Bundesamt für Sicherheit in der Informationstechnik

Bundespolizei

Bundeskriminalamt

Technische Richtlinie TR-03135

Maschinell gestützte Dokumentenprüfung in hoheitlichen Kontrollinfrastrukturen

Technische Richtlinie des Bundesamts für Sicherheit in der Informationstechnik in Zusammenarbeit mit dem Bundespolizeipräsidium und dem Bundeskriminalamt

Version 1.2.1

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: tr-03135@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Mit Einführung des elektronischen Reisepasses (ePass), des elektronischen Personalausweises (nPA) und des elektronischen Aufenthaltstitels (eAT) steht eine Familie an hoheitlichen maschinenlesbaren Dokumenten zur Verfügung (eMRTD), die mit dem integrierten Chip eine maschinell gestützte Dokumentenprüfung in hoheitlichen Kontrollinfrastrukturen sowie die Verknüpfung zwischen Dokument und Inhaber ermöglicht. Der im Dokument integrierte Chip ist in diesem Kontext ein weiteres Sicherheitsmerkmal zur Erhöhung der Fälschungssicherheit.

Inhalt dieser Technischen Richtlinie (TR) ist die Beschreibung der notwendigen Anforderungen und Abläufe, die in einer maschinell gestützten Dokumentenprüfung in hoheitlichen Kontrollinfrastrukturen erforderlich sind. Die Prüfung hoheitlicher Dokumente zielt dabei nicht alleine auf die elektronischen Komponenten moderner e-Dokumente, sondern auch auf die Prüfung optisch-physikalischer Sicherheitsmerkmale der Dokumente ab. Letztere kann auch losgelöst von der Chip-Prüfung eines elektronischen Reisedokuments erfolgen, beispielsweise dann, wenn der auf dem Dokument aufgebrachte Chip einen Defekt aufweist und sich nicht auslesen lässt bzw. auch dann, wenn das jeweilige Einsatzszenario unter Umständen keine elektronische Prüfung vorsieht. Analog ist abhängig vom Einsatzszenario aber auch eine rein elektronische Überprüfung der in das Dokument eingebrachten elektronischen Elemente möglich.

Obwohl die erwähnten elektronischen Dokumente über mehrere sog. MRTD-Anwendungen (Anwendungen für maschinenlesbare Reisedokumente) gemäß [TR-03110] (vgl. dort Kapitel 2) verfügen können, bezieht sich diese Technische Richtlinie (TR) nur auf die ePassport-Anwendung, welche für Dokumentenprüfungen relevant ist. International werden elektronisch lesbare Dokumente u. a. über „Machine Readable Travel Documents“ [ICAO9303], über die [FRONTEX] “Best Practice Technical Guidelines for Automated Border Control (ABC) Systems”, “Best Practice Operational Guidelines for Automated Border Control (ABC) Systems” sowie den „Technical Report on Machine Assisted Document Security Verification“ [ICAOMADSV] beschrieben.

Ein elektronisch lesbares Reisedokument verfügt in der Regel über eine Personaldatenseite, welche standardisierte, maschinenlesbare Bereiche mit biografischen Daten enthält und ggf. über einen elektronischen Chip. Dieser beinhaltet Informationen zum Dokumenteninhaber (z. B. Name, Geburtsdatum, aber auch biometrische Merkmale). Zusätzlich zu diesen maschinenlesbaren Bereichen verfügen viele Dokumente über spezielle optisch-physikalische Merkmale, die mittels entsprechender Bilderfassungstechnik erkannt und ausgewertet werden können. Diese Merkmale können ein zusätzliches Indiz für die Unverfälschtheit eines vorliegenden Dokuments sein oder aber zur Verknüpfung zwischen Dokument und Inhaber herangezogen werden.

Eine Dokumentenprüfung lässt sich in mehrere Prüfprozesse gliedern, dies sind die:

- **Optisch-physikalische Dokumentenprüfung:** Optische Prüfung der physikalischen Sicherheitsmerkmale des Dokuments (z. B. Sicherheitsmerkmale, spezielle Druckbildeigenschaften, aufhellerfreies Substrat, Hologramme etc.).
- **Elektronische Dokumentenprüfung:** Auslesen und Prüfen der elektronischen Sicherheitsmerkmale des integrierten Chips (z. B. Zugriffskontrolle, Integrität der Daten und Echtheit des Chips).
- **Kombiniert optisch-physikalische und elektronische Dokumentenprüfung**: Prüfung oder Vergleich anhand der optisch-physikalisch sowie elektronisch gelesenen Informationen (z. B. Vergleich der optisch gelesenen MRZ mit der gelesenen Datengruppe 1 aus dem Chip).

Typischerweise werden im Anschluss noch weitere Prüfungen durchgeführt. So beispielsweise

- Die biometrische Prüfung: Identitätsüberprüfung des Dokumenteninhabers anhand biometrischer Merkmale (z. B. Gesichtsbild, Fingerabdruckbilder), die bei Beantragung oder Ausstellen des hoheitlichen Dokuments initial aufgenommen wurden und als Referenzdatensatz für die direkte Prüfung mit den vor Ort aufgenommenen biometrischen Daten dienen.
- Anfragen in Auskunftssystemen: Automatisierter Fahndungsabgleich anhand der Personal- und Dokumentendaten (z. B. in INPOL, SIS).

Obwohl in einem vollständigen Kontrollprozess auch die Identitätsfeststellung des Inhabers notwendig ist, legt diese Technische Richtlinie den Schwerpunkt auf die Prüfung des Dokuments. Die Bindung des Inhabers zum Ausweisdokument erfolgt häufig durch den Abgleich biometrischer Merkmale (im Speziellen das Gesichtsbild und Fingerabdrücke) mit den im elektronischen Chip des Dokuments gespeicherten Merkmalen. Außerdem können auch optisch personalisierte Merkmale wie Lichtbild oder Unterschrift herangezogen werden. Eine Prüfung der biometrischen Merkmale kann manuell durch die zuständige Behörde oder mit Hilfe von automatisierten Systemen erfolgen. Anforderungen an derartige Prüfungen und Formate der Protokollierung sind in [TR-03121] („Biometrics in public sector applications“) festgelegt.

1.1 Aufbau des Dokuments

Die verschiedenen Anwendungsszenarien für maschinell gestützte Dokumentenprüfungen in hoheitlichen Kontrollinfrastrukturen und deren spezielle Anforderungen sind in Kapitel 2 beschrieben. Kapitel 3 stellt die grundlegende Architektur von Dokumentenprüfsystemen und deren Prozesse dar. Anforderungen an die Dokumentenlesegeräte sind in Kapitel 4 formuliert, während in Kapitel 5 der Umfang der eigentlichen Dokumentenprüfung inkl. dem Inspektionssystem spezifiziert ist. Kapitel 6 definiert die Inhalte und das Format der Protokollierung des Dokumentenprüfungsprozesses. Kapitel 7 beschreibt die Sende- und Empfangsspezifikation zur Übertragung von XML-Dokumenten gemäß der in Kapitel 6 definierten Protokollierung. In Kapitel 8 sind die Konformitätsanforderungen definiert. Nach Abkürzungs- und Literaturverzeichnis (Kapitel 9 und 10) enthält Kapitel 11 als Anhang A eine exemplarische Umsetzung des Kommunikationsablaufs aller im Dokumentenkontrollprozess beteiligten Komponenten. Anhang B in Kapitel 12 listet die gegenwärtig in der EU verfügbaren Dokumente und deren unterstützte Protokollabläufe auf.

1.2 Terminologie

Die Schlüsselworte „MUSS”, „DARF NICHT“, „ERFORDERLICH“, „SOLLTE“, „SOLLTE NICHT“, „EMPFOHLEN“, „NICHT EMPFOHLEN“, „KANN“ und „OPTIONAL“ in diesem Dokument sind wie die englischen Pendants aus [RFC2119] zu verstehen.

In der folgenden Tabelle sind die in diesem Dokument verwendeten Schlüsselworte und deren Interpretation aufgelistet:

Schlüsselworte	***Interpretation der Schlüsselworte***
MUSS, DARF NICHT, ERFORDERLICH, NORMATIV	Die Anforderungen sind verpflichtend umzusetzen.
EMPFOHLEN, NICHT EMPFOHLEN, SOLLTE, SOLLTE NICHT	Bei den Anforderungen handelt es sich um Empfehlungen. Eine Abweichung hiervon ist stets fachlich zu begründen.
KANN, OPTIONAL	Die Anforderungen sind nicht verpflichtend, können aber optional umgesetzt werden.

Tabelle 1: Interpretation der Schlüsselworte

1.3 Fachbegriffe

Englischsprachige Begriffe wurden der Übersichtlichkeit wegen NICHT ins Deutsche übersetzt. Im Glossar, ab Seite 82, finden sich für die einzelnen Fachbegriffe kurze Erläuterungen auf Deutsch.

2 Anwendungsszenarien

Je nach Anwendungsszenario ergeben sich unterschiedliche Anforderungen an die Prüfung der Dokumente und die dafür einzusetzenden Komponenten. Folgende Anwendungsszenarien werden im Rahmen dieser Technische Richtlinie unterschieden:

- **Stationärer Einsatz:**
  Stationäre Systeme, die dauerhaft an Grenzübergängen, in Polizeidienststellen und an gefährdeten Objekten (z. B. an Einlasskontrollstellen der Verfassungsorgane, Ministerien oder Botschaften) angebracht sind, sowie zeitlich befristete Systeme an entsprechend vorbereiteten Einsatzorten (z. B. bei Großereignissen wie Sport- oder Musikveranstaltungen).
- **Einsatz in Self-Service-Systemen:**
  Stationäre Systeme, an denen eine automatisierte oder semi-automatisierte Dokumenten- und Personenkontrolle durchgeführt wird (z. B. sogenannte eGates/ABC-Systeme, automatisierte Grenzkontrollsysteme/-schleusen).
- **Teil-mobiler Einsatz:**
  Einsatz in Kontroll- oder Befehlsstellen- sowie Streifen- oder Wasserfahrzeugen. Der Aufbau der Systeme ist je nach Einsatzzweck unterschiedlich. Hierunter fallen beispielsweise sogenannte IT-Koffer oder tragbare PC-Stationen im Größenumfang eines Notebooks mit für den maschinell gestützten Kontrollprozess notwendigem Zubehör. Diese Systeme verfügen beispielsweise über ein Swipe- oder Full-Page-Lesegerät, um die MRZ einlesen zu können, sowie über ein RFID-Lesemodul zum Auslesen des Chips eines elektronischen Ausweisdokuments.
- **Voll-mobiler Einsatz:**
  Mobiler Einsatz bei Kontrollen im Bahn-, Luft- und Schiffsverkehr sowie im allgemeinen Streifendienst. Die Systeme werden durch den Beamten mitgeführt. Die verwendeten Geräte entsprechen in Größe und Bauform im Wesentlichen einem Smartphone oder Tablet-PC.

In allen Anwendungsfällen, bei denen eine Online-Verbindung gewährleistet werden kann, MUSS diese auch genutzt werden. In Fällen, in denen dies nicht möglich ist, werden alternative Möglichkeiten benötigt, diese sind nicht im Begegnungsbereich der vorliegenden TR.

Unbenommen davon ist eine lokale Prüfung auch ohne ständige Online-Verbindung möglich. Es bleibt dann jedoch zu beachten, dass unter Umständen nicht alle elektronischen Sicherheitselemente des Dokuments zweifelsfrei bestimmt, ausgelesen oder verifiziert werden können.

Neben den Anwendungsszenarien können die jeweiligen Anforderungen an eine durchzuführende Prüfung

1. verpflichtend **(v)**,
2. optional **(o)** oder
3. evaluierungsbedingt **(e)**

sein.

Verpflichtende Anforderungen MÜSSEN stets durchgeführt werden, optionale Anforderungen können wahlfrei durchgeführt werden, während evaluierungsbedingte Anforderungen zwar durchgeführt und protokolliert werden, allerdings NICHT direkt in das jeweilige Teilprüfergebnis einer hoheitlichen Dokumentenprüfung eingehen.

Optional definierte Anforderungen müssen nicht notwendigerweise implementiert und durchgeführt werden. Wenn sie allerdings in einem Prüfprozess ausgeführt werden, MÜSSEN die ermittelten Prüfergebnisse zwingend in das Endergebnis einfließen.

Anders bei den evaluierungsbedingten Anforderungen: Die Ergebnisse solcher Prüfungen gehen NICHT in das zu bestimmende Endergebnis einer hoheitlichen Dokumentenprüfung ein, sondern werden ausschließlich im Protokoll für nachgelagerte Auswertungen hinterlegt.

Folgende Tabelle fasst durchzuführende Prüfungen und deren Ergebnisse nochmals kurz zusammen:

	Prüfung geht ein	***Prüfung nur evaluierungsbedingt***
Implementierung verpflichtend	v	-
Implementierung nicht verpflichtend, aber umgesetzt	o	e
Implementierung nicht umgesetzt	-	-

Tabelle 2: Anforderungen, Implementierung und Prüfergebnis

Unabhängig von der jeweiligen Anforderung MÜSSEN alle während eines Prüfprozesses ermittelten und bewertbaren Daten entsprechend dem Protokolldatenformat gespeichert werden. Weitere Informationen und Details hierzu finden sich in Kapitel 6 „Protokollierung“. Unter Umständen können die gespeicherten Daten personenbezogene Anteile beinhalten. Im konkreten Anwendungskontext SOLLTE daher gemeinsam mit dem zuständigen Datenschutzbeauftragten eine datenschutzrechtliche Würdigung der zu speichernden Daten vorgenommen werden.

Tabelle 3 stellt die Anforderungen an die Dokumentenprüfung im jeweiligen Anwendungsszenario dar. Eine spezifische Implementierung MUSS im Falle von Wahlmöglichkeiten eine geeignete Auswahl treffen.

Anforderungen	*Kapitel*	*Anwendungsszenario*			
		Stationärer Einsatz	Self-Service-Systeme	Teil-mobiler Einsatz	Voll-mobiler Einsatz
Dokumentenlesegeräte					
Dokumentenformate	4.1.1	v	v	v	v
Lesen der MRZ/CAN	4.1.2	v	v	v	v
Auflage und Handhabung des Dokuments auf einem Full-Page-Lesegerät	4.1.3	o	v	o	o
Kommunikationsanforderungen an das RF-Modul	4.1.4	v	v	v	v
Host-System-Schnittstelle	4.1.5	v	v	v	v
Anforderungen an das optische Lesesystem	4.1.6	v	v	o	o
Optische Lesegeschwindigkeit	4.2.1	v	v	o	o
Elektronische Lesegeschwindigkeit	4.2.2	v	v	v	v
Generelle Anforderungen an die Dokumentenprüfung					
Prozessablauf der Dokumentenprüfung	5.1	v	v	v	v
Behandlung von Fehlern	5.7	v	v	v	v
Optisch-physikalische Dokumentenprüfung[1]					
Serienidentifikation	5.3.1	o/e	o/e	o	o
Prüfung der MRZ-Konsistenz	5.3.2	v	v	v	v
Prüfung der Dokumentengültigkeit	5.3.3	v	v	v	v

1 Der Umfang der mit „v/o/e“ gekennzeichneten Prüfschritte der optisch-physikalischen Dokumentenprüfung kann in Teilen optional sein, wenn eine vollständig elektronische Prüfung bzgl. Integrität der vom Chip gelesenen Daten und die Echtheitsprüfung des Chips erfolgreich durchgeführt werden. Der Umfang der optionalen Prüfschritte MUSS in Abhängigkeit der Zuverlässigkeit der elektronischen und optischen Prüfergebnisse sowie den Erfordernissen des jeweiligen Kontrollszenarios entsprechend spezifisch für Dokumententyp, Serie und Ursprungsland angepasst werden können. Dies gilt insbesondere für die Musterverifikationen einschließlich der jeweiligen Schwellwerte.

Anforderungen	*Kapitel*	*Anwendungsszenario*			
		Stationärer Einsatz	Self-Service-Systeme	Teil-mobiler Einsatz	Voll-mobiler Einsatz
Prüfung der MRZ IR-Lesbarkeit	5.3.4	v	v	o	o
Prüfung der VIZ (Visual Inspection Zone) Lesbarkeit	5.3.5	v/o/e	v/o/e	o	o
Prüfung der UV-Helligkeit	5.3.6	v	v	o	o
MRZ/VIZ-Vergleich	5.3.7	o	o	o	o
Musterverifikation	5.3.8	v/o/e	v/o/e	o	o
Elektronische Dokumentenprüfung					
PKI-Architektur der elektronischen Dokumentenprüfung	5.4.1	v	v	v	v
Sequenz zum Lesen und Prüfen der elektronischen Inhalte	5.4.2	v	v	v	v
Aufbau eines sicheren Kommunikationskanals über BAC oder PACE	5.4.3.1	v	v	v	v
Prüfung der Chipechtheit (AA, CA)	5.4.4	v	v	v	v
Zugriffsprüfung mittels Terminal Authentication (TA)	5.4.3.2	v	v	v	v
Prüfung der elektronischen Daten (PA)	5.4.5	v	v	v	v
Verifikation der Sicherheitsobjekte	5.4.5.1	v	v	v	v
Prüfung der Ausstellerzertifikate	5.4.5.2	v	v	v	v
Verifikation der DS-Zertifikats-Signatur	5.4.5.2.1	v	v	v	v
Prüfung der Zertifikatsgültigkeitsdauer	5.4.5.2.2	v	v	v	v
Prüfung des Widerruf-Status des DS-Zertifikats	5.4.5.2.3	v	v	v	v

Anforderungen	*Kapitel*	*Anwendungsszenario*			
		Stationärer Einsatz	Self-Service-Systeme	Teil-mobiler Einsatz	Voll-mobiler Einsatz
Integrität der Chipinhalte	5.4.5.3	v	v	v	v
Vergleich der Inhalte von EF.SOD und EF.COM	5.4.5.3.1	v	v	v	v
Integritätsprüfung der Datengruppen	5.4.5.3.2	v	v	v	v
Vergleich der Ausstellerstaaten (DG1 und DS-Zertifikat)	5.4.5.4	v	v	v	v
Behandlung und Interpretation von Defekten	5.6	v	v	v	v
Kombiniert optisch-physikalische und elektronische Dokumentenprüfung					
Vergleich der optischen und elektronischen biografischen Daten (optische MRZ und DG1)	5.5.1	v	v	o	o
Protokollierung					
Schutz personenbezogener Daten	6.1	v	v	v	v
Transaktionsbasiertes Format für Prüfungen	6.2	v	v	v	v
Format für Dokumentenprüfungen	6.3	v	v	v	v
Format für biometrische Prüfungen	6.4	v	v	v	v
Format für Anfragen in Auskunftssystemen	6.5	o	v	o	o

Tabelle 3: Anforderungen an die Dokumentenprüfung

3 Maschinell gestützte Dokumentenprüfung

3.1 Grundlagen

Im Rahmen (grenz-)polizeilicher Kontrollen werden hoheitliche Dokumente zunehmend mit maschineller Unterstützung geprüft. Dies ermöglicht eine Prüfung dieser Dokumente auf Authentizität, Integrität sowie Gültigkeit und zusätzlich einen Abgleich mit Informationen aus Hintergrundsystemen.

Ein maschinell lesbares Dokument verfügt in der Regel über (wohldefinierte und standardisierte) erfassbare Informationseinheiten und -merkmale. Diese erfassbaren Informationseinheiten und -merkmale können beispielsweise optischer oder elektronischer Natur sein und durch entsprechende Erfassungstechnik gelesen, geprüft und zur weiteren Verarbeitung genutzt werden. International anerkannte Informationseinheiten und -merkmale auf Reisedokumenten erleichtern dabei die maschinelle Erfassung erheblich, vgl. hierzu [ICAO9303].

Vornehmlich beinhalten die zu erfassenden Informationseinheiten und -merkmale standardisierte biografische Informationen zum Dokumenteninhaber wie beispielsweise Name, Geburtsdatum, Nationalität, aber auch ein Lichtbild. Biometrische Informationseinheiten und -merkmale ermöglichen zusätzlich eine Verknüpfung zwischen Dokument und Inhaber. Kryptografische Informationseinheiten und -merkmale können zudem die Authentizität und Integrität der Daten bestätigen.

Neben diesen personenbezogenen Informationseinheiten und -merkmalen enthalten viele Dokumente auch weitergehende Informationen, die insbesondere als Indiz für die Authentizität und Integrität eines amtlichen Dokuments an sich herangezogen werden können. Diese Informationseinheiten und -merkmale sind häufig nicht standardisiert und können für eine bestimmte Serie von Ausweisdokumenten entsprechende Spezifika aufweisen. Anhand dieser speziellen Eigenschaften können sie katalogisiert werden und sind entsprechend maschinell erfass- und auswertbar.

Moderne hoheitliche Dokumente verfügen in der Regel über eine Kombination aus

- optisch-physikalischen und
- elektronischen (digitalen)

Einheiten (Merkmalen), die mit geeigneter Erfassungstechnik verarbeitet werden können.

Im Rahmen einer maschinell gestützten Dokumentprüfung werden diese von einem **Dokumentenlesegerät** entsprechend ihrer jeweiligen Ausprägung erfasst und in einer **Kontrollanwendung** weiter verarbeitet. So können beispielsweise die physikalischen Eigenschaften des Dokuments optisch erfasst und maschinell weiterverarbeitet werden. Bei Dokumenten mit elektronischen Komponenten können die digitalen Eigenschaften (Speicherinhalte im Chip) des Dokuments elektronisch erfasst und ebenfalls zur weiteren maschinellen Verarbeitung genutzt werden. Dabei müssen die optisch-physikalischen und elektronischen Einheiten nicht notwendigerweise separat betrachtet und geprüft werden. So bestehen an manchen Stellen Überschneidungen, die in einer Prüfung von optisch-physikalischen wie auch elektronischen Merkmalen zugleich münden.

Es sei angemerkt, dass im Rahmen einer maschinell gestützten Dokumentenprüfung **nicht notwendigerweise alle** Informationseinheiten und -merkmale eines Dokuments erfasst und geprüft

werden müssen. Dies ist abhängig vom jeweiligen Einsatzszenario, dem jeweils vorliegenden Dokument und nicht zuletzt auch von der genutzten Erfassungstechnik und den Systemen zur weiteren Auswertung dieser Informationseinheiten und -merkmale.

