ACM_PP)*, Version 1.0., https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0049, 2008

[BSI-TR-03112] Bundesamt für Sicherheit in der Informationstechnik (BSI): *eCard-API-Framework*, Version 1.1.2, TR-03112, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html, 2012

[BSI-TR-03125] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR)*, TR 03125, Version 1.1, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html, 2011.

[BSI-TR-03125-B] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage B zu [BSI-TR-03125], Profilierung für Bundesbehörden*, 2011

[BSI-TR-03125-C.1] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage C.1 zu [BSI-TR-03125], Conformity Test Specification (Level 1 – Functional Conformity)*, geplant für 2012

[BSI-TR-03125-C.2] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage C.2 zu [BSI-TR-03125], Conformity Test Specification (Level 2 – Technical Conformity)*, geplant für 2012

[BSI-TR-03125-E] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage E zu [BSI-TR-03125]: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks*, TR 03125 Version 1.1, 2011

[BSI-TR-03125-F] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage F zu [BSI-TR-03125], Formate und Protokolle*, 2011

[BSI-TR-RESISCAN] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Rechtssicheres ersetzendes Scannen (TR-RESISCAN)*, Version 1.0 geplant für Oktober 2012

[EGovG-RE] Referentenentwurf der Bundesregierung: *Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften*, Bearbeitungsstand 16.03.2012, über http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_EGov.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

[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

[Merk80] R. Merkle: *Protocols for Public Key Cryptosystems*, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA), SS. 122-134, 1980

[OASIS-DSS] OASIS: *Digital Signature Service Core, Protocols, Elements, and Bindings*, Version 1.0, http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html, 2007

[RFC3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato: *Internet X.509 Public Key Infrastructure – Time-Stamp Protocol (TSP)*, IETF RFC 3161, http://www.ietf.org/rfc/rfc3161.txt, 2001

[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 Evidence Record Syntax (XMLERS)*, IETF RFC 6283, http://www.ietf.org/rfc/rfc6283.txt, Juli 2011.

[RoSc06] A. Rossnagel, P. Schmücker (Hrsg.): *Beweiskräftige elektronische Archivierung. Ergebnisse des Forschungsprojektes „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“*, Economica Verlag, 2006

[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, http://www.ftvi.de/

[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