3.1.1 Dokumentenlesegerät

Das Dokumentenlesegerät zeichnet die Informationseinheiten und -merkmale eines maschinell lesbaren hoheitlichen Dokuments entsprechend seiner jeweiligen Ausprägung auf. Das Dokumentenlesegerät übermittelt diese Daten dann an die Kontrollanwendung zur weiteren Verarbeitung.

3.1.2 Kontrollanwendung

Die Kontrollanwendung steuert einerseits den Einleseprozess des Dokumentenlesegeräts und verarbeitet anderseits die von ihm erfassten Informationen weiter. Die Kontrollanwendung ist in der Lage, das Dokumentenlesegerät entsprechend der jeweiligen Erfordernisse (Einsatzszenario und Ausprägung des zu lesenden Dokuments) zu konfigurieren und damit die durchzuführenden Erfassungsschritte aktiv zu überwachen und zu steuern. Wie die jeweilige Verarbeitung der erfassten Merkmale durchgeführt wird, hängt von den jeweiligen Erfordernissen an das Einsatzszenario als auch von der Ausprägung des Dokuments ab.

Die Kontrollanwendung kann aus mehreren Prozessen bestehen, die unabhängig voneinander agieren können. Es ist sicherzustellen, dass die ermittelten Daten sowohl lokal als auch in einem Serversystem weiterverarbeitet werden können. Hierbei ist grundsätzlich ein entsprechender Schutz der IT-Architektur und Datensicherheit zu realisieren. Die genaue IT-Sicherheitsarchitektur der Kontrollanwendung ist nicht Gegenstand dieser TR.

3.2 Prüfprozesse und Prüfergebnisse

Im Rahmen (grenz-)polizeilicher Kontrollen werden amtliche Dokumente einer Prüfung unterzogen. Kern dieser Prüfung ist, festzustellen, ob das vorliegende Dokument

- authentisch (d. h. echt, vom Aussteller stammend),
- integer (unmanipuliert) und
- gültig (z. B. nicht abgelaufen, als verloren/gestohlen verzeichnet, kein Fantasiedokument, hoheitlich anerkannt)

ist.

Diese Prüfung kann auf das gesamte Dokument oder Teilbereiche des Dokuments angewendet werden und bezieht sich auf die optisch-physikalischen oder elektronischen Merkmale des Dokuments. Die einzelnen Prüfungen werden in sog. Prüfprozessen organisiert.

In den einzelnen Prüfprozessen kann beispielsweise geprüft werden, ob das zu prüfende Dokument im IR-Lichtwellenlängenbereich lesbar ist oder unter UV-Beleuchtung definierte Muster aufweist. Die Gültigkeit des Dokuments kann beispielsweise über den Gültigkeitswert der MRZ bestimmt werden. Eine Abfrage in Hintergrundsystemen kann feststellen, ob das Dokument als verloren/gestohlen gekennzeichnet ist. Von den Datengruppen des Chips können Prüfsummen berechnet werden, diese wiederum können mit den digital signierten Prüfsummen des Chips auf Authentizität und Integrität geprüft werden. Außerdem kann eine Plausibilitätsprüfung zwischen

den optisch-physikalischen Werten und den korrespondierenden Werten im Chip (z. B. MRZ) durchgeführt werden.

Um Nachvollziehbarkeit- und Prüfbarkeit zu garantieren, müssen die einzelnen Prüfprozesse stets zu wohldefinierten und nachkontrollierbaren Ergebnissen führen. Eine einzelne Prüfung (d. h. ein einzelner Prüfprozess) wird entweder

- vollständig entsprechend seines Algorithmus abgearbeitet, bis er terminiert, und liefert im Sinne der durch ihn repräsentierten Prüfung ein wohldefiniertes Ergebnis zurück, oder
- er wird vorzeitig abgebrochen und liefert für die durch ihn repräsentierte Prüfung kein Ergebnis für die (grenz-)polizeiliche Kontrolle zurück.

Ob und welche Prüfprozesse im Einzelnen letztlich durchgeführt werden, ist abhängig vom jeweiligen Einsatzszenario und den darin festgelegten Arbeitseinheiten, die im Sinne der für sie definierten **vollständigen Prüfung** hoheitlicher Dokumente vorgegeben sind.

In der Regel werden die Einzelprüfungen am Ende des gesamten Prüfprozesses zu einem Gesamtergebnis kumuliert, welches die Grundlage für eine abschließende Bewertung der jeweiligen (grenz-)polizeilichen Kontrolle bildet.

3.2.1 Der Prüfprozess

Unter einem Prüfprozess wird im Rahmen dieses Dokuments formal (architektonisch) der organisierte und gerichtete Ablauf einer Prüfung verstanden. Dieser legt fest, was im Rahmen seiner Prüfung zu erfassen, messen und kontrollieren ist und zu welchen Ergebnissen die Prüfung dieses Prozesses kommen kann. Der Prüfprozess stellt im Sinne dieser Technischen Richtlinie eine abstrakte/architektonische Größe dar und definiert nicht, wie eine Prüfung letztlich (software-)technisch umzusetzen ist – die Beschreibung der Ausgestaltung eines Prozesses, seiner Ein- und Ausgabewerte sowie das Verhalten sind nicht Bestandteil dieser Technischen Richtlinie.

Ein Prüfprozess P beschreibt formal den Ablauf kausaler Zustandsübergänge zu Zeitpunkten t_1 , … t_i, …., t_E, also dem Ablauf des Prüfgeschehens vom Anfang (t_1) bis Ende (t_E). Ein Prüfprozess ist dabei eine Folge von deterministischen Zustandsübergängen [(Z_i) → (Z_{i+1})] vom Zustand (Z_i) nach Zustand (Z_{i+1}), bei dem jeder Zustand ursächlich von anderen, zeitlich vorangegangenen Zuständen abhängig ist und von diesen eindeutig bestimmt wird.

Für einen Prüfprozess ergeben sich im Kontext der Dokumentenprüfung ausschließlich die folgenden globalen Zustände:

1. initiiert

   Der Prüfprozess wurde noch nicht gestartet (ausgeführt), es hat noch keine Aktivität stattgefunden. Der Prozess befindet sich in $Z_{\{\}}$ (im Leerlauf).

2. laufend

   Der Prüfprozess befindet sich zum Zeitpunkt t im Zustand Z_t und wird in diesem ausgeführt.

3. terminiert

   Der Prüfprozess wurde für die durch ihn definierte Prüfung bis zum deterministischen Ende (Zeitpunkt t_E) seines Lebenszyklus mit Endzustand Z_{t_E} ausgeführt. Er liefert für die durch ihn ausgeführte Prüfung ein Ergebnis (vgl. hierzu Abschnitt 3.2.2).

4. abgebrochen

   Der Prüfprozess wurde vor seinem definierten Ende zum Zeitpunkt t_X des Lebenszyklus mit Zustand Z_{t_X} abgebrochen. Der Prüfprozess konnte eine vorgesehene Prüfung nicht bis zum Ende ausführen und liefert demnach kein für die Bewertung nutzbares Ergebnis.

Die Ergebnismenge eines Prüfprozesses kann dann und nur dann als verbindliche Grundlage für die Bestimmung der Authentizität, Integrität und Gültigkeit herangezogen werden, wenn der Prozess bis zum Ende (terminiert zum Zeitpunkt t_E, Zustand Z_{t_E}) ausgeführt wurde. Das Ergebnis eines vollständig bis zum Ende ausgeführten Prüfprozesses kann selbst wieder Grundlage eines anderen Prozesses sein.

Fehler bei der Bedienung, in der Hardware oder Software können zu einem vorzeitigen Abbruch des Prozesses in einem zum Zeitpunkt t_X vorliegenden Zustand Z_{t_X} führen (d. h. abgebrochen). Um die Nachvollziehbarkeit und Prüfbarkeit eines Prüfprozesses zu garantieren, dürfen ausschließlich die Informationen des Endzustands Z_{t_E} genutzt werden. Informationen eines abgebrochenen Prozesses dürfen allenfalls in einem Protokoll für eine Analyse im Rahmen der Qualitätssicherung festgehalten und genutzt werden, eine Grundlage für die abschließende Bewertung der jeweiligen (grenz-)polizeilichen Kontrolle dürfen diese Werte allerdings **nicht** bilden.

3.2.2 Prüfergebnisse

Ein vollständig durchgeführter Prüfprozess (terminiert zum Zeitpunkt t_E, Zustand Z_{t_E}) liefert für die weitere Verarbeitung entsprechende Prüfergebnisse. Bei einer Prüfung muss es sich nicht zwangsläufig um die reine Prüfung von optisch-physikalischen bzw. elektronischen Merkmalen auf dem Dokument handeln, sondern auch um die erfolgreiche Durchführung von Chipkommunikations- und Zugriffsprotokollen, die ein Prüfsystem erfolgreich auf einem bestimmten Dokument ausführen können muss (z. B. Protokolle wie BAC, PACE oder TA).[2]

Ein Prüfergebnis eines Prüfprozesses besitzt genau einen der folgenden Zustände:

1. erfolgreich (bestanden, *engl. successful*)

   Im Rahmen der Prüfung hat der zu prüfende Teil des Dokuments erfolgreich bestanden, d. h. eine bestimmte Prüfung konnte auf das Dokument angewendet und nach entsprechenden Vorgaben bewertet werden.

2. fehlgeschlagen (nicht bestanden, *engl. failed*)

   Im Rahmen der Prüfung hat der zu prüfende Teil des Dokuments die Prüfung NICHT erfolgreich bestanden, sprich die Prüfung ist fehlgeschlagen. Das Dokument SOLLTE einer weiterführenden (manuellen) Kontrolle bzgl. Authentizität, Integrität und Gültigkeit unterzogen werden.

3. unbestimmt (*engl. undetermined*)

   Es konnte im Rahmen der Prüfung nicht (eindeutig) bestimmt werden, ob der zu prüfende Bereich des Dokuments authentisch, integer oder gültig ist.

   Abgebrochene Prüfungen haben ebenfalls das Prüfergebnis unbestimmt.

2 Ein Scheitern bzw. die fehlende Unterstützung eines bestimmten Protokolls lässt ggf. ebenfalls Rückschlüsse bzgl. der Authentizität, Integrität und Gültigkeit des Dokuments zu.

4. nicht unterstützt (*engl. not supported*)

   Das spezifische Dokument unterstützt die zu prüfenden Einheiten nicht (beispielsweise ein Dokument ohne Chip, ein Dokument, das bestimmte Sicherheitsmerkmale per Definition nicht aufweist, nicht unterstütztes Protokoll etc.).

5. nicht durchgeführt (*engl. not performed*)

   Die Prüfung wurde nicht durchgeführt. Dieses Ergebnis ist anzuwenden, wenn eine bestimmte Prüfung in der Prüfumgebung niemals durchgeführt wird, weil beispielsweise die technischen Voraussetzungen nicht gegeben sind oder weil die Prüfung im vorliegenden Fall grundsätzlich deaktiviert oder nicht implementiert wurde.

An den Zustand des Prüfergebnisses werden unter Umständen weitere Informationen (Daten) augmentiert (angeheftet), die für eine weiterführende Ver- oder Bearbeitung notwendig sind. Ein Prüfergebnis kann mitsamt seiner angehängten Daten in weiteren Prüfprozessen oder für das kumulierte Endergebnis genutzt werden. Das Gesamtergebnis der Dokumentenprüfung MUSS entsprechend den oben angeführten Werten dargestellt werden.

3.3 Optisch-physikalische Dokumentenprüfung

Bei der optisch-physikalischen Dokumentenprüfung werden physikalische Eigenschaften des Dokuments optisch erfasst und an die Kontrollanwendung zur weiteren Verarbeitung übermittelt.

Die optische Prüfung der physikalischen Sicherheitsmerkmale des Dokuments beinhaltet meist die Prüfung spezieller Druckbildeigenschaften, die Prüfung auf aufhellerfreies Substrat und weiterer Eigenschaften, durch Aufnahme der Bilder unter Beleuchtung in unterschiedlichen Wellenlängenbereichen wie beispielsweise Weißlicht-, UV- und IR-Beleuchtung.

Neben der optischen Prüfung physikalischer Eigenschaften des Dokuments müssen auch maschinell lesbare Bereiche verarbeitet werden. Hierzu zählt insbesondere die sog. maschinenlesbare Zone (MRZ). Der Inhalt der MRZ ist durch [ICAO9303] standardisiert, sodass sich die MRZ maschinell auf Korrektheit und Konsistenz prüfen lässt.

Abhängig von der Art des Reisedokuments befindet sich die maschinenlesbare Zone (MRZ) und das Lichtbild auf der gleichen oder auf unterschiedlichen Seiten des Dokuments. So besitzt beispielsweise ein Reisepass eine Personaldatenseite mit Lichtbild und MRZ. TD1-Karten (z. B. der neue elektronische Personalausweis) weisen dagegen auf der Vorderseite nur biografische Daten und das Lichtbild auf, während sich die MRZ auf der Rückseite befindet. D. h., dass bei einer maschinell durchgeführten optisch-physikalischen Dokumentenprüfung auch automatisiert erkannt werden muss, welcher Dokumententyp vorliegt, um diesen seiner Spezifika entsprechend vollständig prüfen zu können.

3.4 Elektronische Dokumentenprüfung

Durch Verwendung von Mikroelektronik werden traditionelle Identitätsdokumente zu elektronisch gestützten Ausweisdokumenten. Der integrierte „Radio Frequency“-Chip (RF-Chip) nimmt dabei die personenbezogenen Daten wie z. B. Name, Geburtsdatum sowie biometrische Merkmale des Ausweisinhabers auf. Dazu werden die digitalen Eigenschaften (Speicherinhalte im Chip) elektronisch erfasst und an die Kontrollanwendung zur weiteren Verarbeitung übermittelt. Die

unterschiedlichen auf dem Identitätsdokument gespeicherten Informationen werden dazu in sog. Anwendungen organisiert, vgl. [TR-03127][3].

Bei der elektronischen Dokumentenprüfung werden die auf dem Chip gespeicherten Daten unter anderem durch starke kryptografische Verfahren auf Authentizität und Integrität geprüft. Über technische Sicherungsmaßnahmen in Kombination mit standardisierten Public-Key-Infrastrukturen wird einerseits der Zugriff auf die im Chip gespeicherten Informationen geregelt (BAC, PACE sowie EAC) und andererseits die auf dem Chip gespeicherten Daten auf Integrität und Authentizität geprüft. Die im Rahmen dieses Dokuments als verwendet angenommenen PKI-Infrastrukturen sind die ICAO PKI und die EAC PKI.

Sofern die Daten dann als authentisch, integer und gültig bewertet werden, kann die elektronische Komponente des Ausweisdokuments anerkannt werden und die auf ihr gespeicherten Daten können in weiterführenden Prüfschritten genutzt werden. Hierzu zählt insbesondere der Abgleich/Vergleich der biografischen Chip-Daten mit den optisch erfassten Daten des Dokuments sowie in weiteren Schritten ggf. ein biometrischer Abgleich mit der Person, die das Ausweisdokument bei der Prüfung als Identitätsnachweis vorgelegt hat oder eine Abfrage bzgl. der Daten in Hintergrundsystemen.

3.5 Kombiniert optisch-physikalische und elektronische Dokumentenprüfung

Die kombiniert optisch-physikalische und elektronische Dokumentenprüfung stellt eine Mischform der Dokumentenprüfung aus den Abschnitten 3.3 und 3.4 dar. Hierbei handelt es sich um hybride Prüfungen, die einerseits optisch-physikalische Merkmale als auch elektronische Merkmale für ihre Prüfung benötigen.

Ein Beispiel hierfür ist der Vergleich der optisch-physikalisch lesbaren MRZ und der MRZ aus der Datengruppe 1 (DG1) des Chips. Eine weitere Möglichkeit besteht z. B. im Vergleich des auf der Ausweisdatenseite aufgedruckten Gesichtsbildes mit dem im Chip auf DG2 gespeicherten Gesichtsbild.

3 Im Kontext hoheitlicher Kontrollen sind zusätzliche Funktionalitäten eines Ausweisdokuments wie die eSign-Anwendung nicht von Interesse und werden in diesem Dokument nicht weiter betrachtet.

4 Dokumentenlesegeräte

In Abhängigkeit des Anwendungsszenarios können unterschiedliche Anforderungen an die Dokumentenlesegeräte entstehen. In bestimmten Anwendungsszenarien reicht das Lesen des Dokuments unter Beleuchtung im sichtbaren Lichtwellenlängenbereich allein nicht aus (Prüfung der Dokumentenechtheit oder -version), sodass die zu verwendenden Lesegeräte dann in der Lage sein müssen, die Dokumente in anderen Lichtwellenlängenbereichen zu beleuchten (beispielsweise IR oder UV) um diese optisch-physikalisch zu erfassen. Dabei muss das Dokument optisch nicht immer ganzheitlich erfasst werden. Abhängig vom Einsatzszenario oder der verwendeten Hardware können ggf. auch nur Teilbereiche eines Dokuments (beispielsweise nur die MRZ bei Verwendung eines sog. Swipe-Lesegeräts) optisch erfasst und weiterverarbeitet werden.

4.1 Technische Anforderungen

4.1.1 Dokumentenformate

Das vollformatige (Full-Page-)Lesegerät MUSS die in [ICAO9303] spezifizierten Formgrößen und Formate für hoheitliche Dokumente unterstützen. Dies sind Dokumente in den Formgrößen TD-1, TD-2 und TD-3 (beispielsweise dreizeilige MRZ mit jeweils 30 Zeichen pro Zeile, zweizeilige MRZ mit jeweils 36 Zeichen pro Zeile oder die zweizeilige MRZ mit jeweils 44 Zeichen) sowie maschinell lesbare Visa in den Formaten MRV1 und MRV2[4].

4.1.2 Lesen der MRZ/CAN

Das Dokumentenlesegerät MUSS das automatisierte Lesen der maschinenlesbaren Zone (MRZ) gemäß Definition in [ICAO9303] unterstützen. Das Dokumentenlesegerät MUSS Bilder im Nah-Infrarotlicht (B900-Band (900 +/- 50) nm) und SOLLTE Bilder im sichtbaren Wellenlängenbereich aufnehmen. Für weiterführende Informationen siehe [ISO1831]. Ergänzend dazu SOLLTE ein Dokumentenlesegerät die Anforderungen an MRTDs zur Sicherstellung der Lesbarkeit der MRZ berücksichtigen.

Sofern ein Full-Page-Lesegerät verwendet wird, MUSS dieses Lesegerät auch das automatisierte Lesen der sechsstelligen *Card Access Number* (CAN) unterstützen. Es wird EMPFOHLEN, dass auch sog. *Swipe*-Leser das automatisierte Lesen der CAN unterstützen.

4 Das Dokumentenlesegerät MUSS in der Lage sein, auch Dokumente, deren Einband die Datenseite nach allen Seiten um bis zu 5mm überragt, verarbeiten zu können. Dies gilt insbesondere für den Reisepass aus Deutschland.

4.1.3 Auflage und Handhabung des Dokuments auf einem Full-Page-Lesegerät

Die Dokumente MÜSSEN auf das Dokumentenlesegerät (hier Full-Page-Lesegerät) gelegt werden

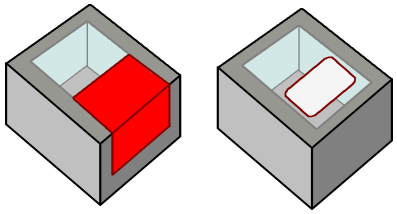

Abbildung 1: Beispiel für die Auflage eines Reisepasses und einer ID-Karte auf einem exemplarischen Dokumentenlesegerät

können, sodass die personalisierte Datenseite in ihrer Gesamtheit optisch erfasst werden kann. Bauartbedingt KANN ein Dokumentenlesegerät so beschaffen sein, dass ein Streifen von höchstens 5mm entlang der Bindung nicht erfasst wird. Es ist zulässig, andere Technologien als die der Erstellung eines Kamerabildes eines auf eine Dokumentenauflage aufgelegten Dokuments zu verwenden, wenn die in dieser Technische Richtlinie gestellten Anforderungen an die erfassten Daten erfüllt werden.

Die MRZ oder die CAN liegen in Richtung des Dokumentenlesegeräts. Abbildung 1 veranschaulicht beispielhaft die mögliche Auflage eines elektronischen Reisepasses sowie einer ID-Karte auf einem Dokumentenlesegerät:

Die Bilderfassungstechnik des Lesegeräts kann dann die MRZ-Datenseite erfassen und weiterführende Prüfschritte starten. Das elektronische Lesen des Dokuments kann beginnen, sobald die MRZ oder die CAN nach dem optischen Lese- und Analyseprozess des Full-Page-Lesegeräts vorliegen.

Das Lesegerät MUSS eine erleichterte Handhabung sowohl für Rechts- als auch Linkshänder gewährleisten, sowie die Nutzung von Dokumenten mit unterschiedlichen Personaldatenseiten ermöglichen. Für die komfortable und erleichterte Handhabung kann das Lesegerät optional über einen animierten Anzeigebereich verfügen, welcher die Bedienung des Geräts in einem Video oder in Form einer Animation veranschaulicht. Alternativ wäre es hier auch möglich, das vom optisch-physikalischen Lesemodul aktuell aufgenommene Bild (sog. Live-Aufnahme) für den Anwender visualisiert darzustellen, ggf. mit optischen Hinweisen bzw. Hilfslinien zum Sollzustand eines optimal und korrekt aufgelegten Dokuments.

Das Dokumentenlesegerät MUSS auch elektronische Reisedokumente mit einer im Einband befindlichen elektrisch leitfähigen Abschirmung (sog. Shielding) auslesen können.

4.1.4 Kommunikationsanforderungen an das RF-Modul

Das RF-Modul MUSS die Anforderungen [ICAO9303] Kapitel 10 dem Lesertyp entsprechend erfüllen. Dieses Modul SOLLTE über PC/SC angesprochen werden können. Für den Dokumentenleser MÜSSEN die in [ISO18745-2] für den jeweiligen Gerätetyp spezifizierten Tests erfolgreich absolviert werden. Die folgenden in [ICAO9303] definierten optionalen Eigenschaften MÜSSEN unterstützt werden:

Ausprägung/Eigenschaft	*Definition/Basisstandard*	*Anforderungen*
eMRTD Lesegerät Typ (Full Page etc.)	ICAO9303	Muss vom Hersteller definiert werden.
Unterstützte Bitraten	ISO/IEC 14443-2:2010, ISO/IEC 14443-2:2010/Amd3:2012 ISO/IEC 14443-3:2011, ISO/IEC 14443-3:2011/Amd2:2012 ISO/IEC 14443-4:2008, ISO/IEC 14443-4:2008/Amd2:2012	Minimal: eMRTD Leser → eMRTD: 424kbit/s eMRTD → eMRTD Leser: 424kbit/s Optional: bis 6.8 Mbit/s, alle Kombinationen
Temperaturbereich		Muss von Hersteller definiert werden.
Z_{max} Readervolumen in mm	ICAO 9303	Min : 7.5 mm Max : Je nach Herstellerdeklaration des Lesegerättyps
Schnittstelle PC/SC	PC/SC Workgroup Spezifikation	Verpflichtend
EMD Unterstützung	ISO/IEC 14443-2:2010/Amd 1:2011 ISO/IEC 14443-3:2011/Amd 1:2011	Verpflichtend
Austausch weiterer Parameter	ISO/IEC 14443-4:2008/Amd 1:2011	Optional
Frame-Größe	ISO/IEC 14443-3: 2011 ISO/IEC 14443-3:2011/Amd2:2012 ISO/IEC 14443-4:2008/Amd2:2012	Minimal: eMRTD Leser → eMRTD: 256 Byte eMRTD → eMRTD Leser: 256 Byte

Tabelle 4: Minimale und optionale Anforderungen an die kontaktlose Schnittstelle von eMRTD Lesegeräten

4.1.5 Host-System-Schnittstelle

Wird das Dokumentenprüfsystem in mehrere Komponenten, wie z. B. Dokumentenlesegerät und Kontrollanwendungs-PC, partitioniert, SOLLEN die Verbindungsschnittstellen zwischen den Komponenten mittels standardisierter netzbasierter Technologien (derzeit z. B. Ethernet, Bluetooth, WiFi, USB, FireWire) Verwendung finden. Die zu realisierende Schnittstellengeschwindigkeit ergibt sich aufgrund der Anforderungen an die maximale Zeit des Auslese- und Prüfvorganges aus

den folgenden Kapiteln. Es wird die Verwendung von Technologien mit einer Brutto-Übertragungsrate von mindestens 400 Mbit/s EMPFOHLEN. Die Bildverarbeitung KANN auch in Teilen im Lesegerät durchgeführt werden. In einem solchen Fall ist es auch möglich, dass eine weniger performante Schnittstelle ausreichend ist.

4.1.6 Anforderungen an das optische Lesesystem

Das Dokumentenlesegerät, gemeint sind Full-Page-Lesegeräte, MUSS Bilder von der gelesenen Datenseite im Infrarotlicht (IR, im B900-Band, bei (900 +/- 50) nm, vgl. [ISO1831]), UV-A-Licht und sichtbaren Wellenlängenbereich aufnehmen können.

Umgebungslicht DARF die Qualität der Aufnahmen NICHT signifikant negativ beeinflussen, daher wird EMPFOHLEN, dass das Dokumentenlesegerät gegen einstrahlendes Umgebungslicht möglichst unempfindlich ist bzw. sich durch (technische) Schutzmaßnahmen abschirmen lässt.

Das Dokumentenlesegerät MUSS den existierenden Bestimmungen gemäß EMC und UV-A Lichtemission entsprechen.

Das Dokumentenprüfsystem MUSS alle Aufnahmen der Datenseite als Bilddateien in einem Abbildungsmaßstab von mindestens 385 ppi bereitstellen und die entsprechenden Aufnahmeparameter wie z. B. Abbildungsmaßstab, Länge und Höhe in diese Bilddateien standardkonform einfügen. Sämtliche Bilddateien MÜSSEN in den Formaten BMP und JPEG (komprimiert) bereitgestellt werden können, vergleiche hierzu [ISO10918-1]. Das Dekodieren für JPEG-Bilder unterschiedlicher Kompressionsfaktoren und Qualitätseinstellungen MÜSSEN durch den Anwender konfigurierbar sein.

4.2 Anforderungen an die Leistungsfähigkeit

4.2.1 Optische Lesegeschwindigkeit

Die optisch-physikalische Aufnahme und Bereitstellung der Bilder der Personaldatenseiten eines Reisepasses nach [ICAO9303] unter Beleuchtung in den unterschiedlichen Wellenlängenbereichen DARF auf einem gemäß der dokumentierten Herstelleranforderungen installierten Prüfsystem NICHT mehr als 7 Sekunden erfordern. Die extrahierte MRZ oder CAN MUSS dem System in weniger als 5 Sekunden nach Auflage des Dokuments (z. B. für eine Weiterverarbeitung in einer Anwendung, Hintergrundsystemen etc.) zur Verfügung stehen.

4.2.2 Elektronische Lesegeschwindigkeit

Das Lesen der elektronischen Daten (zumindest EF.COM, EF.SOD, DG1 und DG2) eines elektronischen Reisedokuments DARF NICHT länger als 7 Sekunden in Anspruch nehmen[5].

5 Referenzdokument für Messungen ist der deutsche Musterpass der Generation 2.

Das folgende Zeitleistendiagramm illustriert die Beziehung zwischen optisch-physikalischer Erfassung und dem elektronischen Lesen des Dokuments:

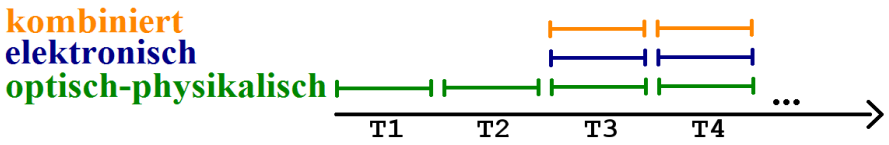

Abbildung 2: Zeitliche Beziehung optisch-physikalisch, elektronisch und kombiniert

Durch frühzeitiges Weiterreichen der MRZ/CAN-Daten an die Verarbeitungskomponente der elektronischen Prüfung kann die Gesamtdauer der Prüfung ggf. reduziert werden, da die elektronische Prüfkomponente bereits mit der elektronischen Prüfung des Dokuments beginnen kann, während die optisch-physikalische Prüfung noch läuft. Jeder Prozessschritt SOLLTE gestartet werden, sobald die für seinen Prozess zwingend notwendigen Eingangsdaten (z. B. MRZ oder CAN, Bilder der Datenseite, elektronische Datengruppen) vorhanden sind und die vorliegende Ausprägung eines Dokumentenprüfsystems ein solches Vorgehen nahelegt.

Es wird daher EMPFOHLEN, die Gesamtprüfzeit durch Parallelisierung, soweit sinnvoll und (technisch) möglich, zu reduzieren. Vgl. als mögliches Beispiel hierzu Tabelle 5:

Zeitpunkt	***Operation***
T_1	• optisch-physikalisches Erfassen des Dokuments
T_2	• Extrahieren der MRZ/CAN
T_3	• weitere optisch-physikalische Erfassungs- und Prüfschritte • Lesen von Daten aus dem Chip • Start der elektronischen Prüfung mit MRZ/CAN-Daten • Start der kombinierten optisch-physikalischen und elektronischen Prüfung
$T_{4, 5, \ldots n}$	• **weitere optisch-physikalische** Erfassungs- und Prüfschritte • **weitere elektronische** Erfassungs- und Prüfschritte • **weitere kombiniert optisch-physikalische und elektronische** Prüfschritte

Tabelle 5: Beziehung zwischen optischem und elektronischem Lesen eines Dokuments

5 Umfang der Dokumentenprüfung

5.1 Prozessablauf der Dokumentenprüfung

Formal existieren die folgenden Prozessschritte, die bei einer Dokumentenprüfung durchgeführt werden:

- Optisch-physikalisches Lesen des Dokuments
- Optisch-physikalisches Prüfen des Dokuments
- Elektronisches Lesen des Dokuments
- Elektronisches Prüfen des Dokuments
- Kombiniert optisch-physikalische und elektronische Dokumentenprüfung

Sobald die Informationen aus dem optisch-physikalischen und elektronischen Lesevorgang vorhanden sind, können die jeweiligen Prüfungen des Dokuments durchgeführt werden. Im Rahmen der kombiniert optisch-physikalischen und elektronischen Dokumentenprüfung werden die Eingangsdaten des optisch-physikalischen und elektronischen Lesevorgangs gleichermaßen für die Prüfung verwendet.

In Abbildung 3 ist der Prozessablauf der Dokumentenprüfung exemplarisch dargestellt:

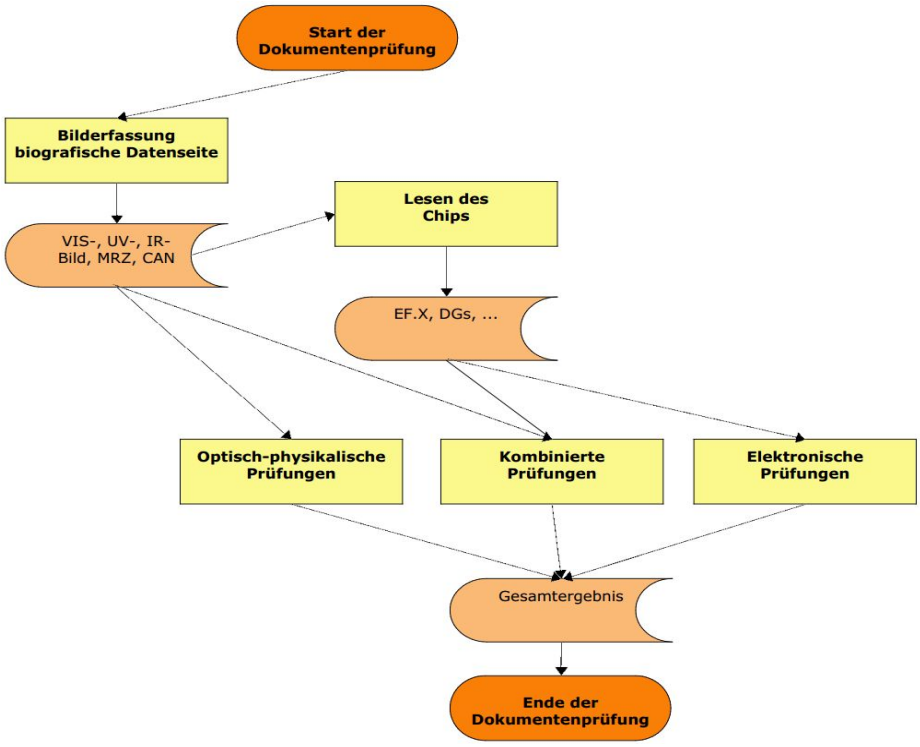

Abbildung 3: Prozessablauf der Dokumentenprüfung

Der Prozess beginnt mit dem optisch-physikalischen Lesen des Dokuments. In Abhängigkeit vom verwendeten Dokumentenlesegerät und entsprechenden Anwendungsszenarios werden die auf diese Weise gelesenen Informationen verarbeitet und ausgewertet (beispielsweise Musterverifikation,

Analyse und Erkennung von Sicherheitsmerkmalen)[6]. Basierend auf den erhaltenen Daten (Bilder der Personaldatenseite, MRZ oder CAN) wird eine Prüfung des Dokuments durchgeführt. Abschnitt 5.3 spezifiziert diese optisch-physikalischen Prüfungen.

Das elektronische Lesen des Dokuments kann beginnen, sobald die MRZ oder die CAN des Dokuments vorliegen oder sich ein RF-Tag im Feld des Lesegeräts befindet und dieses erkannt wird. Die Architektur, welche für das elektronische Auslesen des Dokuments gefordert ist, ist in 5.4.1 festgelegt. Im dargestellten Beispiel handelt es sich um ein Inspektionssystem, welches die zum elektronischen Auslesen des Dokuments notwendigen Protokolle (im Speziellen Terminal Authentication (TA) und Passive Authentication (PA) nach [TR-03110] und [ICAO9303]) anbietet. Der Ablauf für den elektronischen Zugriff auf die Datengruppen ist in Abschnitt 5.4.2 definiert. Die zusätzlichen elektronischen Prüfungen der Datengruppen, welche nach dem elektronischen Lesen des Dokuments durchgeführt werden müssen, sind in Abschnitt 5.4.5 definiert.

Sobald die optisch-physikalischen und elektronischen Daten für die kombiniert optisch-physikalische und elektronische Prüfung vorliegen, werden die dort definierten Prüfungen durchgeführt, vgl. hierzu Abschnitt 5.5.

Abhängig vom gewählten Einsatzszenario kann auf Anteile der optisch-physikalischen Prüfung verzichtet werden, sofern eine vollständige elektronische Prüfung, inkl. Echtheitsprüfung des Chips, erfolgreich durchgeführt werden kann, vgl. hierzu Tabelle 3 ab Seite 15 an den entsprechenden Stellen, in denen die jeweiligen optisch-physikalische Prüfungen als optional gekennzeichnet sind.

Es wird EMPFOHLEN, den in Abbildung 3 dargestellten Prozessablauf umzusetzen.

5.2 Prüfergebnisse in der Kontrollanwendung

Im Rahmen (grenz-)polizeilicher Kontrollen geht es darum, eine Aussage zur Echtheit, Integrität und Gültigkeit eines Dokuments zu treffen. Kontrollanwendungen MÜSSEN die Ergebnisse **der einzelnen** Teilprüfungen für die Anwender in reduzierter Detailtiefe zur Verfügung stellen, um aufgetretene Fehler schnell identifizieren zu können. Eine einzige, kumulierte Darstellung aller Teilprüfungen (optisch-physikalisch, elektronisch und kombiniert) wird nicht empfohlen.

Es wird EMPFOHLEN, die in Kapitel 3.2.2 auf Seite 19 definierten Werte der Prüfergebnisse in der Kontrollanwendung in Form einer Ampel mit den folgenden Farben abzubilden:

Prüfergebnis	***Ampelfarbe***
erfolgreich (successful)	grün
fehlgeschlagen (failed)	rot
unbestimmt (undetermined)	gelb
nicht unterstützt (not supported)	grau
nicht durchgeführt (not performed)	grau

Tabelle 6: Zuordnung der Prüfergebnisse zu einer möglichen Visualisierungsform mit Ampelfarben

6 Abhängig vom Dokument können mehrere Seiten optisch-physikalisch geprüft werden. Im Sinne dieser Richtlinie wird dies als mehrere Einzelprüfungen aufgefasst.

Je nach Einsatzszenario kann auch eine andere Zuordnung (z. B. andere Farben oder weniger Variation) geeignet sein. Die Prüfergebnisse in Form von Ampelfarben darzustellen ist eine Empfehlung zur Vereinfachung komplexer Prüfergebnisse. Eine andere Form der Visualisierung und ein höherer Grad an Detaillierung SOLLTEN möglich sein, wenn durch das Einsatzszenario gefordert oder durch den Anwender gewünscht.

Es wird EMPFOHLEN, auch die Ergebnisse der folgenden Teilprüfungen in einer (optional einblendbaren) Detailansicht zu visualisieren:

- Optisch-physikalische Dokumentenprüfergebnisse von Prozessschritten gemäß Abschnitt 5.3
  - Serienidentifikation gemäß Abschnitt 5.3.1
  - Prüfung der MRZ-Konsistenz gemäß Abschnitt 5.3.2
  - Prüfung der Dokumentengültigkeit gemäß Abschnitt 5.3.3
  - Prüfung der MRZ IR-Lesbarkeit gemäß Abschnitt 5.3.4
  - Prüfung der VIZ (Visual Inspection Zone) Lesbarkeit gemäß Abschnitt 5.3.5
  - Prüfung der UV-Helligkeit gemäß Abschnitt 5.3.6
  - MRZ/VIZ-Vergleich gemäß Abschnitt 5.3.7
  - Musterverifikation gemäß Abschnitt 5.3.8
- Elektronische Dokumentenprüfergebnisse von Prozessschritten gemäß Abschnitt 5.4
  - Sequenz zum Lesen und Prüfen der elektronischen Inhalte gemäß Abschnitt 5.4.2
  - Prüfung der Chipkommunikations- und Zugriffsprotokolle gemäß Abschnitt 5.4.3
  - Prüfung der Chipechtheit (AA, CA) gemäß Abschnitt 5.4.4
  - Verifikation der Sicherheitsobjekte gemäß Abschnitt 5.4.5.1
  - Prüfung der Ausstellerzertifikate gemäß Abschnitt 5.4.5.2
  - Integrität der Chipinhalte gemäß Abschnitt 5.4.5.3
  - Vergleich der Ausstellerstaaten (DG1 und DS-Zertifikat) gemäß Abschnitt 5.4.5.4
- Kombiniert optisch-physikalische und elektronische Dokumentenprüfung gemäß Abschnitt 5.5
  - Vergleich der optischen und elektronischen biografischen Daten (optische MRZ und DG1) gemäß Abschnitt 5.5.1

5.3 Optisch-physikalische Dokumentenprüfung

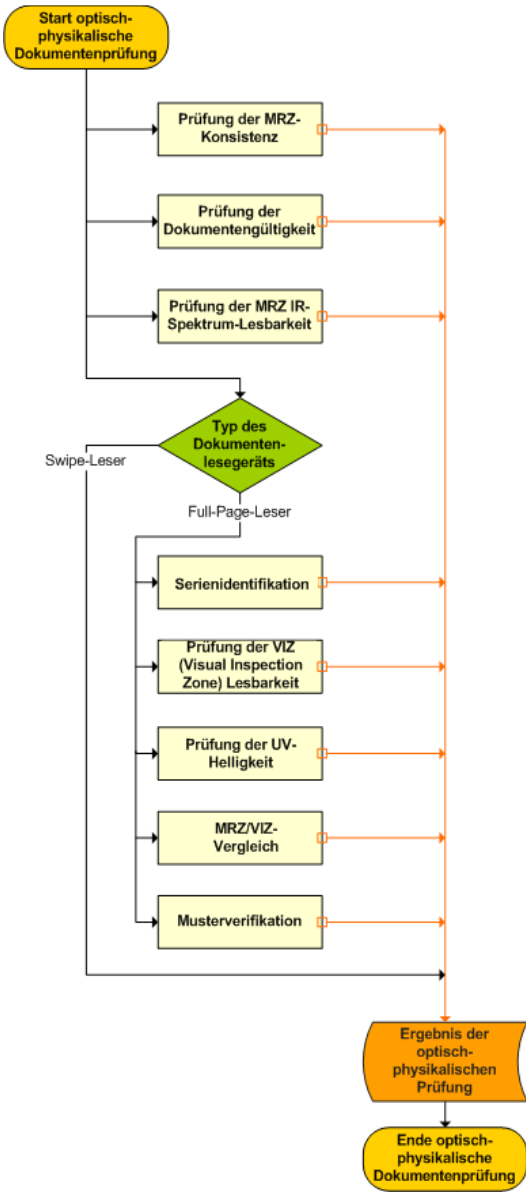

Abbildung 4: Beispielhafter Ablauf der optisch-physikalischen Dokumentenprüfung

Kontrollanwendungen MÜSSEN die optisch-physikalischen Sicherheitsmerkmale des Dokuments gemäß dem jeweiligen Anwendungsszenario prüfen. In den folgenden Abschnitten werden die einzelnen Tests der optisch-physikalischen Dokumentenprüfung genauer erläutert. Abbildung 4 stellt den Ablauf der optisch-physikalischen Dokumentenprüfung grafisch dar. Die Prüfung der MRZ-Konsistenz und die Prüfung der Dokumentengültigkeit sind dabei für alle Dokumentenlesegeräte durchzuführen, während die restlichen optisch-physikalischen Prüfungen (bei Bedarf auch serienspezifisch) nur mit Hilfe von Full-Page-Lesegeräten durchführbar sind. Das Gesamtergebnis der optisch-physikalischen Dokumentenprüfung setzt sich aus den Ergebnissen aller Teilprüfungen zusammen und MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn alle der in den Unterabschnitten vorgeschriebenen, für das Anwendungsszenario zutreffenden Prüfungen als erfolgreich durchgeführt einzustufen sind. Das Dokument weist keine optisch-physikalischen Hinweise auf Fälschungsmanipulationen auf.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn mindestens eine der in den Unterabschnitten vorgeschriebenen Prüfungen als fehlgeschlagen einzustufen ist. Das Dokument weicht in Teilprüfungen vom erwarteten Sollzustand ab. Es besteht der Verdacht einer Manipulation.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn in mindestens einer der in den Unterabschnitten vorgeschriebenen, für das Anwendungsszenario zutreffenden Prüfungen das Ergebnis als unbestimmt einzustufen ist, da bestimmte Informationen für die Durchführung einer Prüfung fehlen.
nicht unterstützt (not supported)	Dieser Wert ist hier nicht von Bedeutung bzw. SOLLTE nicht vergeben werden.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn generell keine optisch-physikalische Dokumentenprüfung durchgeführt wurde.

Tabelle 7: Prüfergebnisse der optisch-physikalischen Dokumentenprüfung

Teilprüfungen, die in Kapitel 2 für das jeweilige Anwendungsszenario als *optional* eingestuft werden und *nicht durchgeführt* werden oder *nicht unterstützt* sind, *beeinflussen* das Gesamtergebnis der optisch-physikalischen Dokumentenprüfung *nicht*.

Im Gegensatz dazu führen Teilprüfungen, die in Kapitel 2 für das jeweilige Anwendungsszenario als *verpflichtend* eingestuft sind und *nicht durchgeführt* werden, zu einem *unbestimmten* oder *fehlgeschlagenen* Prüfergebnis der optisch-physikalischen Dokumentenprüfung. Teilprüfungen, die *nicht unterstützt* werden, *beeinflussen* das Gesamtergebnis der optisch-physikalischen Dokumentenprüfung *nicht*.

5.3.1 Serienidentifikation

Die maschinelle (im Ausnahmefall auch manuelle) Identifikation der Dokumentenserie ist für alle weitergehenden serienspezifischen Prüfschritte (inklusive Parametrierung der Aufnahmebedingungen) wie z. B. UV-Helligkeit, Musterverifikation erforderlich. Unter Serienidentifikation wird in diesem Zusammenhang die eindeutige Zuordnung des zu prüfenden Dokuments zu einem Dokumenten-Grundmodell verstanden, welches über die gleiche sicherungstechnische Ausstattung bezüglich der Eigenschaften im Visuellen sowie unter UV-Fluoreszenz und IR-Absorption verfügt. Der Rückgabewert stellt eine eindeutige Serienkennzeichnung dar, die mit einer Datenbank abgeglichen werden kann. Sofern vom Dokument selbst unterstützt, kann bei der Serienbestimmung auch eine auf dem Dokument aufgebrachte Serien-Marke (beispielsweise ein Strich- oder Barcode) genutzt werden.

Ist eine erste Analyse auf Basis der MRZ beispielsweise nicht für eine eindeutige Serienidentifikation ausreichend, SOLLTE auf Basis des Weißlichtbildes (VIS-Bild) eine Musterverifikation zum Zwecke der Serienidentifikation stattfinden.

Das Ergebnis der Serienidentifikation MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Die Serienidentifikation ist als erfolgreich zu bewerten, wenn die Serienauswahl erfolgte.
fehlgeschlagen (failed)	Die Serienidentifikation ist als fehlgeschlagen zu bewerten, wenn die Serienauswahl nicht erfolgte.
unbestimmt (undetermined)	Ein unbestimmtes Ergebnis kann hier nicht auftreten.
nicht unterstützt (not supported)	Dieser Wert kann hier nicht auftreten.
nicht durchgeführt (not performed)	Die Serienidentifikation muss als nicht durchgeführt bezeichnet werden, wenn nicht versucht wurde, die Serie zu ermitteln.

Tabelle 8: Serienidentifikation

5.3.2 Prüfung der MRZ-Konsistenz

Die Kontrollanwendung MUSS die gelesene MRZ des Dokuments auf Konsistenz gemäß [ICAO9303] prüfen. Bei der Verwendung von Full-Page-Lesegeräten MUSS ein Versuch auf Basis des Weißlicht-Bildes durchgeführt werden, sofern das OCR-Lesen der MRZ (auf Basis der IR-Aufnahme) nicht erfolgreich war.

Es existieren Dokumente, deren MRZ nicht gemäß [ICAO9303] gebildet wird. Solche Fälle können anhand einer entsprechenden Dokumentendatenbank optional ebenfalls unterstützt werden und werden dann so behandelt, als wäre die MRZ gemäß [ICAO9303] gelesen worden. Die Spezifikation MUSS zwischen Technologielieferant und Anwender abgestimmt werden.

Das Ergebnis dieser Prüfung MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn alle Prüfziffern korrekt berechnet wurden.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn mindestens eine Prüfziffernberechnung ein falsches Ergebnis aufweist.
unbestimmt (undetermined)	Ein unbestimmtes Prüfergebnis kann hier nicht auftreten.
nicht unterstützt (not supported)	Prüfung muss als nicht unterstützt bezeichnet werden, wenn die eingelesene Dokumentenseite keine MRZ aufweist. Dies ist beispielsweise bei ID-Karten (nPA, eAT) der Fall; hier würde dann die CAN gelesen.
nicht durchgeführt (not performed)	Die Prüfung muss als nicht durchgeführt bezeichnet werden, wenn die MRZ-Konsistenz-Prüfung nicht durchgeführt wurde.

Tabelle 9: Prüfergebnisse MRZ-Konsistenz

5.3.3 Prüfung der Dokumentengültigkeit

Das aus der MRZ extrahierte Ablaufdatum des Dokuments MUSS mit dem aktuellen Datum der Dokumentenprüfung verglichen werden, um feststellen zu können, ob das Dokument noch gültig ist oder nicht.

Da die Jahreszahl des Ablaufdatums in der MRZ nur mit den letzten zwei Ziffern des Jahres codiert ist, MÜSSEN die folgenden Regeln zur Berechnung des tatsächlichen Ablaufdatums (Jahreszahl) angewendet werden:

- Liegen die zwei Ziffern der Jahreszahl aus der MRZ in einem Bereich zwischen dem aktuellen Jahr und 10 Jahren[7] in der Zukunft, MUSS die tatsächliche Jahreszahl so ergänzt werden, dass das gesamte Ablaufdatum in der Zukunft liegt (z. B. extrahiertes Ablaufdatum aus der MRZ = 150401, aktuelles Datum = 02.05.2012, tatsächliches Ablaufdatum = 01.04.2015).
- Liegen die zwei Ziffern der Jahreszahl aus der MRZ nicht im Bereich zwischen dem aktuellen Jahr und 10 Jahren in der Zukunft, MUSS angenommen werden, dass das tatsächliche Ablaufdatum in der Vergangenheit liegt (z. B. extrahiertes Ablaufdatum aus der MRZ = 110302, aktuelles Datum = 02.05.2012, tatsächliches Ablaufdatum = 02.03.2011).

Diese Regeln können allerdings nicht sämtliche (möglichen) Sonderfälle abdecken. Im Zweifel MUSS das System Reisedokumente für eine nachfolgende manuelle Prüfung markieren, da bzgl. der Dokumentengültigkeit in Sonderfällen automatisiert keine gesicherte Aussage getroffen werden kann.

7 Bei vorab bekannten Dokumenten mit einer längeren Gültigkeitsdauer, KANN hier abweichend ein anderer Wert angenommen werden (z. B. russische Inlandspässe oder rumänische ID-Karte). Darüber hinaus gibt es abweichende Zeiträume, in denen das Dokument zum Grenzübertritt zugelassen ist, obgleich es abgelaufen ist.

Das Ergebnis dieser Prüfung MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn das Dokument noch gültig ist.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn das Ablaufdatum des Dokuments in der Vergangenheit liegt und somit das Dokument nicht mehr gültig ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn das Ablaufdatum des Dokuments nicht aus der MRZ extrahiert werden kann.
nicht unterstützt (not supported)	Dieser Wert kann hier nicht auftreten.
nicht durchgeführt (not performed)	Die Prüfung muss als nicht durchgeführt bezeichnet werden, wenn die Prüfung der Dokumentengültigkeit nicht durchgeführt wurde.

Tabelle 10: Prüfergebnisse Dokumentengültigkeit

Wird für den Zugriff auf das Dokument die CAN verwendet, so MUSS dieser Test auf Basis der elektronischen MRZ (DG1) durchgeführt werden.

5.3.4 Prüfung der MRZ IR-Lesbarkeit

Die Kontrollanwendung MUSS prüfen und sicherstellen, dass die MRZ/CAN komplett im IR-Spektrum der Personaldatenseite sichtbar und lesbar ist.

Das Ergebnis dieses Tests MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die MRZ/CAN des Dokuments im IR-Spektrum der Personaldatenseite lesbar ist.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die MRZ/CAN nicht im IR-Spektrum der Personaldatenseite lesbar ist.
unbestimmt (undetermined)	Ein unbestimmtes Prüfergebnis DARF hier nicht auftreten.
nicht unterstützt (not supported)	Die Prüfung ist als nicht unterstützt zu bewerten, wenn die Dokumentenserie selbst nicht IR-lesbar ist (in Abweichung der Vorgaben von [ICAO9303]).
nicht durchgeführt (not performed)	Die Prüfung muss als nicht durchgeführt bezeichnet werden, wenn nicht versucht wurde, die MRZ IR-Lesbarkeit durchzuführen, z. B. wenn ein Swipe-Leser für die Extraktion der MRZ nicht im IR-Spektrum liest.

Tabelle 11: Prüfergebnisse MRZ IR-Lesbarkeit

5.3.5 Prüfung der VIZ (Visual Inspection Zone) Lesbarkeit

Bei Prüfung der VIZ-Lesbarkeit MUSS die Kontrollanwendung prüfen, dass die Elemente der VIZ, deren Sichtbarkeit im IR für das vorliegende Dokument aus der Dokumentendatenbank bekannt ist, sichtbar sind. Außerdem MUSS geprüft werden, dass Elemente, von denen bekannt ist, dass sie im IR nicht sichtbar sein dürfen, nicht sichtbar sind.

Das Ergebnis dieses Tests MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfungsergebnis ist als erfolgreich zu bewerten, wenn die Elemente der VIZ, deren Sichtbarkeit im IR für das vorliegende Dokument aus der Dokumentendatenbank bekannt ist, sichtbar sind, wenn die Elemente, von denen bekannt ist, dass sie im IR nicht sichtbar sein dürfen, nicht sichtbar sind und zumindest die Dokumentennummer per OCR lesbar ist.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die VIZ nicht im IR-Spektrum der Personaldatenseite sichtbar ist.
unbestimmt (undetermined)	Ein unbestimmtes Prüfergebnis kann hier nicht auftreten.
nicht unterstützt (not supported)	Das Prüfungsergebnis ist als nicht unterstützt zu bewerten, wenn für ein Dokument aus der Dokumentendatenbank bekannt ist, dass dieses die IR-Personalisierung nicht standardkonform implementiert.
nicht durchgeführt (not performed)	Die Prüfung muss als nicht durchgeführt bezeichnet werden, wenn nicht versucht wurde, die VIZ-Lesbarkeit durchzuführen oder wenn z. B. ein Swipe-Leser verwendet wurde.

Tabelle 12: Prüfergebnisse VIZ Lesbarkeit

5.3.6 Prüfung der UV-Helligkeit

Die Kontrollanwendung MUSS prüfen, ob unter Beleuchtung mit UV-Licht (365 nm) die reflektierte UV-Helligkeit ggf. auf ein mit sog. optisch-physikalischen Aufhellern versehenes Substrat hinweist.

Zum eigentlichen optisch-physikalischen Ergebnis SOLLTE die Kontrollanwendung optional auch die unterschiedlich geprüften optisch-physikalischen Bereiche des Dokuments samt Helligkeits-Messwert als Rückgabewerte liefern können. Auf diese Weise ist es möglich, auf unterschiedlichen Teilen im UV-Bereich unterschiedliche Helligkeitsmessungen durchzuführen und mit Referenzwerten für einen bestimmten Dokumententyp abzugleichen, sofern die Dokumentenserie bekannt und eindeutig bestimmt werden konnte.

Aufgrund der Mannigfaltigkeit sich im Umlauf befindlicher Dokumententypen ist eine abgeschlossene und vollständige Datenbank bzgl. der UV-Helligkeit nicht abschließend spezifizierbar. Es wird daher EMPFOHLEN, die Inhalte der Datenbank zur UV-Helligkeit zusammen mit dem jeweiligen Bedarfsträger initial zu spezifizieren und in gemeinsamer Absprache zwischen Hersteller und Bedarfsträger zu pflegen. Die hinterlegten Schwellwerte MÜSSEN für den Betreiber transparent, nachvollziehbar und anpassbar sein. Dies beinhaltet:

- Definition von Merkmalen zu Serienidentifikatoren zum Erkennen unterschiedlicher Dokumente sowie deren erwartete UV-Helligkeitswerte.
- Nachträgliche Erweiterung, Korrektur und Nachjustierung der spezifizierten Prüfungen, um Erfahrungen hinsichtlich der Streuung der zu prüfenden Eigenschaften von Echtdokumenten berücksichtigen zu können (z. B. wegen Alterungseffekten, Gebrauchsspuren, Produktionsschwankungen).

Diese Flächen MÜSSEN dabei in sog. Bereichskoordinaten angegeben werden, wobei der Punkt (0, 0) der linken oberen Ecke des eingelesenen digitalisierten Bildes entspricht. Für jeden Bereich MUSS in einem Tupel angegeben werden:

- MaxRange: Dieses Attribut enthält die obere Grenze des Wertebereichs.
- MinRange: Dieses Attribut enthält die untere Grenze des Wertebereichs.
- Result: Dieses Attribut repräsentiert das Ergebnis des UV-Helligkeitstests im angegebenen Bereich des Dokuments.
- Threshold: Dieses Attribut enthält den konfigurierten Schwellwert für den UV-Helligkeitstest dieses Bereichs.
- Value: Dieses Attribut enthält den erreichten Wert (UV-Helligkeitswert) des UV-Helligkeitstests.

Ist der geprüfte Bereich selbst kein Rechteck (z. B. ein Polygon), sind in den folgenden Werten die Koordinaten des umhüllenden Rechtecks einzutragen:

- X1: Dieses Attribut enthält die X-Koordinate der linken oberen Ecke des für diesen UV-Helligkeitstest relevanten Bereichs in Millimeter. Die Koordinaten (0,0) sind dabei am linken oberen Rand des Dokuments anzusiedeln.
- X2: Dieses Attribut enthält die X-Koordinate der rechten unteren Ecke des für diesen UV-Helligkeitstest relevanten Bereichs in Millimeter. Die Koordinaten (0,0) sind dabei am linken oberen Rand des Dokuments anzusiedeln.
- Y1: Dieses Attribut enthält die Y-Koordinate der linken oberen Ecke des für diesen UV-Helligkeitstest relevanten Bereichs in Millimeter. Die Koordinaten (0,0) sind dabei am linken oberen Rand des Dokuments anzusiedeln.
- Y2: Dieses Attribut enthält die Y-Koordinate der rechten unteren Ecke des für diesen UV-Helligkeitstest relevanten Bereichs in Millimeter. Die Koordinaten (0,0) sind dabei am linken oberen Rand des Dokuments anzusiedeln.

Das Ergebnis dieses Tests MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn der Sollzustand[8] erreicht ist.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn vom Sollzustand abgewichen wird.

8 Unter Sollzustand wird hier der Wert verstanden, der durch den Hersteller der Dokumentendatenbank und den Bedarfsträger für den jeweiligen Dokumententyp definiert wurde.

Prüfergebnis	*Beschreibung*
unbestimmt (undetermined)	Dieser Wert kann hier nicht auftreten.
nicht unterstützt (not supported)	Die Prüfung muss als nicht unterstützt bezeichnet werden, wenn ein UV-Helligkeitstest für das Dokument nicht definiert ist.
nicht durchgeführt (not performed)	Die Prüfung muss als nicht durchgeführt bezeichnet werden, wenn der UV-Helligkeitstest nicht durchgeführt wurde.

Tabelle 13: Prüfergebnisse UV-Helligkeitstest

5.3.7 MRZ/VIZ-Vergleich

Die aus der MRZ extrahierten Daten KÖNNEN von der Kontrollanwendung mit den Daten[9], die aus der sichtbaren Personaldatenseite (VIZ) extrahiert wurden, verglichen werden. Da in der VIZ auch nicht-lateinische Zeichen enthalten sein können, ist für den Vergleich ggf. eine zum jeweiligen Ausweisdokument passende Transliteration erforderlich. Die Transliteration SOLLTE gemäß [ICAO9303] erfolgen.

Die VIZ SOLLTE im ersten Versuch aus der IR-Aufnahme durch OCR analysiert werden. Schlägt der Versuch fehl, die dort gelesenen Daten vollständig und korrekt zu extrahieren, MUSS eine Weißlichtaufnahme als Grundlage für einen weiteren OCR-Analyseschritt genutzt werden.

Das Ergebnis dieses Vergleichs MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn MRZ- und VIZ-Daten plausibel zueinander sind.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn MRZ- und VIZ-Daten nicht plausibel zueinander sind.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn das Prüfergebnis aufgrund fehlender Informationen nicht bestimmt werden kann (z. B. wenn gewisse Daten der VIZ nicht extrahiert werden können).
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, falls die Daten der VIZ nicht erhoben werden können.
nicht durchgeführt (not performed)	Die Prüfung muss als nicht durchgeführt bezeichnet werden, wenn nicht versucht wurde, den MRZ/VIZ-Vergleich durchzuführen (z. B. weil ein Swipe-Leser zum Lesen der MRZ verwendet wurde).

Tabelle 14: Prüfergebnisse MRZ/VIZ-Vergleich

9 Nicht gemeint ist dabei die Plausibilität der Ausstellungs- und Ablaufdatumseintragungen.

5.3.8 Musterverifikation

Kontrollanwendungen MÜSSEN optisch-physikalische Sicherheitselemente und Muster des optisch erfassten Dokuments anhand einer passenden Musterdatenbank prüfen können.

Das Ergebnis der Musterverifikation MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn nach Prüfung aller zu prüfenden Muster eine mit dem Bedarfsträger abgestimmte Entscheidungsfunktion unter Berücksichtigung der Ergebnisse aller dieser Musterprüfungen zu einem positiven Ergebnis kommt[10].
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn nach Prüfung aller zu prüfenden Muster eine mit dem Bedarfsträger abgestimmte Entscheidungsfunktion unter Berücksichtigung der Ergebnisse aller dieser Musterprüfungen zu einem negativen Ergebnis kommt.
unbestimmt (undetermined)	Dieser Wert kann hier nicht auftreten.
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn für das vorliegende Dokument keine Referenzdaten in der Musterdatenbank vorhanden sind.
nicht durchgeführt (not performed)	Die Prüfung muss als nicht durchgeführt bezeichnet werden, wenn nicht versucht wurde, die Musterverifikation durchzuführen.

Tabelle 15: Prüfergebnisse Musterverifikation

In allen Fällen wird die Verwendung einer dedizierten Datenbank für das jeweilige Kontrollszenario EMPFOHLEN. Diese Musterdatenbank MUSS in Absprache mit dem Bedarfsträger regelmäßig aktualisiert werden, um Falschrückweisungsraten zu senken bzw. ganz zu vermeiden. Die durchschnittliche Falschrückweisungsrate SOLLTE 5% nicht überschreiten.

Es wird EMPFOHLEN, die Inhalte der Musterdatenbank zusammen mit dem jeweiligen Bedarfsträger zu spezifizieren und gemeinsam zu pflegen, dies beinhaltet meist:

- Definition von Serienidentifikatoren zum Erkennen unterschiedlicher Dokumente sowie deren Ausprägung (Dokumentenfamilien).
- Definition von Suchbereichen und deren Musterinhalt sowie den darauf basierenden Prüfungen, einschließlich Schwell- und Erwartungswerten.
- Nachträgliche Erweiterung, Korrektur und Nachjustierung der spezifizierten Prüfungen, um Erfahrungen hinsichtlich der Streuung der zu prüfenden Eigenschaften von Echtdokumenten berücksichtigen zu können (z. B. wegen Alterungseffekten, Gebrauchsspuren, Produktionsschwankungen).

Aufgrund der Mannigfaltigkeit sich im Umlauf befindlicher Dokumententypen ist eine abgeschlossene und vollständige Musterdatenbank nicht finit herstellbar. Die hinterlegten

10 Die einfachste Entscheidungsfunktion ist das logischen UND, in der Regel werden allerdings häufig komplexere Funktionen verwendet werden.

Prüfmuster sowie die zugehörigen Schwellwerte müssen für den Betreiber transparent, nachvollziehbar und jederzeit anpassbar sein. Die Flächen der Prüfmuster MÜSSEN dabei in sog. Bereichskoordinaten angegeben werden, wobei der Punkt (0, 0) der linken oberen Ecke des eingelesenen digitalisierten Bildes entspricht. Für jeden Bereich MÜSSEN in einem Tupel angegeben werden[11]:

- Id: Dieses Attribut enthält eine eindeutige ID des Musters (z. B. gemäß Eintrag in der Musterdatenbank).
- MaxRange: Dieses Attribut enthält die obere Grenze des Wertebereichs.
- MinRange: Dieses Attribut enthält die untere Grenze des Wertebereichs.
- Result: Dieses Attribut repräsentiert das Ergebnis der Prüfung des aktuellen Musters.
- Threshold: Dieses Attribut enthält den konfigurierten Schwellwert für die Musterverifikation dieses Musters.
- Value: Dieses Attribut enthält den erreichten Wert des Mustertests für dieses Muster.

Ist der geprüfte Bereich kein Rechteck (z. B. ein Polygon), sind in den folgenden Werten die Koordinaten des umhüllenden Rechtecks einzutragen:

- X1: Dieses Attribut enthält die X-Koordinate der linken oberen Ecke des für diesen Mustertest relevanten Bereich in Millimeter. Die Koordinaten (0,0) sind dabei am linken oberen Rand des Dokuments anzusiedeln.[12]
- X2: Dieses Attribut enthält die X-Koordinate der rechten unteren Ecke des für diesen Mustertest relevanten Bereich in Millimeter. Die Koordinaten (0,0) sind dabei am linken oberen Rand des Dokuments anzusiedeln.
- Y1: Dieses Attribut enthält die Y-Koordinate der linken oberen Ecke des für diesen Mustertest relevanten Bereich in Millimeter. Die Koordinaten (0,0) sind dabei am linken oberen Rand des Dokuments anzusiedeln.
- Y2: Dieses Attribut enthält die Y-Koordinate der rechten unteren Ecke des für diesen Mustertest relevanten Bereich in Millimeter. Die Koordinaten (0,0) sind dabei am linken oberen Rand des Dokuments anzusiedeln.

5.4 Elektronische Dokumentenprüfung

In den folgenden Unterabschnitten finden sich die notwendigen (Protokoll-)Prüfprozesse der elektronischen Dokumentenprüfung. Das Gesamtergebnis der elektronischen Dokumentenprüfung setzt sich aus den Ergebnissen aller Teilprüfungen zusammen und MUSS entsprechend der folgenden Tabelle abgebildet werden:

11 Vergleiche hierzu nochmals Abschnitt 5.3.6 und das dort definierte Tupel.

12 In [ICAO9303] wird als Referenzursprung (0,0) abweichend zu dem hier beschriebenen Ursprung die linke untere Ecke verwendet.

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Der Prüfprozess ist als erfolgreich zu bewerten, wenn alle der in den Unterabschnitten vorgeschriebenen Prüfungen als erfolgreich durchgeführt einzustufen sind. Der Chipinhalt ist zweifelsfrei echt und unverfälscht und die für das vorliegende Dokument spezifizierten Protokolle konnten erfolgreich angewendet werden.
fehlgeschlagen (failed)	Der Prüfprozess ist als fehlgeschlagen zu bewerten, wenn mindestens eine der in den Unterabschnitten vorgeschriebenen Prüfungen als fehlgeschlagen einzustufen ist. Das Dokument wurde elektronisch entweder fehlerhaft ausgestellt oder es besteht der Verdacht einer Manipulation. Ein Fehlschlagen eines Zugriffsprotokolls (BAC, PACE oder TA) *beeinflusst* das Gesamtergebnis der elektronischen Dokumentenprüfung *nicht* negativ.
unbestimmt (undetermined)	Der Prüfprozess ist als unbestimmt zu bewerten, wenn in mindestens einer der in den Unterabschnitten vorgeschriebenen Prüfungen das Ergebnis als unbestimmt einzustufen ist.
nicht unterstützt (not supported)	Dieser Wert ist zu verwenden, wenn für das vorliegende Dokument keine elektronische Prüfung möglich ist, beispielsweise wenn das Dokument keinen Chip enthält oder ein Chip nicht spezifikationskonform auslesbar bzw. defekt ist. In diesem Fall sind dann alle Teilprüfungen auf den Status *nicht durchgeführt* zu setzen.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, eine elektronische Dokumentenprüfung durchzuführen, z. B. in der Software deaktiviert oder kein entsprechendes Lesegerät vorhanden.

Tabelle 16: Prüfergebnisse elektronische Dokumentenprüfung

Teilprüfungen, die in Kapitel 2 für das jeweilige Anwendungsszenario als *optional* eingestuft sind und *nicht durchgeführt* oder *nicht unterstützt* werden, *beeinflussen* das Gesamtergebnis der elektronischen Dokumentenprüfung *nicht*.

Im Gegensatz dazu führen Teilprüfungen, die in Kapitel 2 für das jeweilige Anwendungsszenario als *verpflichtend* eingestuft sind und *nicht durchgeführt* werden, zu einem *unbestimmten* oder *fehlgeschlagenen* Prüfergebnis der elektronischen Dokumentenprüfung. Teilprüfungen, die *nicht unterstützt* werden, *beeinflussen* das Gesamtergebnis der elektronischen Dokumentenprüfung *nicht*.

5.4.1 PKI-Architektur der elektronischen Dokumentenprüfung

Die Prüfung der elektronischen Komponenten sowie weiterer digitaler Sicherheitsmerkmale (beispielsweise digitales Siegel) MUSS entsprechend der auf nationaler wie internationaler Ebene standardisierten Protokolle erfolgen. Diese Protokolle basieren auf hierarchisch strukturierten Public-Key-Infrastrukturen (PKI bzw. PKIen), welche die auf dem Ausweisdokument aufgebrachten Daten sowie ihre Repräsentanten als elektronische Signatur auf einem Chip oder optischen Code zweifelsfrei bestätigen helfen. Die im Rahmen dieses Dokuments als verwendet angenommenen PKIen sind Aussteller-PKIen gemäß [ICAO9303] und EAC-PKIen gemäß [EC_2252/2004].

Das Inspektionssystem (IS) ist die Basis für die maschinell gestützte Dokumentenprüfung der elektronischen Merkmale des jeweiligen vorliegenden elektronischen Reisedokuments. Um eine vollständige Prüfung der Dokumente durch das Inspektionssystem zu ermöglichen, MUSS dieses mindestens die folgenden Schritte durchführen können:

- Durchführung der TA (siehe auch Abschnitt 5.4.3.2)
- Verifikation von DS- und CSCA-Zertifikaten (siehe auch Abschnitt 5.4.5.2)
- Bereitstellen von Defektlisten für ein gegebenes DS- bzw- CSCA-Zertifikat (siehe auch Abschnitt 5.6).

Im Gegenzug MÜSSEN Kontrollanwendungen die folgenden Anforderungen erfüllen:

- Durchführung von TA über ein IS
- Verifikation des DS-Zertifikats durch Anfrage bei einem IS
- Durchführung von Passive Authentication mittels IS
- Verarbeiten der bekannten Defekte, die vom IS übermittelt werden.

Das IS MUSS für jedes DS-Zertifikat eine Prüfung durchführen und einen Vertrauensstatus vergeben, der die Integrität des Zertifikats beschreibt. Die Basis für diesen Vertrauensstatus liefern die Master- und Defektlisten.

Die folgenden Werte sind für den Vertrauensstatus zulässig:

Vertrauensstatus	***Beschreibung***
vertrauenswürdig (trusted)	Das Zertifikat ist als vertrauenswürdig eingestuft.
nicht vertrauenswürdig (not trusted)	Das Zertifikat ist nicht vertrauenswürdig. Ergebnisse von Prüfungen, bei denen dieses Zertifikat verwendet wird, DÜRFEN NICHT als vertrauenswürdig angesehen werden.
unbestimmt (undetermined)	Der Vertrauensstatus des Zertifikats ist unbestimmt.

Tabelle 17: Mögliche Werte des Vertrauensstatus

Auch wenn der Vertrauensstatus eines vorliegenden DS-Zertifikats nicht gegeben ist, MÜSSEN Teilprüfungen wie z. B. die *Passive Authentication* durchgeführt werden, wenngleich das Gesamtergebnis der elektronischen Prüfung dann nicht mehr „bestanden“ sein kann.

5.4.1.1 Bezugsquellen der Master-/Defektlisten und Zugriffsberechtigungszertifikate

Das IS bezieht die Master- und Defektlisten und Zugriffsberechtigungszertifikate über die DV, welche ihrerseits über den SPOC mit der nationalen CVCA verbunden ist. Die nationale CVCA ist über den SPOC mit CVCA´s anderer Länder verbunden. Das nationale PKD (N-PKD) steht mit dem ICAO PKD und der nationalen CSCA in Verbindung und verwaltet die nationalen und internationalen CSCA- und DS-Zertifikate, die letztlich in Form von Master- und Defektlisten veröffentlicht werden. Abbildung 5 verdeutlicht diese Architektur schematisch:

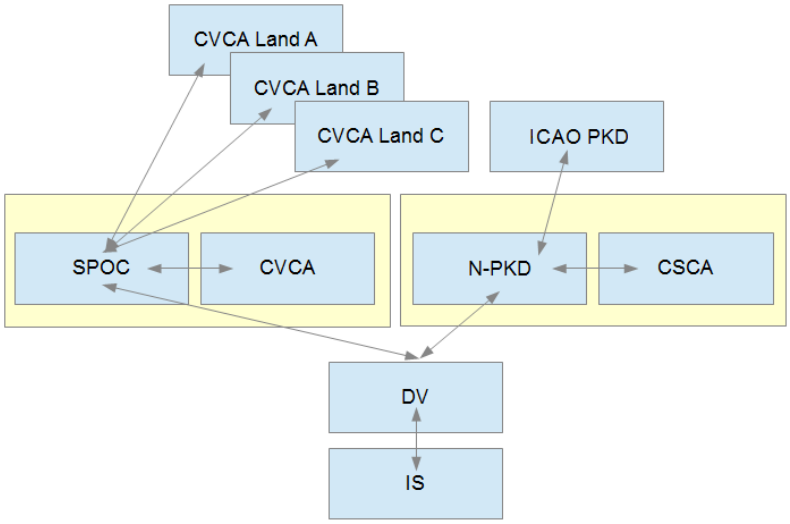

Abbildung 5: Schematische Darstellung der Gesamten Architektur IS ↔ DV ↔ CVCA und PKD

Eine Onlineverbindung des IS in Richtung DV ist hierbei nicht in jedem Szenario zwingend notwendig, jedoch stets dann, wenn für die Bestimmung von digitalen Signaturen die notwendigen Zertifikate aktuell sein müssen oder (tages-)aktuelle Defekte verarbeitet werden können müssen. Zudem kann es im Wege der Zugriffsberechtigung der EAC-PKI notwendig sein, Berechtigungszertifikate zu aktualisieren und zu verteilen.

Die möglichen Umsetzungen für die Infrastruktur der Inspektionssysteme sind in [TR-03129-2] definiert, wobei im Rahmen hoheitlicher Kontrollinfrastrukturen (wie z. B. Grenzkontrollen) die Architektur auf Basis eines verteilten Inspektionssystems gemäß Abschnitt 1.2.1 aus [TR-03129-2] verwendet werden SOLLTE.

5.4.2 Sequenz zum Lesen und Prüfen der elektronischen Inhalte

Der Zugriff auf die elektronischen Datengruppen ist durch die in [ICAO9303] und [TR-03110] definierten Zugriffskontrollmechanismen und Sicherheitsprotokolle geregelt. Inspektionssysteme MÜSSEN die folgenden Protokolle und Sicherheitsmechanismen unterstützen:

- Basic Access Control (BAC) gemäß [ICAO9303]
- Password Authentication Connection Establishment (PACE) gemäß [ICAOSAC]
- Passive Authentication (PA) gemäß [ICAO9303]
- Active Authentication (AA) gemäß [ICAO9303]
- Chip Authentication Version 1 (CA1) gemäß [TR-03110]
- Chip Authentication Version 2 (CA2) gemäß [TR-03110]
- Terminal Authentication Version 1 (TA1) gemäß [TR-03110]
- Terminal Authentication Version 2 (TA2) gemäß [TR-03110]

Um die einzelnen Protokolle ausführen zu können, MÜSSEN die folgenden Dateien und Datengruppen von der Kontrollanwendung gelesen und verarbeitet werden können, sofern sie auf dem Dokument spezifikationskonform vorhanden sind:

- EF.COM (Index, der angibt, welche Datengruppen auf dem Chip gespeichert sind)

- EF.SOD (Hashwerte aller Datengruppen sowie elekt. Signatur über diese Hashwerte)
- DG14 (Chip Authentication Public Key)
- DG15 (Active Authentication Public Key)
- EF.CVCA (Country Verifying CA)
- EF.CardAccess (Sicherheitsinformationen gemäß [TR-03110])
- EF.CardSecurity (Sicherheitsinformationen gemäß [TR-03110])
- EF.ChipSecurity (Sicherheitsinformationen gemäß [TR-03110])

Zusätzlich MÜSSEN die folgenden Datengruppen gelesen und verarbeitet werden können, sofern sie auf dem Dokument spezifikationskonform vorhanden sind, um weitere Prüfungen der Datengruppen der ePassport-Anwendung zu ermöglichen und ggf. weiterführende Prüfungen auf den gelesenen Daten durchzuführen (z. B. biometrischer Vergleich des Gesichtsbilds):

- DG1 (enthält biografische Daten des Inhabers)
- DG2 (enthält das Gesichtsbild)

Des Weiteren SOLLTE die Datengruppe

- DG3 (enthält Fingerabdrücke)

gelesen und verarbeitet werden, sofern sie auf dem Dokument spezifikationskonform vorhanden ist und entsprechenden Berechtigungen (z. B. mittels TA) zum Lesen vorhanden sind, um diese Daten einer weiteren Verarbeitung zuzuführen (z. B. biometrischer Vergleich von Fingerabdrücken).

Außerdem SOLLTEN die Kontrollanwendungen auch alle anderen gespeicherten Datengruppen auslesen und verarbeiten können (DG4 – DG13, DG16), sofern auf dem Chip vorhanden und lesbar.

Die Reihenfolge des Zugriffs auf die einzelnen Dateien und Datengruppen auf dem elektronischen Chip des Dokuments hängt von den unterstützten Protokollen des vorliegenden Dokuments ab.

Grundsätzlich MÜSSEN mindestens die Protokollabläufe aus den Abschnitten 5.4.2.1, 5.4.2.2 und 5.4.2.3 vom Inspektionssystem unterstützt werden. Die Technische Richtlinie macht keine Vorgaben, wie für ein bestimmtes Dokument der korrekte Protokollablauf festzulegen ist, da es verschiedene technische Möglichkeiten (heuristisch, dokumententypbasiert, etc.) zur Umsetzung gibt. Eine exemplarische Umsetzung des Kommunikationsablaufs zwischen den im Kontrollprozess beteiligten Komponenten ist in Kapitel 11 (Anhang A) angeführt. Eine beispielhafte Auflistung der verfügbaren EU-Dokumente und deren Unterstützung der einzelnen Protokollabläufe findet sich in Kapitel 12 (Anhang B).

Für die Protokollabläufe in den folgenden Abschnitten wird stets vorausgesetzt, dass die zum Aufbau des sicheren Kanals (BAC, PACE) erforderlichen Informationen (MRZ, CAN) bereits vorab durch das Dokumentenlesegerät optisch erfasst und zur weiteren Verarbeitung zur Verfügung gestellt wurden bzw. durch den Anwender manuell zur Verfügung gestellt wurden (z. B. durch Eingabe über die Tastatur).

5.4.2.1 Protokollablauf Version 1

Kontrollanwendungen MÜSSEN den Prozessablauf aus Abbildung 6 implementieren und unterstützen.

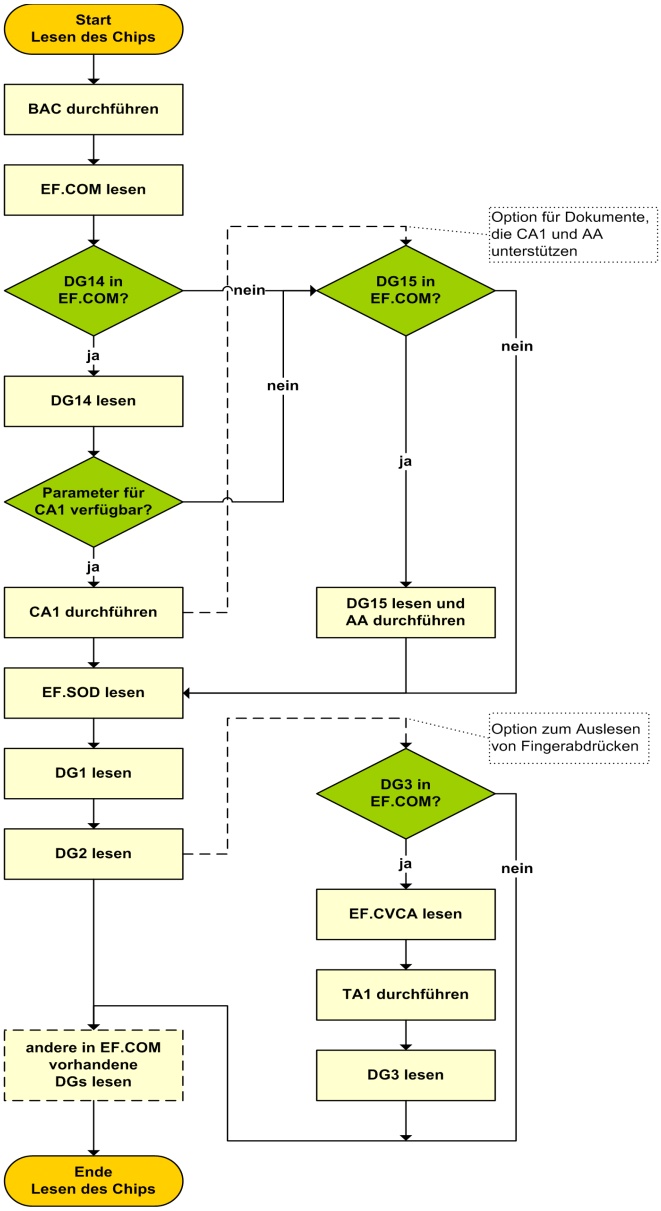

Abbildung 6: Protokollablauf Version 1

Nach dem Lesen von EF.COM wird geprüft, ob DG14 auf dem Dokument vorhanden ist. Ist DG14 vorhanden und die notwendigen Parameter für CA sind darin enthalten, wird CA in der Version 1 durchgeführt, um den Chip zu authentifizieren. Wenn DG14 vorhanden ist, die notwendigen Parameter für CA aber nicht enthalten sind, dienen die in DG14 vorhandenen Informationen als Domain-Parameter für die AA (bei der Verwendung von elliptischen Kurven) [ICAO-LDS-PKI].

Ist DG14 nicht vorhanden, wird geprüft, ob DG15 vorhanden ist. Ist DG15 vorhanden, wird AA durchgeführt. Ist auch DG15 nicht vorhanden, kann die Echtheit des Chips nicht verifiziert werden,

da weder AA noch CA1 durchgeführt werden konnten. Im Falle, dass DG14 und DG15 vorhanden sind, KANN AA zusätzlich zu CA1 durchgeführt werden.

Im Anschluss an die ggf. durchgeführte Echtheitsprüfung können sodann die Dateien mit einfachem Zugriffsschutz gelesen werden. Dazu gehören z. B. EF.SOD, DG1, DG2.

Sofern Fingerabdrücke in DG3 gespeichert sind und diese mit EAC gemäß [TR-03110] geschützt sind, können diese erst dann ausgelesen werden, wenn TA in Version 1 erfolgreich durchgeführt wurde. Dazu muss die Datei EF.CVCA zuerst gelesen werden, um die notwendigen Informationen für die Durchführung von TA zu besitzen. Weitere vorhandene Datengruppen können anschließend ebenfalls vom Chip gelesen werden.

5.4.2.2 Protokollablauf Version 2

Kontrollanwendungen MÜSSEN den Prozessablauf aus Abbildung 7

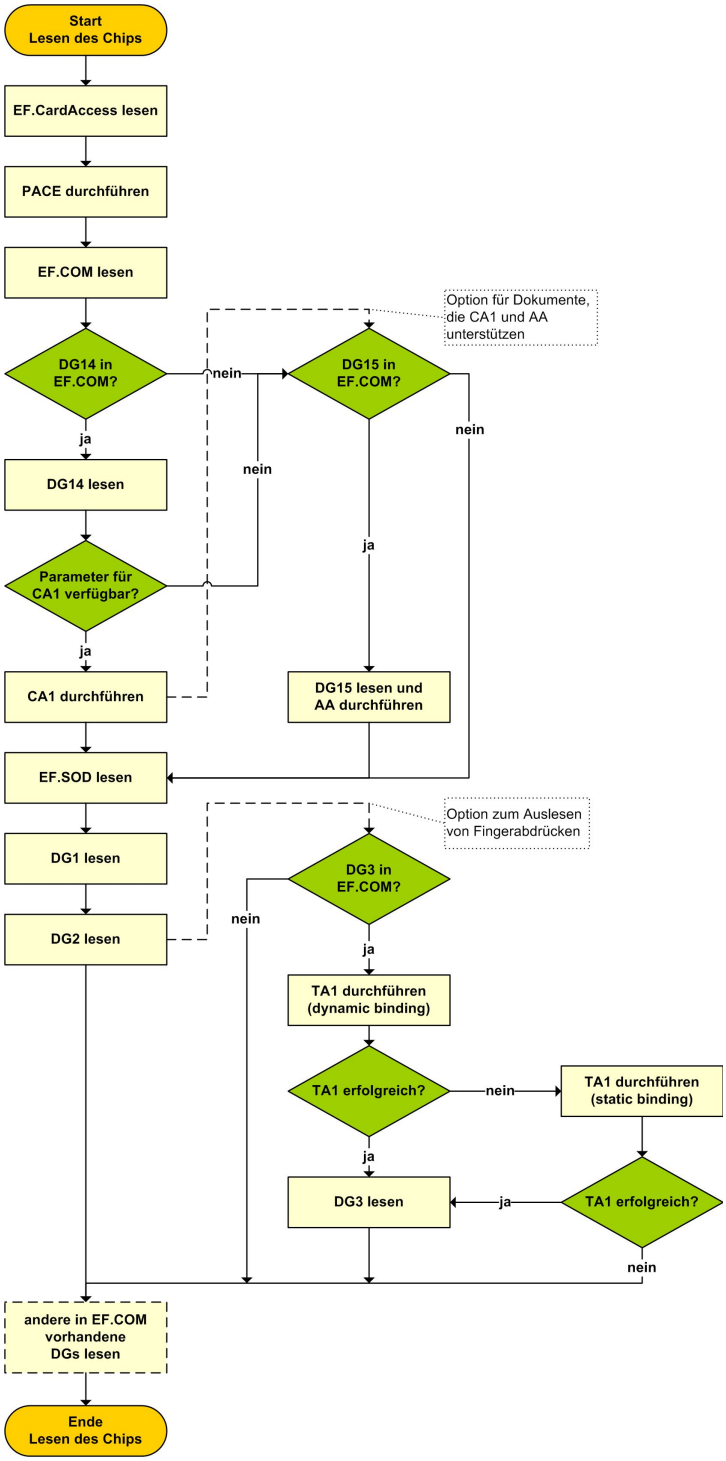

Abbildung 7: Protokollablauf Version 2

implementieren und unterstützen.

Zuerst muss die Datei EF.CardAccess gelesen werden, um im Anschluss PACE durchführen zu können. Nach dem erfolgreichen Aufbau der Secure-Messaging-Session wird EF.COM gelesen.

Danach wird geprüft, ob DG14 auf dem Dokument vorhanden ist. Ist DG14 vorhanden und die notwendigen Parameter für CA sind darin enthalten, wird CA in der Version 1 durchgeführt, um den Chip zu authentifizieren. Wenn DG14 vorhanden ist, die notwendigen Parameter für CA aber nicht enthalten sind, dienen die in DG14 vorhandenen Informationen als Domain-Parameter für die AA (bei Verwendung von elliptischen Kurven) [ICAO-LDS-PKI].

Ist DG14 nicht vorhanden, wird geprüft, ob DG15 vorhanden ist. Ist DG15 vorhanden, wird AA durchgeführt. Ist auch DG15 nicht vorhanden, kann die Echtheit des Chips nicht verifiziert werden, da weder AA noch CA1 durchgeführt werden konnten. Im Falle, dass DG14 und DG15 vorhanden sind, KANN AA zusätzlich zu CA1 durchgeführt werden. Im Anschluss können dann die Dateien mit einfachem Zugriffsschutz gelesen werden. Dazu gehören z. B. EF.SOD, DG1, DG2.

Sofern Fingerabdrücke in DG3 gespeichert sind, können diese erst dann ausgelesen werden, wenn TA in Version 1 erfolgreich durchgeführt wurde. Dazu SOLLTE zuerst TA1 mit *dynamic binding* (siehe [TR-03110]) probiert werden. Schlägt TA1 fehl, SOLLTE TA1 mit *static binding* probiert werden. Die notwendigen Informationen für die Durchführung von TA stammen dabei aus Ergebnissen des PACE-Protokolls. Wurde TA1 erfolgreich durchgeführt, kann ein Zugriff auf DG3 erfolgen. Weitere vorhandene Datengruppen können im Anschluss ebenfalls vom Chip gelesen werden.

5.4.2.3 Protokollablauf Version 3

Kontrollanwendungen MÜSSEN den Prozessablauf aus Abbildung 8 implementieren und

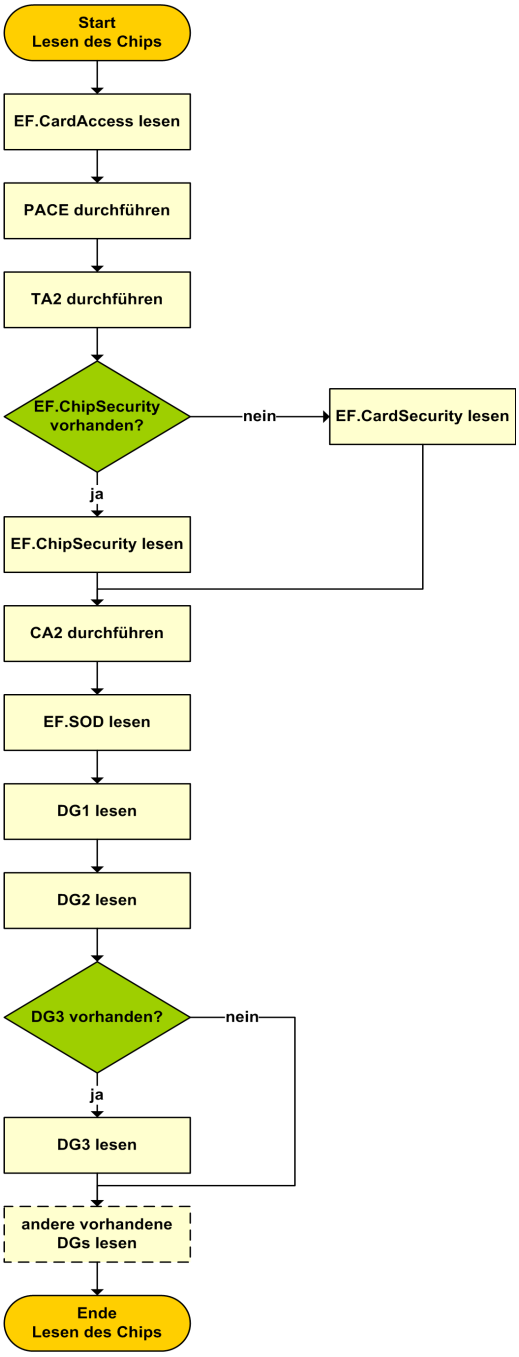

Abbildung 8: Protokollablauf Version 3

unterstützen.

Für den Zugriff auf das Dokument MUSS PACE durchgeführt werden. Dafür muss die Datei EF.CardAccess gelesen werden. Im Anschluss an PACE wird TA in der Version 2 durchgeführt. Sofern die Datei EF.ChipSecurity vorhanden ist, wird diese gelesen. Ist die Datei nicht vorhanden, wird EF.CardSecurity gelesen, um die notwendigen Daten für CA in der Version 2 zu erhalten. Basierend auf dem vorhandenen Schlüsselmaterial MUSS CA2 dann durchgeführt werden.

Danach können alle Datengruppen vom Dokument gelesen werden. Dazu gehören z. B. EF.SOD, DG1, DG2, DG3 und alle anderen auf dem Dokument gespeicherten Datengruppen.

5.4.3 Prüfung der Chipkommunikations- und Zugriffsprotokolle

Bei der Prüfung der Chipkommunikations- und Zugriffsprotokolle handelt es sich nicht um eine Dokumentenprüfung im eigentlichen Sinne, sondern um die Prüfung der erfolgreichen Durchführung oder Anwendung bestimmter Kommunikations- und Zugriffsprotokolle. Diese Protokolle sind Teil einer vollständigen elektronischen Dokumentenprüfung und werden entsprechend protokolliert, stellen aber für sich gesehen keine eigenständige Prüfung dar, anhand derer beispielsweise eine Fälschung oder Verfälschung eines elektronischen Ausweisdokuments unmittelbar erkannt werden kann. Das Fehlschlagen oder Nichtvorhandensein bestimmter Chipkommunikations- und Zugriffsprotokolle kann jedoch Indiz für ein möglicherweise manipuliertes oder sogar vollständig gefälschtes Dokument sein, wenn beispielsweise die Unterstützung eines festgelegten Protokolls für ein Dokument einer bestimmten Serie bindend ist, d. h. unterstützt und durchführbar sein MUSS.

5.4.3.1 Aufbau eines sicheren Kommunikationskanals über BAC oder PACE

Wie in Abschnitt 5.4.2 beschrieben, ist in Abhängigkeit vom vorliegenden Dokument entweder BAC oder PACE durchzuführen, um einen über die Luftschnittstelle sicheren Chipzugriff zu gewährleisten, es sei denn, es ist bekannt, dass das Dokument weder BAC noch PACE unterstützt. Die einzelnen Prüfergebnisse sind den folgenden Unterabschnitten zu entnehmen und werden in folgendes Gesamtergebnis zusammengefasst. Zusätzlich besteht die Möglichkeit, dass ein Dokument sowohl PACE als auch BAC unterstützt. In diesem Fall KANN der Bedarfsträger festlegen, welches Protokoll primär zu verwenden ist. Die Ergebnisse der einzelnen Schritte sind entsprechend der folgenden Tabellen zu protokollieren.

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn entweder BAC oder PACE erfolgreich durchgeführt werden konnte.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn BAC oder PACE durchgeführt wurde, das durchgeführte Protokoll aber fehlgeschlagen ist. Der Secure-Messaging-Kanal konnte nicht erfolgreich aufgebaut werden.
unbestimmt (undetermined)	Dieser Wert kann hier nicht auftreten.
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn für den Zugriff auf das Dokument weder die Durchführung von BAC noch PACE notwendig ist (Zugriff auf das Dokument ist unverschlüsselt möglich). Es ist jedoch nicht erforderlich, für ein Dokument, welches mit BAC oder PACE gelesen werden kann, zu prüfen, ob der Zugriff nicht auch ohne BAC/PACE möglich gewesen wäre.

Prüfergebnis	*Beschreibung*
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, BAC oder PACE durchzuführen. Dieses Prüfergebnis tritt nur auf, wenn ein Applikationsszenario keine Anwendung von BAC oder PACE vorsieht.

Tabelle 18: Protokollprüfergebnisse Chipzugriff BAC

Chipzugriff über BAC

Das Ergebnis des Chipzugriffs für BAC MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn BAC erfolgreich durchgeführt werden konnte.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn BAC durchgeführt wurde, das durchgeführte Protokoll aber fehlgeschlagen ist. Der Secure-Messaging-Kanal konnte nicht erfolgreich aufgebaut werden.
unbestimmt (undetermined)	Dieser Wert kann hier nicht auftreten.
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn für den Zugriff auf das Dokument die Durchführung von BAC nicht notwendig ist (Zugriff auf das Dokument ist möglicherweise unverschlüsselt oder mit PACE möglich). Es ist nicht erforderlich, für ein Dokument, welches mit BAC gelesen werden kann, zu prüfen, ob der Zugriff auch ohne BAC möglich gewesen wäre.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, BAC durchzuführen. Dieses Prüfergebnis tritt nur auf, wenn ein Applikationsszenario keine Anwendung von BAC vorsieht.

Tabelle 19: Protokollprüfergebnisse Chipzugriff BAC

Chipzugriff über PACE

Das Ergebnis des Chipzugriffs für PACE MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn PACE erfolgreich durchgeführt werden konnte.

Prüfergebnis	*Beschreibung*
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn PACE durchgeführt wurde, das durchgeführte Protokoll aber fehlgeschlagen ist. Der Secure-Messaging-Kanal konnte nicht erfolgreich aufgebaut werden.
unbestimmt (undetermined)	Dieser Wert kann hier nicht auftreten.
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn für den Zugriff auf das Dokument die Durchführung von PACE nicht notwendig ist (Zugriff auf das Dokument ist möglicherweise unverschlüsselt oder mit BAC möglich). Es ist nicht erforderlich, für ein Dokument, welches mit PACE gelesen werden kann, zu prüfen, ob der Zugriff auch ohne PACE möglich gewesen wäre.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, PACE durchzuführen. Dieses Prüfergebnis tritt nur auf, wenn ein Applikationsszenario keine Anwendung von PACE vorsieht.

Tabelle 20: Protokollprüfergebnisse Chipzugriff PACE

5.4.3.2 Zugriffsprüfung mittels Terminal Authentication (TA)

Um sensible Daten vom Dokument auslesen zu können (z. B. biometrische Daten wie z. B. Fingerabdrücke), muss bei entsprechend geschützten Chips vor dem Lesezugriff eine entsprechende (Lese-)Berechtigung vorgewiesen werden. Gemäß Abschnitt 5.4.2 muss dazu TA durchgeführt werden können. Die in Kapitel 5.4.1 definierten Anforderungen an die Architektur der PKI gemäß der dort referenzierten Technischen Richtlinien MÜSSEN beachtet und entsprechend umgesetzt werden.

Das Ergebnis von TA MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn TA erfolgreich durchgeführt werden konnte und das Terminal berechtigt ist, die sensitiven Daten vom Chip zu lesen.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn das TA-Protokoll fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Durchführung von TA fehlen (z. B. keine Verbindung zum Inspektionssystem, fehlende Zertifikate).
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn das Dokument TA nicht unterstützt.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn TA nicht durchgeführt wurde. Die Berechtigungen des Terminals wurden nicht geprüft.

Tabelle 21: Zugriffsprotokollergebnis Berechtigungen des Terminals

5.4.4 Prüfung der Chipechtheit (AA, CA)

Um die Echtheit des elektronischen Chips zu prüfen, MÜSSEN wie in Abschnitt 5.4.2 beschrieben, die Protokolle CA oder AA durchgeführt werden. Die einzelnen Prüfergebnisse aus AA bzw. CA sind den folgenden Unterabschnitten zu entnehmen und werden in folgendes Gesamtergebnis zusammengefasst.

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn AA *und/oder* CA erfolgreich durchgeführt werden konnten.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Protokolle AA und CA durchgeführt wurden, die Durchführung **beider** Protokolle jedoch jeweils fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn mittels beider Protokolle die Chipechtheitsprüfung weder mit AA noch mit CA bestimmt werden konnte (z. B. fehlende Informationen für die Prüfung).
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn weder AA noch CA durchgeführt werden konnte (z. B. weil das Dokument die beiden Protokolle nicht unterstützt). Die Chipechtheit wurde nicht geprüft.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, AA *und/oder* CA durchzuführen. Dieses Prüfergebnis tritt nur auf, wenn ein Applikationsszenario keine Prüfung der Chipechtheit vorsieht.

Tabelle 22: Gesamtergebnis Prüfung der Chipechtheit (AA, CA)

5.4.4.1 Prüfung der Chipechtheit mittels AA

Das Ergebnis der Prüfung der Chipechtheit mittels AA gemäß [ICAO9303] MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn AA erfolgreich durchgeführt werden konnte und die jeweilige Prüfung nicht fehlgeschlagen ist.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn AA durchgeführt wurde, das durchgeführte Protokoll aber fehlgeschlagen ist, obwohl die notwendigen Daten auf dem Chip verfügbar sind.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn das Ergebnis der Chipechtheitsprüfung nicht bestimmt werden kann (z. B. wegen fehlender Informationen für die Prüfung).

Prüfergebnis	*Beschreibung*
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn AA nicht durchgeführt werden konnte (z. B. weil das Dokument AA nicht unterstützt).
nicht durchgeführt (not performed)	Das Prüfergebnis ist als „nicht durchgeführt“ zu bewerten, wenn die Option AA gemäß Protokollablauf in Version 1 oder 2 nicht ausgeführt wurde.

Tabelle 23: Prüfergebnisse Chipechtheit AA

Wenn der Defekt *Active Authentication Private Keys Compromised* im Zuge dieser Prüfung auftritt, MÜSSEN die Anforderungen aus Abschnitt 5.6.1.1.4 umgesetzt werden.

5.4.4.2 Prüfung der Chipechtheit mittels CA

Das Ergebnis der Prüfung der Chipechtheit mittels CA gemäß [TR-03110] MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn CA erfolgreich durchgeführt werden konnte und die jeweilige Prüfung nicht fehlgeschlagen ist.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn CA durchgeführt wurde, das durchgeführte Protokoll aber fehlgeschlagen ist, obwohl die notwendigen Daten auf dem Chip verfügbar sind.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn das Ergebnis der Chipechtheitsprüfung nicht bestimmt werden kann (z. B. fehlende Informationen für die Prüfung).
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn CA nicht durchgeführt werden konnte (weil das Dokument CA nicht unterstützt).
nicht durchgeführt (not performed)	Dieser Fall kann hier nicht auftreten, da CA in allen Protokollabläufen verpflichtend durchzuführen ist.

Tabelle 24: Prüfergebnisse Chipechtheit CA

Wenn der Defekt *Chip Authentication Private Keys Compromised* im Zuge dieser Prüfung auftritt, MÜSSEN die Anforderungen aus Abschnitt 5.6.1.1.3 umgesetzt werden.

5.4.5 Prüfung der elektronischen Daten (PA)

Nach dem elektronischen Lesen des Chips MÜSSEN die gelesenen Daten des Dokuments verifiziert werden. Dieser Verifikationsprozess wird durch PA gemäß [ICAO9303] definiert.

Die Vertrauenswürdigkeit der PA ist nur sichergestellt, wenn vertrauenswürdige Zertifikate (DS und CSCA) verwendet werden. Wenn nicht sichergestellt werden kann, dass ein DS-Zertifikat aus einer vertrauenswürdigen Quelle stammt oder von einer offiziellen, vertrauenswürdigen CSCA ausgestellt wurde, ist die Integrität des Ergebnisses dieses Verifikationsprozesses nicht gegeben. Daher MÜSSEN Inspektionssysteme ihre Zertifikate aus einem vertrauenswürdigen Zertifikatsspeicher

beziehen. Die Prüfung vertrauenswürdiger Zertifikate erfolgt gemäß Abschnitt 5.4.1 anhand von Masterlisten, die dem Inspektionssystem vom hoheitlichen DV zur Verfügung gestellt werden. Prozesse zur Sicherstellung eines korrekten und vertrauenswürdigen Inhalts der Masterlisten und das Masterlistenformat werden in [ICAO-ML] beschrieben.

In den folgenden Abschnitten werden die einzelnen Prüfungen des Verifikationsprozesses beschrieben. Abbildung 9 stellt die elektronische Dokumentenprüfung grafisch dar. Eine Onlineverbindung des IS in Richtung DVCA ist nicht in jedem Szenario zwingend notwendig, jedoch stets dann, wenn für die Bestimmung von digitalen Signaturen die notwendigen Zertifikate aktuell sein müssen oder (tages-)aktuelle Defekte verarbeitet werden können müssen. Zudem kann es im Wege der Zugriffsberechtigung der EAC-PKI notwendig sein, Berechtigungszertifikate zu aktualisieren und zu verteilen.

Im Rahmen (grenz-)polizeilicher Kontrollszenarien können die einzelnen Knotenpunkte (IS, DVCA, CVCA, N-PKD) der PKIs nur dann angemessen genutzt werden, wenn sie über aktuelles Schlüssel- und Zertifikatsmaterial verfügen, welches über eine Onlineverbindung zur Verfügung gestellt wird. Offlineszenarien werden insbesondere für aktive (grenz-)polizeilichen Kontrollszenarien im Kontext dieser Technische Richtlinie daher ausdrücklich NICHT EMPFOHLEN.

5.4.5.1 Verifikation der Sicherheitsobjekte

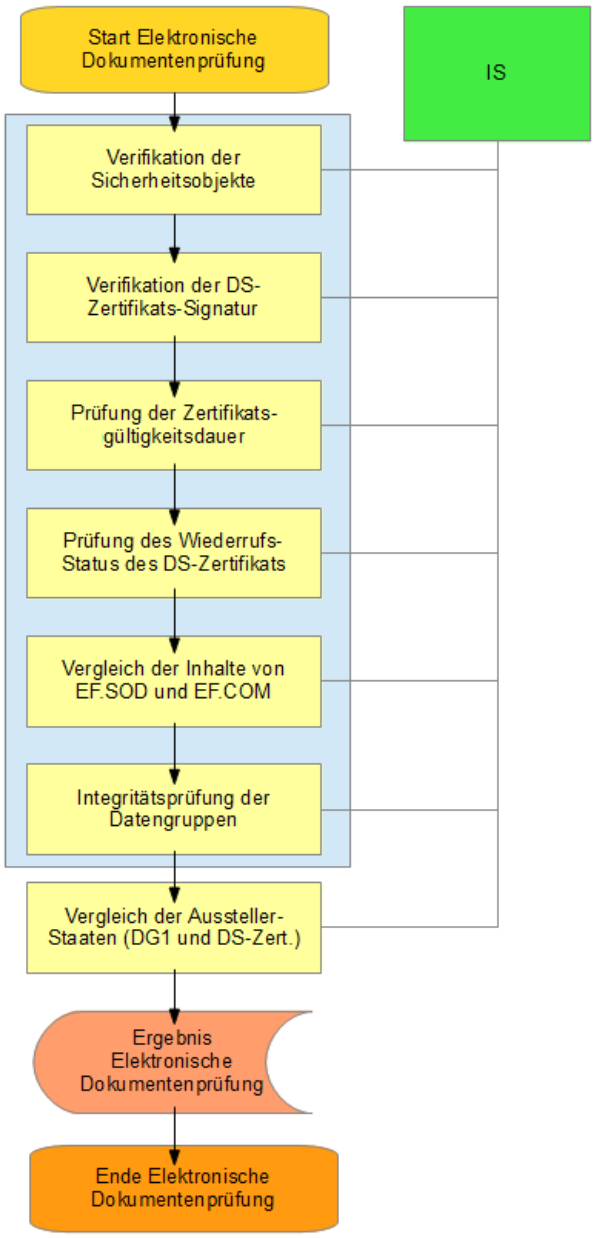

Abbildung 9: Ablauf der elektronischen Dokumentenprüfung

Die gelesenen Sicherheitsobjekte des Dokuments MÜSSEN bzgl. ihrer Echtheit geprüft werden, was technisch eine Prüfung der Chipsignatur impliziert. Die folgenden Sicherheitsobjekte MÜSSEN dabei geprüft werden, sofern sie vorhanden sind:

- **EF.SOD:** Struktur definiert nach [ICAO9303].
- **EF.CardSecurity:** Struktur definiert nach [TR-03110].
- **EF.ChipSecurity:** Struktur definiert nach [TR-03110].

Inspektionssysteme MÜSSEN die in der *SignedData*-Struktur enthaltene digitale Signatur verifizieren. Um diese Prüfung durchführen zu können, wird ein DS-Zertifikat für das

entsprechende Sicherheitsobjekt benötigt. Da in der *SignedData*-Struktur auch der Hashwert gespeichert ist, MUSS dieser mit dem aus dem gelesenen Sicherheitsobjekt berechneten Hashwert verglichen werden. Schlägt diese Hashwert-Prüfung fehl, ist die gesamte Prüfung als *fehlgeschlagen* zu interpretieren.

In der Praxis werden viele Dokumente ausgestellt, die bereits das entsprechende DS-Zertifikat im Chip speichern. Inspektionssysteme MÜSSEN in der Lage sein, Sicherheitsobjekte mit einem, mehreren oder keinen DS-Zertifikaten zu verarbeiten. Entsprechend MÜSSEN Inspektionssysteme auch in der Lage sein, die passenden DS-Zertifikate vom Inspektionssystem (gemäß Kapitel 5.4.1) zu beziehen, wenn diese nicht auf dem Dokument selbst gespeichert sind.

5.4.5.1.1 Verifikation EF.SOD (Gesamtergebnis, Hash- und Signatur-Verifikation)

Die Verifikation von EF.SOD besteht aus der Verifikation des Hashes und Verifikation der Signatur (siehe Tabelle 26 und Tabelle 27). Beide Teilergebnisse MÜSSEN für die Bestimmung des Endergebnisses der Verifikation EF.SOD herangezogen werden.

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Prüfung des Hashwerts und die Signatur-Verifikation von EF.SOD erfolgreich waren.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Hash- bzw. Signatur-Verifikation von EF.SOD fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Verifikation der Sicherheitsobjekte fehlen (z. B. DS-Zertifikat fehlt).
nicht unterstützt (not supported)	Dieser Wert kann nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Hash- bzw. Signatur-Verifikation durchzuführen.

Tabelle 25: Prüfergebnisse der Verifikation von EF.SOD

Verifikation des Hashwerts von EF.SOD

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Prüfung des Hashwerts von EF.SOD erfolgreich war.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Hash-Verifikation von EF.SOD fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Verifikation der Sicherheitsobjekte fehlen.

Prüfergebnis	*Beschreibung*
nicht unterstützt (not supported)	Dieser Wert kann nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Hash-Verifikation durchzuführen.

Tabelle 26: Verifikation des Hashwerts von EF.SOD

Verifikation der Signatur von EF.SOD

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Signatur-Verifikation von EF.SOD erfolgreich war.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Signatur-Verifikation von EF.SOD fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Verifikation der Sicherheitsobjekte fehlen (z. B. DS-Zertifikat fehlt).
nicht unterstützt (not supported)	Dieser Wert kann nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Signatur-Verifikation durchzuführen.

Tabelle 27: Verifikation Signatur von EF.SOD

5.4.5.1.2 Verifikation EF.CardSecurity (Gesamtergebnis, Hash- und Signatur-Verifikation)

Die Verifikation von EF.CardSecurity besteht aus der Verifikation des Hashes und Verifikation der Signatur (siehe Tabelle 29 und Tabelle 30). Beide Teilergebnisse MÜSSEN für die Bestimmung des Endergebnisses der Verifikation EF.CardSecurity herangezogen werden.

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Prüfung des Hashwerts und die Signatur-Verifikation von EF.CardSecurity erfolgreich waren.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Hash- bzw. Signatur-Verifikation von EF.CardSecurity fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Verifikation fehlen (z. B. DS-Zertifikat fehlt).

Prüfergebnis	*Beschreibung*
nicht unterstützt (not supported)	Dieser Wert kann nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Hash- bzw. Signatur-Verifikation durchzuführen.

Tabelle 28: Prüfergebnisse der Verifikation von EF.CardSecurity

Verifikation des Hashwerts von EF.CardSecurity

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Prüfung des Hashwerts von EF.CardSecurity erfolgreich war.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Hash-Verifikation von EF.CardSecurity fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Hash-Verifikation fehlen.
nicht unterstützt (not supported)	Dieser Wert kann nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Hash-Verifikation durchzuführen.

Tabelle 29: Verifikation des Hashwerts von EF.CardSecurity

Verifikation der Signatur von EF.CardSecurity

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Signatur-Verifikation von EF.CardSecurity erfolgreich war.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Signatur-Verifikation von EF.CardSecurity fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Signatur-Verifikation fehlen (z. B. DS-Zertifikat fehlt).
nicht unterstützt (not supported)	Dieser Wert kann nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Signatur-Verifikation durchzuführen.

Tabelle 30: Verifikation Signatur von EF.CardSecurity

5.4.5.1.3 Verifikation EF.ChipSecurity (Gesamtergebnis, Hash- und Signatur-Verifikation)

Die Verifikation von EF.ChipSecuritry besteht aus der Verifikation des Hashes und Verifikation der Signatur (siehe Tabelle 32 und Tabelle 33). Beide Teilergebnisse MÜSSEN für die Bestimmung des Endergebnisses der Verifikation EF.ChipSecurity herangezogen werden.

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Prüfung des Hashwerts und die Signatur-Verifikation von EF.ChipSecurity erfolgreich waren.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Hash- bzw. Signatur-Verifikation von EF.ChipSecurity fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Verifikation fehlen (z. B. DS-Zertifikat fehlt).
nicht unterstützt (not supported)	Dieser Wert kann nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Hash- bzw. Signatur-Verifikation durchzuführen.

Tabelle 31: Prüfergebnisse der Verifikation von EF.ChipSecurity

Verifikation des Hashwerts von EF.ChipSecurity

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Prüfung des Hashwerts von EF.ChipSecurity erfolgreich war.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Hash-Verifikation von EF.ChipSecurity fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Hash-Verifikation fehlen.
nicht unterstützt (not supported)	Dieser Wert kann nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Hash-Verifikation durchzuführen.

Tabelle 32: Verifikation des Hashwerts von EF.ChipSecurity

Verifikation der Signatur von EF.ChipSecurity

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Signatur-Verifikation von EF.ChipSecurity erfolgreich war.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Signatur-Verifikation von EF.ChipSecurity fehlgeschlagen ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Signatur-Verifikation fehlen (z. B. DS-Zertifikat fehlt).
nicht unterstützt (not supported)	Dieser Wert kann nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Signatur-Verifikation durchzuführen.

Tabelle 33: Verifikation Signatur von EF.ChipSecurity

5.4.5.1.4 Gesamtergebnis der Verifikation

Jedes der oben angeführten Sicherheitsobjekte MUSS, sofern vorhanden, verifiziert und das jeweilige Gesamtergebnis in das nun folgende Gesamtergebnis der Verifikation abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die digitalen Signaturen ALLER vorhandenen Sicherheitsobjekte erfolgreich geprüft werden konnte und die Hashwerte identisch sind.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Verifikation mindestens eines Sicherheitsobjekts fehlschlägt (z. B. weil die Signatur nicht verifiziert werden kann oder weil die Hashwert-Prüfung fehlschlägt).
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Verifikation der Sicherheitsobjekte fehlen (z. B. DS-Zertifikat fehlt).
nicht unterstützt (not supported)	Dieser Wert kann für das Gesamtergebnis der Verifikation der Sicherheitsobjekte nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Verifikation der Sicherheitsobjekte durchzuführen.

Tabelle 34: Prüfergebnisse der Verifikation der Sicherheitsobjekte

Wenn der Defekt *Document Security Object Malformed* im Zuge dieser Prüfung auftritt, MÜSSEN die Anforderungen aus Abschnitt 5.6.1.2.2 umgesetzt werden.

Wenn der Defekt *Card Security Object Malformed* im Zuge dieser Prüfung auftritt, MÜSSEN die Anforderungen aus Abschnitt 5.6.1.3.1 umgesetzt werden.

Wenn der Defekt *Chip Security Object Malformed* im Zuge dieser Prüfung auftritt, MÜSSEN die Anforderungen aus Abschnitt 5.6.1.3.2 umgesetzt werden.

5.4.5.2 Prüfung der Ausstellerzertifikate

Die Prüfung der Ausstellerzertifikate enthält die in den folgenden Unterabschnitten definierten Teilprüfungen. Für jedes vorhandene Sicherheitsobjekt

- EF.SOD
- EF.CardSecurity
- EF.ChipSecurity

MÜSSEN die Ausstellerzertifikate gemäß den Unterabschnitten 5.4.5.2.1 ff. geprüft werden. Dafür sind die in Kapitel 5.4.1 definierten Anforderungen an die Architektur des Inspektionssystems umzusetzen.

Das Ergebnis der Prüfung der Ausstellerzertifikate MUSS für jedes der drei Sicherheitsobjekte in den folgenden Werten abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Prüfung des Ausstellerzertifikats des jeweiligen Sicherheitsobjekts erfolgreich durchgeführt werden konnte.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn die Prüfung des Ausstellerzertifikats für das jeweilige Sicherheitsobjekt fehlschlägt.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Durchführung der Prüfung fehlen.
nicht unterstützt (not supported)	Dieser Wert kann hier nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn das Ausstellerzertifikat des Sicherheitsobjekts nicht geprüft wurde.

Tabelle 35: Prüfergebnisse der Ausstellerzertifikate für ein Sicherheitsobjekt

Beim Auftreten des Defekts *Document Signer Certificate Malformed* bei einer der Prüfungen in den folgenden Unterabschnitten MÜSSEN die Anforderungen aus Abschnitt 5.6.1.1.2 umgesetzt werden.

Beim Auftreten des Defekts *Document Signer Certificate incorrectly encoded or malformed* bei einer der Prüfungen in den folgenden Unterabschnitten MÜSSEN die Anforderungen aus Abschnitt 5.6.1.1.5 umgesetzt werden.

Abhängig vom Einsatzszenario unterscheiden sich die Prüfergebnisse, falls eines der Zertifikate zum Zeitpunkt der Prüfung nicht gültig ist (vgl. 5.4.5.2.2) wie folgt:

Prüfung der Zertifikatsgültigkeitsdauer in Self-Service-Systemen

Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn eines der Zertifikate zum Zeitpunkt der Prüfung nicht gültig ist.

Prüfung der Zertifiktasgültigkeitsdauer in stationären, teil-mobilen u. voll-mobilen Systemen

Das Prüfergebnis ist als unbestimmt zu bewerten, wenn eines der Zertifikate zum Zeitpunkt der Prüfung nicht gültig ist.

Das Gesamtergebnis der Prüfung der Ausstellerzertifikate muss zu dem folgenden Gesamtergebnis kumuliert werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn alle der beschriebenen Prüfungen bzgl. Ausstellerzertifikaten für alle Sicherheitsobjekte erfolgreich durchgeführt werden konnten.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn mindestens eine der Prüfungen bzgl. Ausstellerzertifikaten eines Sicherheitsobjekts fehlschlägt.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Durchführung von Prüfungen fehlen.
nicht unterstützt (not supported)	Dieser Wert kann hier nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn keine Prüfung der Ausstellerzertifikate für alle Sicherheitsobjekte durchgeführt wurde (d. h. nicht geprüft).

Tabelle 36: Kumuliertes Gesamtprüfergebniss der Ausstellerzertifikate

5.4.5.2.1 Verifikation der DS-Zertifikats-Signatur

Die Prüfung der Zertifikatskette bis zu einem bekannten, vertrauenswürdigen Zertifikat ist ein essenzieller Schritt im gesamten Verifikationsprozess. Wenn nicht verifiziert werden kann, dass ein DS-Zertifikat von einer vertrauenswürdigen Quelle stammt oder von einer offiziellen, vertrauenswürdigen CSCA[13] ausgestellt wurde, kann den Ergebnissen der anderen Sicherheitsüberprüfungen nicht vertraut werden. Die Ausgabe einer Verifikation SOLLTE zudem klar zwischen verifiziertem DS- oder CSCA-Zertifikat unterscheiden, um dem Anwender anzuzeigen, welches Zertifikat letztlich zu welcher Meldung geführt hat.

Es gelten die folgenden Anforderungen an die Inspektionssysteme:

- Wenn die digitale Signatur des Sicherheitsobjekts (siehe auch 5.4.5.1) mit dem DS-Zertifikat, das auf dem Dokument gespeichert ist oder aus einer nicht vertrauenswürdigen Quelle stammt (z. B. eine nicht authentifizierte Datenbank), verifiziert wurde, MÜSSEN Inspektionssysteme auch die Signatur des DS-Zertifikats verifizieren. Es MUSS das DS-Zertifikat gegen das zugehörige CSCA-Zertifikat aus der aktuell gültigen Masterliste geprüft werden.

13 Z.B. CSCA-Zertifikate aus einer von hoheitlicher Stelle vertrauenswürdig veröffentlichten Masterliste.

- Wenn das DS-Zertifikat im TCC als vertrauenswürdig eingestuft ist, KANN die Verifikation der DS-Zertifikats-Signatur übersprungen werden.
- Neben wenigen Ausnahmen werden DS-Zertifikate normalerweise direkt im Dokument im entsprechenden Sicherheitsobjekt (EF.SOD, EF.CardSecurity, EF.ChipSecurity) gespeichert. Deswegen ist es in der Praxis häufig so, dass dieses DS-Zertifikat für die Prüfung der digitalen Signatur im Sicherheitsobjekt und das dazu entsprechende CSCA-Zertifikat für die Verifikation dieses DS-Zertifikats verwendet werden. Um dies durchführen zu können, müssen Inspektionssysteme das zugehörige CSCA-Zertifikat aus einer Menge an Zertifikaten im Zertifikatsspeicher suchen. Die Suche des passenden CSCA-Zertifikats erfolgt mit folgenden Mechanismen:
  - Es wird EMPFOHLEN, dass Inspektionssysteme die *AuthorityKeyIdentifier*-Erweiterung aus dem DS-Zertifikat extrahieren und damit das eigentliche CSCA-Zertifikat mit der entsprechenden *SubjectKeyIdentifier*-Erweiterung suchen.
  - Obwohl diese Erweiterung gemäß [ICAO9303] verpflichtend ist, gibt es Länder, die Dokumente ohne diese Erweiterungen ausstellen. Deshalb wird ausschließlich in diesen Fällen EMPFOHLEN, wenn kein passendes CSCA-Zertifikat über die Zertifikatserweiterungen gefunden werden kann, dass Inspektionssysteme die Suche des CSCA-Zertifikats (basierend auf dem Antragssteller (*Subject*)) anhand der Aussteller-Informationen (*Issuer*) des DS-Zertifikats durchführen. Werden hierbei ein oder mehrere passende CSCA-Zertifikate gefunden, MUSS die DS-Zertifikats-Signatur-Prüfung als erfolgreich betrachtet werden, wenn die Prüfung der digitalen Signatur mit einem der gefundenen CSCA-Zertifikate erfolgreich war und der Inhaber (*Subject*) des CSCA-Zertifikats mit dem Aussteller (*Issuer*) des DS-Zertifikats übereinstimmt.[14]
- Liegt ausschließlich ein CSCA-Link-Zertifikat vor, DARF die digitale Signatur dieses CSCA-Link-Zertifikats NICHT verifiziert werden, da die Überprüfung fehlschlagen würde.[15]

Die Prüfergebnisse der Verifikation der DS-Zertifikats-Signatur MÜSSEN in den folgenden Werten abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn alle der in diesem Abschnitt genannten Kriterien erfüllt werden und die Signatur des DS-Zertifikats erfolgreich geprüft werden kann.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn mindestens eine der in diesem Abschnitt genannten Kriterien nicht erfüllt wird und die Signatur des DS-Zertifikats nicht erfolgreich geprüft werden kann.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Durchführung von Prüfungen fehlen (z. B. Nichtverfügbarkeit eines CSCA-Zertifikats).

14 Bei der Suche über den Ausstellernamen kann daher nicht „failed“ als Ergebnis auftreten.

15 Bei selbst-signierten CSCA-Zertifikaten wird EMPFOHLEN, dass die digitale Signatur des CSCA-Zertifikats nicht verifiziert wird, da einige Länder CSCA-Zertifikate ausstellen, die nicht einwandfrei selbst-signiert sind. Da alle gültigen und vertrauenswürdigen CSCA-Zertifikate auf Masterlisten verzeichnet sein müssen, wird dies nicht als eine Verminderung der Sicherheit betrachtet.

Prüfergebnis	*Beschreibung*
nicht unterstützt (not supported)	Dieser Wert kann hier nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn die DS-Zertifikats-Signatur nicht verifiziert wird.

Tabelle 37: Prüfergebnisse der Verifikation der DS-Zertifikats-Signatur

5.4.5.2.2 Prüfung der Zertifikatsgültigkeitsdauer

Inspektionssysteme MÜSSEN prüfen, dass die aktuelle Zeit (= Zeitpunkt, an dem die Prüfung durchgeführt wird) innerhalb der Gültigkeitsdauer des DS-Zertifikats liegt. Zusätzlich MÜSSEN Inspektionssysteme auch sicherstellen, dass die aktuelle Ortszeit zwischen Beginn und Ende der Gültigkeit des CSCA-Zertifikats liegt. Es wird daher EMPFOHLEN, der Kontrollanwendung durch einen geeigneten Zeitdienst die korrekte aktuelle Zeit bereitzustellen.

Das Ergebnis der Prüfung der Zertifikatsgültigkeitsdauer MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn beide Zertifikate zum Zeitpunkt der Prüfung gültig sind.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn eines der Zertifikate zum Zeitpunkt der Prüfung nicht gültig ist.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Prüfung der Zertifikatsgültigkeitsdauer fehlen (z. B. keine Verbindung zum Inspektionssystem).
nicht unterstützt (not supported)	Dieser Wert kann hier nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn die Prüfung der Zertifikatsgültigkeitsdauer nicht durchgeführt wurde.

Tabelle 38: Prüfergebnisse der Zertifikatsgültigkeitsdauer

5.4.5.2.3 Prüfung des Widerruf-Status des DS-Zertifikats

Die Prüfung des Widerruf-Status des DS-Zertifikats ist ein verpflichtender Schritt bei der PA. Deshalb MÜSSEN Inspektionssysteme den Widerruf-Status anhand von Defektlisten prüfen. Wenn der Defekt *Document Signer Certificate Revoked* in der Defektliste enthalten ist, MÜSSEN der Vertrauensstatus des DS-Zertifikats gemäß Abschnitt 5.6.1.1.1 gesetzt und die Anforderungen an das Prüfergebnis ebenfalls aus Abschnitt 5.6.1.1.1 umgesetzt werden.

Das Ergebnis der Prüfung des Widerrufs-Status des DS-Zertifikats MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn das Zertifikat nicht widerrufen wurde.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn das Zertifikat widerrufen wurde (siehe Abschnitt 5.6.1.1.1 für Details).
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen für die Prüfung des Widerruf-Status fehlen oder der Vertrauensstatus gemäß Abschnitt 5.6.1.1.1 auf unbestimmt gesetzt wird.
nicht unterstützt (not supported)	Dieser Wert kann hier nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn die Prüfung des Widerruf-Status des DS-Zertifikats nicht durchgeführt wurde.

Tabelle 39: Prüfergebnisse des Widerruf-Satus des DS-Zertifikats

5.4.5.3 Integrität der Chipinhalte

Die Prüfung der Integrität der Chipinhalte enthält die in den folgenden Abschnitten definierten Teilprüfungen.

Das Ergebnis dieser Prüfungen MUSS in den folgenden Werten abgebildet werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn alle in den folgenden Abschnitten beschriebenen Prüfungen erfolgreich durchgeführt werden konnten, die Inhalte von EF.SOD und EF.COM übereinstimmen und die Hashwerte aller gelesenen Datengruppen mit den Hashwerten aus EF.SOD übereinstimmen.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn mindestens eine der in den folgenden Abschnitten beschriebenen Prüfungen zu einem fehlgeschlagenen Integritätstest führt.
unbestimmt (undetermined)	Dieser Wert kann für diese Prüfung nicht auftreten.
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn die Prüfung technisch nicht durchgeführt werden konnte (z. B. nicht unterstützter Hashalgorithmus).
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn keine der Prüfungen der folgenden Abschnitte durchgeführt wurde. Die Integrität der Chipinhalte wurde somit nicht geprüft.

Tabelle 40: Prüfergebnisse der Integrität der Chipinhalte

5.4.5.3.1 Vergleich der Inhalte von EF.SOD und EF.COM

Sofern das Dokument die beiden Dateien EF.SOD und EF.COM enthält (z. B. aktueller ePass aus Deutschland), MÜSSEN die Inhalte der beiden Dateien auf deren Konsistenz geprüft werden. Da EF.SOD keinen Hashwert von EF.COM enthält, kann eine Modifikation von EF.COM nicht alleine durch die Prüfung der digitalen Signatur von EF.SOD erkannt werden. Aus diesem Grund MÜSSEN Inspektionssysteme prüfen, dass jede Datengruppe (DG), die in EF.SOD aufgelistet ist, auch in EF.COM enthalten ist. Auch MUSS jede Datengruppe, die in EF.COM aufgelistet ist, in EF.SOD enthalten sein.

Das Ergebnis dieser Prüfung MUSS in den folgenden Werten abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn die Inhalte von EF.COM und EF.SOD konsistent zueinander sind.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn Inkonsistenzen zwischen EF.COM und EF.SOD festgestellt wurden.
unbestimmt (undetermined)	Dieser Wert kann für diese Prüfung nicht auftreten.
nicht unterstützt (not supported)	Das Prüfergebnis ist als nicht unterstützt zu bewerten, wenn mit dem vorliegenden Dokument ein Vergleich der Inhalte von EF.COM und EF.SOD nicht möglich ist (z. B. weil das Dokument nicht die beiden Dateien enthält).
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Inhalte von EF.COM und EF.SOD zu vergleichen, obwohl die beiden Dateien im Dokument vorhanden sind.

Tabelle 41: Prüfergebnisse des Vergleichs der Inhalte von EF.SOD und EF.COM

Wenn der Defekt *COM and SOD descripancy* im Zuge dieser Prüfung auftritt, MÜSSEN die Anforderungen aus Abschnitt 5.6.1.2.3 umgesetzt werden.

5.4.5.3.2 Integritätsprüfung der Datengruppen

Für jede Datengruppe, die vom Chip des Dokuments gelesen wurde und deren Inhalt für Prüfzwecke verwendet werden soll, MUSS der Hashwert berechnet und mit dem entsprechenden Hashwert aus EF.SOD verglichen werden. Inspektionssysteme DÜRFEN nur auf den Inhalt der Datengruppen vertrauen, deren Hashwerte identisch sind.

Wenn im Rahmen des Auslesevorgangs AA durchgeführt wurde, MÜSSEN Inspektionssysteme den Hashwert der Datengruppe 15 (DG15) prüfen. Wenn für die Durchführung von AA Informationen aus DG14 benötigt werden, MÜSSEN Inspektionssysteme auch den Hashwert der Datengruppe 14 (DG14) prüfen. Wenn im Rahmen des Auslesevorgangs CA1 durchgeführt wurde, MÜSSEN Inspektionssysteme auch den Hashwert der Datengruppe 14 (DG14) prüfen.

Für alle Datengruppen (DG1 bis DG16) MUSS das Ergebnis der Integritätsprüfung in den Werten der folgenden Tabelle abgebildet werden:

Prüfergebnis	*Beschreibung*
identisch (identical)	Der Integritätsstatus einer Datengruppe wird als identisch festgelegt, wenn die Datengruppe vorhanden ist, erfolgreich gelesen wurde und der Hashwert der gelesenen Datengruppe identisch mit dem Hashwert aus EF.SOD ist.
nicht identisch (not identical)	Der Integritätsstatus einer Datengruppe wird als nicht identisch festgelegt, wenn die Datengruppe vorhanden ist, erfolgreich gelesen wurde, aber der Hashwert der gelesenen Datengruppe nicht identisch mit dem Hashwert aus EF.SOD ist.
vorhanden (present)	Der Integritätsstatus einer Datengruppe wird als vorhanden festgelegt, wenn die Datengruppe vorhanden ist, aber nicht vom Dokument gelesen wurde.
nicht vorhanden (not present)	Der Integritätsstatus einer Datengruppe wird als nicht vorhanden festgelegt, wenn die Datengruppe nicht auf dem Dokument enthalten ist.

Tabelle 42: Einzelprüfergebnisse der Integritätsprüfung der Datengruppen

Wenn der Defekt *Data Group Malformed* in der Defektliste geführt und in einer Datengruppe identifiziert werden kann, müssen die Anforderungen aus Abschnitt 5.6.1.2.1 umgesetzt werden.

Als Gesamtprüfergebnis der Integritätsprüfung aller Datengruppen MÜSSEN die Werte aus der folgenden Tabelle übernommen werden:

Prüfergebnis	*Beschreibung*
erfolgreich (successful)	Das Gesamtprüfergebnis ist als erfolgreich einzustufen, wenn alle für das Anwendungsszenario zwingend benötigten Datengruppen gelesen und die betreffenden Hashwerte als identisch eingestuft wurden.
fehlgeschlagen (failed)	Die Gesamtprüfung ist als fehlgeschlagen zu bewerten, wenn mindestens eine der verwendeten bzw. gelesenen Datengruppen den Integritätswert nicht identisch erhalten hat.
unbestimmt (undetermined)	Das Gesamtprüfergebnis ist als unbestimmt zu bewerten, wenn nicht alle für das Anwendungsszenario zwingend benötigten Datengruppen gelesen wurden.
nicht unterstützt (not supported)	Dieser Wert kann hier nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Integrität der Datengruppen festzustellen.

Tabelle 43: Gesamtprüfergebnisse der Integritätsprüfung aller Datengruppen (DG1 bis DG16)

5.4.5.4 Vergleich der Ausstellerstaaten (DG1 und DS-Zertifikat)

Inspektionssysteme MÜSSEN das Länderattribut aus dem Ausstellernamen (*Issuer*) des DS-Zertifikats extrahieren und mit der Information des Ausstellerstaats in der Datengruppe 1 (DG1)

vergleichen. Diese Prüfung kann nur durchgeführt werden, wenn die folgenden Bedingungen erfüllt sind:

- Eine Zuordnungstabelle[16] mit den eindeutigen Zuweisungen zwischen ICAO 3-Buchstaben-Ländercodes und ISO 2-Buchstaben-Ländercodes MUSS entsprechend [ISO3166-2] erstellt werden[17].
- Der Ausstellername (*Issuer*) des entsprechenden DS-Zertifikats enthält ein Länderattribut, welches einen gültigen ISO 2-Buchstaben-Ländercode enthält.

Folgende Prüfschritte MÜSSEN durchgeführt werden:

1. Extrahieren des ICAO 3-Buchstaben-Ländercodes aus DG1 (im Folgenden *ICAO-Ländercode* genannt).
2. Extrahieren des ISO 2-Buchstaben-Ländercodes aus dem DS-Zertifikat (im Folgenden *ISO-Ländercode* genannt).
3. Vergleichen des *ICAO-Ländercodes* und des *ISO-Ländercodes* basierend auf der definierten Zuordnungstabelle.

Das Ergebnis dieser Prüfung MUSS in den Werten der folgenden Tabelle abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn der *ICAO-Ländercode* und der *ISO-Ländercode* basierend auf den Informationen aus der Zuordnungstabelle zueinanderpassen.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn der *ICAO-Ländercode* und der *ISO-Ländercode* basierend auf den Informationen aus der Zuordnungstabelle nicht zueinanderpassen.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn Informationen zur Durchführung der Prüfung fehlen (z. B. weil ICAO-Ländercodes in der Zuordnungstabelle oder ISO-Ländercodes im DS-Zertifikat fehlen).
nicht unterstützt (not supported)	Dieser Wert kann hier nicht auftreten.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, den Vergleich der Ausstellerstaaten durchzuführen.

Tabelle 44: Prüfergebnisse des Vergleichs der Ausstellerstaaten

16 Diese Zuordnungstabelle wird in Abstimmung zwischen Technologielieferant und Anwender entsprechend den jeweils gültigen Fassungen von ISO 3166-1 und ISO 3166-2 erstellt. Dabei werden die Werte nach ISO 3166 ALPHA-2 und ALPHA-3 sowie die eventuell abweichenden Zweizeichencodes von Ländern mit territorialen Gliederungen nach ISO 3166-2 berücksichtigt. Durch den ISO 3166-1 Newsletter publizierte Änderungen und andere Anpassungen MÜSSEN in Abstimmung zwischen Technologielieferant und Anwender im vereinbarten Wartungszyklus eingearbeitet werden.

17 Diese Zuordnung ist nicht notwendigerweise für jedes Land eindeutig, so kann z. B. ein ISO 2-Buchstaben-Ländercode mehreren ICAO 3-Buchstaben-Ländercodes zugeordnet sein; auch ein ICAO 3-Buchstaben-Ländercode kann mehreren ISO 2-Buchstaben-Ländercodes zugeordnet sein.

5.5 Kombiniert optisch-physikalische und elektronische Dokumentenprüfung

In den folgenden Unterabschnitten finden sich die notwendigen Teilprüfungen der kombiniert optisch-physikalischen und elektronischen Dokumentenprüfung. Das Gesamtergebnis der Dokumentenprüfung setzt sich aus den Ergebnissen der jeweiligen Teilprüfungen zusammen und MUSS entsprechend der folgenden Tabelle abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn alle der in den Unterabschnitten vorgeschriebenen Prüfungen als erfolgreich durchgeführt einzustufen sind.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn mindestens eine der in den Unterabschnitten vorgeschriebenen Prüfungen als fehlgeschlagen einzustufen ist. Das Dokument wurde optisch-physikalisch oder elektronisch entweder fehlerhaft ausgestellt oder es besteht der Verdacht einer Manipulation.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn in mindestens einer, der in den Unterabschnitten vorgeschriebenen Prüfungen das Ergebnis als unbestimmt einzustufen ist.
nicht unterstützt (not supported)	Dieser Wert ist zu verwenden, wenn das vorliegende Dokument keine kombiniert optisch-physikalische und elektronische Dokumentenprüfung unterstützt.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die kombiniert optisch-physikalische und elektronische Dokumentenprüfung durchzuführen.

Tabelle 45: Prüfergebnisse der kombiniert optisch-physikalischen und elektronischen Dokumentenprüfung

Teilprüfungen, die in Kapitel 2 für das jeweilige Anwendungsszenario als *optional* eingestuft werden und *nicht durchgeführt* werden oder *nicht unterstützt* sind, *beeinflussen* das Gesamtergebnis dieser Dokumentenprüfung *nicht*.

Im Gegensatz dazu führen Teilprüfungen, die in Kapitel 2 für das jeweilige Anwendungsszenario als *verpflichtend* eingestuft sind und *nicht durchgeführt* werden, zu einem *unbestimmten* oder *fehlgeschlagenen* Prüfergebnis der kombiniert optisch-physikalischen und elektronischen Dokumentenprüfung. Teilprüfungen, die *nicht unterstützt* werden, *beeinflussen* das Gesamtergebnis der kombiniert optisch-physikalischen und elektronischen Dokumentenprüfung *nicht*.

5.5.1 Vergleich der optischen und elektronischen biografischen Daten (optische MRZ und DG1)

Wenn Hintergrundabfragen in Auskunftssystemen Teil des gesamten Kontrollprozesses sind, werden die Informationen für die Abfragen typischerweise aus der optisch erfassten MRZ

extrahiert, da diese Informationen in der Regel zuerst zur Verfügung stehen. Wenn ein Dokument für die Zugriffskontrolle BAC oder PACE (und die MRZ wird für den Zugriff verwendet) fordert, werden einige Daten der MRZ implizit gegen Fehler beim Lesen der MRZ geprüft, wenn das Protokoll erfolgreich durchgeführt wird. Trotzdem ist es für einen Angreifer möglich, andere Teile der MRZ, die nicht für BAC oder PACE verwendet werden (z. B. Vor- und Nachname) zu verändern.

Um solche Veränderungen zu erkennen, MÜSSEN die einzelnen Gruppenelemente (Vorname, Nachname, Ablaufdatum des Dokuments, Geburtsdatum, Geschlecht, etc.) der optisch erfassten MRZ mit den gelesenen Gruppenelementen der Datengruppe 1 (DG1) verglichen werden. Alle Gruppenelemente MÜSSEN exakt übereinstimmen. Das Gruppenelement optionale Daten ist separat zu untersuchen und führt im Fehlerfall nicht zu einem Fehlschlagen der Prüfung.

Folgende Ausnahmen in Abweichung zu [ICAO9303] sind zu beachten:

- Für das Geburtsdatum gilt dies nicht, sofern nicht alle 6 Zeichen besetzt sind und Füllzeichen verwendet werden. Die Ausnahme betrifft nur diese Füllzeichen.
- Eine weitere Ausnahme gilt für den Bereich optionale Daten.

Dieser Test kann nicht durchgeführt werden, wenn für den Zugriff auf das Dokument die CAN verwendet wurde.

Das Ergebnis dieser Prüfung MUSS in den folgenden Werten abgebildet werden:

Prüfergebnis	***Beschreibung***
erfolgreich (successful)	Das Prüfergebnis ist als erfolgreich zu bewerten, wenn gemäß der oben beschriebenen Anforderungen die Daten der DG1 mit den Daten der optischen MRZ übereinstimmen.
fehlgeschlagen (failed)	Das Prüfergebnis ist als fehlgeschlagen zu bewerten, wenn gemäß der oben beschriebenen Anforderungen Gruppenelemente (ausgenommen das Gruppenelement *optionalen Daten*) der DG1 nicht mit den Daten der optischen MRZ übereinstimmen.
unbestimmt (undetermined)	Das Prüfergebnis ist als unbestimmt zu bewerten, wenn gemäß der oben beschriebenen Anforderungen ausschließlich das Gruppenelement das Gruppenelement *optionalen Daten* der DG1 nicht mit den Daten der optischen MRZ übereinstimmt.
nicht unterstützt (not supported)	Die Prüfung muss als nicht unterstützt bezeichnet werden, wenn die CAN für den Zugriff auf das Dokument verwendet wurde.
nicht durchgeführt (not performed)	Das Prüfergebnis ist als nicht durchgeführt zu bewerten, wenn nicht versucht wurde, die Inhalte von DG1 und optischer MRZ zu vergleichen.

Tabelle 46: Prüfergebnisse des Vergleichs der Inhalte der optischen MRZ und DG1

5.6 Behandlung und Interpretation von Defekten

Defektlisten MÜSSEN gemäß der in [TR-03129-2] definierten Formate und Protokolle verarbeitet werden können, um Produktionsfehler in Dokumenten sowie Rückrufe von bereits ausgestellten Zertifikaten zu signalisieren.

Dieser Abschnitt definiert die umzusetzende Vorgehensweise der Inspektionssysteme beim Auftreten von Defekten. Entsprechend aus [TR-03129-2] nicht ableitbare, also unbekannte, Defekt MÜSSEN ignoriert werden.

5.6.1.1 Authentication-Defekte

5.6.1.1.1 Document Signer Certificate Revoked

Wenn der Defekt *Document Signer Certificate Revoked* gemäß Anhang A.2.1.1 von [TR-03129-2] für ein DS-Zertifikat gefunden wird, muss das Inspektionssystem keine weitere Prüfung des DS-Zertifikats durchführen. Des Weiteren beeinflusst der *Status-Code* des Defekts den Vertrauensstatus, der als Antwort vom Inspektionssystem an die Kontrollanwendung zurückgeliefert wird. Der erforderliche Vertrauensstatus für das jeweilige DS-Zertifikat in Abhängigkeit des *Status-Codes* des Defekts ist in der folgenden Tabelle definiert:

Status-Code	***Beschreibung des Status-Codes***	***Vertrauensstatus für das jeweilige DS-Zertifikat***
0	keine weiteren Details vorhanden	nicht vertrauenswürdig
1	Widerruf wird geprüft	unbestimmt
2	das Zertifikat wird für Testzwecke verwendet	nicht vertrauenswürdig
3	vom Aussteller zurückgerufen	nicht vertrauenswürdig
4	vom Defektlisten-Signer zurückgerufen	nicht vertrauenswürdig
5	Fehler bekannt	unbestimmt
≥ 32	proprietäre Status-Codes	unbestimmt

Tabelle 47: Vertrauensstatus-Zuweisungen für Status-Codes von Defektlisten

Ein Defekt dieses Typs hat in der Kontrollanwendung die Auswirkung, dass der vom Sperrgrund abhängige und vom Inspektionssystem gemeldete Vertrauensstatus des Zertifikats in die Teilprüfung des DS-Zertifikats einbezogen wird. Dies MUSS entsprechend zum Ergebnis *unbestimmt* oder *fehlgeschlagen* beim Ergebnis der Prüfung der elektronischen Datengruppen (siehe Abschnitt 5.4.5), beim Ergebnis der Prüfung der Ausstellerzertifikate (siehe Abschnitt 5.4.5.2) und bei der Teilprüfung des Widerruf-Status des DS-Zertifikats (siehe Abschnitt 5.4.5.2.3) führen.

5.6.1.1.2 Document Signer Certificate Malformed

Wenn der Defekt *Document Signer Certificate Malformed* gemäß Anhang A.2.1.2 von [TR-03129-2] für ein DS-Zertifikat gefunden wird, wird das von der Kontrollanwendung an das IS

gesendete DS-Zertifikat nicht weiter benutzt. Die Signaturprüfung MUSS ohne Prüfung auf gültig gesetzt werden. Die Gültigkeitsinformationen der Antwort MÜSSEN aus dem ersetzten Zertifikat genommen werden. Der Vertrauensstatus der Antwort des Inspektionssystems MUSS auf *vertrauenswürdig* gesetzt werden.

Ein Defekt dieses Typs hat in der Kontrollanwendung zur Folge, dass die Signaturprüfung des Sicherheitsobjekts mit dem vom Inspektionssystem übermittelten Austauschzertifikat durchgeführt werden MUSS.

5.6.1.1.3 Chip Authentication Private Keys Compromised

Wenn der Defekt *Chip Authentication Private Keys Compromised* gemäß Anhang A.2.1.3 von [TR-03129-2] gefunden wird, MUSS das Inspektionssystem diesen Defekt an die Kontrollanwendung weiterreichen.

Ein Auftreten eines derartigen Defekts MUSS dazu führen, dass die Kontrollanwendung die Prüfung der Chipechtheit (Chip Authentication) als *fehlgeschlagen* einstuft.

5.6.1.1.4 Active Authentication Private Keys Compromised

Wenn der Defekt *Active Authentication Private Keys Compromised* gemäß Anhang A.2.1.4 von [TR-03129-2] gefunden wird, MUSS das Inspektionssystem diesen Defekt an die Kontrollanwendung weiterreichen.

Ein Auftreten eines derartigen Defekts MUSS dazu führen, dass die Kontrollanwendung die Prüfung der Chipechtheit (Active Authentication) als *fehlgeschlagen* einstuft.

5.6.1.1.5 Document Signer Certificate incorrectly encoded or malformed

Wenn der *Document Signer Certificate incorrectly encoded or malformed* gemäß Anhang A.2.1.5 von [TR-03129-2] gefunden wird, dies MUSS entsprechend zum Ergebnis *unbestimmt* führen.

5.6.1.2 Anwendungsdefekte

5.6.1.2.1 Data Group Malformed

Wenn der Defekt *Data Group Malformed* gemäß Anhang A.2.2.1 von [TR-03129-2] gefunden wird, MUSS das Inspektionssystem diesen Defekt an die Kontrollanwendung weiterreichen.

Die Kontrollanwendung SOLLTE Informationen über falsch codierte Datengruppen anzeigen. Die Kontrollanwendung KANN, sofern es technisch möglich ist, fehlerhafte Codierungen korrigieren.

5.6.1.2.2 Document Security Object Malformed

Wenn der Defekt *Document Security Object Malformed* gemäß Anhang A.2.2.2 von [TR-03129-2] gefunden wird, MUSS das Inspektionssystem diesen Defekt an die Kontrollanwendung weiterreichen. Sofern der Parameter SOD-Fault Status übergeben wird, können diese Informationen ebenfalls an die Kontrollanwendung weitergereicht werden.

Die Kontrollanwendung MUSS bei einer fehlerhaft verifizierten Signatur des Sicherheitsobjekts (EF.SOD) das Ergebnis als *unbestimmt* und nicht als *fehlgeschlagen* einstufen. Das Ergebnis der Verifikation des Sicherheitsobjekts (EF.SOD) MUSS in diesem Fall auf *unbestimmt* gesetzt werden, das Gesamtprüfergebnis der elektronischen Dokumentenprüfung ebenfalls.

5.6.1.2.3 COM and SOD Descripancy

Wenn der Defekt *COM and SOD Descripancy* gemäß Anhang A.2.2.3 von [TR-03129] gefunden wird, MUSS die Kontrollanwendung bei den über EF.SOD verifizierbaren Datengruppen das Ergebnis der jeweiligen Teilprüfung als erfolgreich setzen, in allen anderen Fällen ist das Ergebnis der Verifikation als *fehlgeschlagen* einzustufen.

5.6.1.2.4 Personalisierungsdefekte der eID-Anwendung

Für die Verarbeitung von Defekten der eID-Anwendung werden in dieser Technischen Richtlinie KEINE Vorgaben gemacht.

5.6.1.3 Dokumentendefekte

5.6.1.3.1 Card Security Object Malformed

Wenn der Defekt *Card Security Object Malformed* gemäß Referenz Anhang A.2.4.1 von [TR-03129-2] gefunden wird, MUSS das Inspektionssystem diesen Defekt an die Kontrollanwendung weiterreichen.

Die Kontrollanwendung MUSS bei einer fehlerhaft verifizierten Signatur des Sicherheitsobjekts (EF.CardSecurity) das Ergebnis als *unbestimmt* und nicht als *fehlgeschlagen* einstufen. Das Ergebnis der Verifikation des Sicherheitsobjekts (EF.CardSecurity) MUSS in diesem Fall auf *unbestimmt* gesetzt werden, das Gesamtprüfergebnis der elektronischen Dokumentenprüfung ebenfalls.

5.6.1.3.2 Chip Security Object Malformed

Wenn der Defekt *Chip Security Object Malformed* gemäß Referenz Anhang A.2.4.2 von [TR-03129-2] gefunden wird, MUSS das Inspektionssystem diesen Defekt an die Kontrollanwendung weiterreichen.

Die Kontrollanwendung MUSS bei einer fehlerhaft verifizierten Signatur des Sicherheitsobjekts (EF.ChipSecurity) das Ergebnis als *unbestimmt* und nicht als *fehlgeschlagen* einstufen. Das Ergebnis der Verifikation des Sicherheitsobjekts (EF.ChipSecurity) MUSS in diesem Fall auf *unbestimmt* gesetzt werden, das Gesamtprüfergebnis der elektronischen Dokumentenprüfung ebenfalls.

5.6.1.3.3 Erforderliches Abschalten des Chips

Für die Verarbeitung des Defekts zur Abschaltung des Chips werden in dieser Technischen Richtlinie KEINE Vorgaben gemacht.

5.7 Behandlung von Fehlern

Jede Kontrollanwendung MUSS eine Liste möglicher Verarbeitungsfehler mit den dazugehörigen numerischen Fehlercodes definieren. Die Fehler können beispielsweise Programmabstürze, Fehlbedienung, Hardwarefehler etc. sein und zu einem vorzeitigen Abbruch eines definierten Prüfprozesses führen.

Wie in Kapitel 3 beschrieben, können Prüfergebnisse eines vorzeitig abgebrochenen Prozesses nicht als Grundlage für eine qualifizierte Bewertung des vorliegenden Dokuments dienen. Die Ursache des Fehlers SOLLTE dennoch zur Qualitätssicherung und Identifizierung von Problemen protokolliert werden. Ggf. können für die Analyse auch bis zum Auftreten des Fehlers ermittelte Teilergebnisse und Daten der bis dahin durchgeführten Prüfung protokolliert werden.

Jede Kontrollanwendung SOLLTE zu jedem definierten Fehlercode eine kurze und prägnante Fehlerbeschreibung spezifizieren, die eine spätere Analyse der Fehler vereinfacht. Ein Fehlercode vom Wert 0 MUSS dabei bedeuten, dass kein Fehler aufgetreten ist und ein Vorgang erfolgreich durchgeführt wurde.

Eine Spezifikation möglicher Fehlerzustände in den einzelnen Kontrollprozessen findet in dieser Technischen Richtlinie nicht statt und MUSS im jeweiligen Kontext vorgenommen werden. Die Spezifikation MUSS zwischen Technologielieferant und Anwender abgestimmt werden.

6 Protokollierung

Dieses Kapitel definiert den Umfang und Format der Protokollierung, welcher im Kontext von maschinell gestützten Dokumentenprüfungen in hoheitlichen Kontrollinfrastrukturen umgesetzt werden MUSS. Generell wird zwischen einer einfachen Protokollierung (*basic*) und einer erweiterten Protokollierung (*extended*) unterschieden.

Die einfache Protokollierung enthält dabei keinerlei personenbezogene Daten bzw. falls doch, in einer derart anonymisierten Form, dass eine eindeutige Identifikation des jeweiligen Dokumenteninhabers nicht möglich ist.

Die erweiterte Protokollierung umfasst Datensätze, die einzelfallbezogen und im Rahmen weiterführender (grenz-)polizeilicher Kontrollen (beispielsweise sog. Kontrolle in der zweiten Linie bei Verdachtsfällen an Grenzübergängen) zwingend für den weiteren Fahndungs- und Verarbeitungsprozess notwendig sind. Diese Protokolldaten werden nicht in einem zentralen Informationssystem gespeichert, sondern dienen dem jeweiligen Beamten als Informationsquelle für die weitere Durchführung seiner Ermittlungstätigkeit. Es wird EMPFOHLEN, die erweiterten Logdaten gemäß VSA einzustufen.

Die Struktur der Protokollierung besteht aus einem transaktionsbasierten Format (siehe Abschnitt 6.2ff.), welches die im Kontrollprozess durchgeführten Prüfungen als Teilkomponenten inkludiert. Dabei kann es sich um optisch-physikalische, elektronische sowie kombiniert optisch-physikalische und elektronische Dokumentenprüfung (siehe Abschnitt 6.3), biometrische Prüfungen (siehe Abschnitt 6.4) und um Anfragen in Auskunftssystemen (siehe Abschnitt 6.5) handeln. In Abschnitt 6.7 werden einige Beispiele für eine konforme Protokollierung dargestellt.

Das Protokollierungsformat wird durch XML Schemata definiert. Die XML-Schemata sind selbst-dokumentiert. Die in der Schemadokumentation enthaltenen Anforderungen MÜSSEN von der jeweiligen Implementierung umgesetzt werden.

6.1 Schutz personenbezogener Daten

Bei der Speicherung personenbezogener Daten MÜSSEN die unten angeführten XML-Elemente (sofern vorhanden) durch die Kontrollanwendung verschlüsselt werden. Für die Verschlüsselung dieser XML-Elemente MUSS ein öffentlicher Schlüssel der berechtigten Stelle vorliegen. Die Verschlüsselung der XML-Elemente erfolgt dabei mittels XML Encryption [XMLENC]. Es werden nur die Teile der Nachricht mit Vertraulichkeitscharakter (*extended*) verschlüsselt. Alle nicht-personenbezogenen Daten der einfachen Protokollierung (*basic*) bleiben unverschlüsselt.

Folgende Verarbeitungsregeln sind einzuhalten:

- Zu verschlüsseln sind die folgenden XML-Elemente der erweiterten Protokollierung:
  - `<dc:ExtendedDocumentInformation>` wird durch das Element `<dc:EncryptedExtendedDocumentInformation>` ersetzt
  - `<dco:ExtendedOpticalCheckInformation>` wird durch das Element `<dco:EncryptedExtendedOpticalCheckInformation>` ersetzt
  - `<dce:ExtendedElectronicCheckInformation>` wird durch das Element `<dce:EncryptedExtendedElectronicCheckInformation>` ersetzt

  - `<dcc:ExtendedCombinedCheckInformation>` wird durch das Element `<dcc:EncryptedExtendedCombinedCheckInformation>` ersetzt
  - `<bc:ExtendedBackgroundCheckInformation>` wird durch das Element `<bc:EncryptedExtendedBackgroundCheckInformation>` ersetzt
- Der XML-Encryption-Typ ist `http://www.w3.org/2011/04/xmlenc#Element`.
- Die Verschlüsselung erfolgt mit einem symmetrischen Schlüssel, der mit dem öffentlichen Schlüssel des Lesers (der berechtigten Stelle) verschlüsselt wird (hybrides Verfahren mittels `<xenc:EncryptedKey>`). Hierbei ist der verwendete Schlüssel über ein *KeyInfo*-Element mit *X509SubjectName* anzugeben.
- Für die jeweils anzuwendenden Algorithmen für die Blockverschlüsselung und Schlüsselverschlüsselung sind entsprechend den Veröffentlichungen des BSI[18] zulässige Ausprägungen zu wählen. Vorgaben für zu verwendende PKI'n sind **nicht** im Regelungsbereich dieser Technischen Richtlinie.

6.2 Transaktionsbasiertes Format für Prüfungen

Die Protokollierung der Prüfungen ist als Container-Format zu sehen, welches eine Sammlung verschiedener Teilprüfungen (Dokumentenprüfungen, biometrische Prüfungen, Anfragen an Auskunftssysteme, weitere applikationsspezifische Prüfungen) einer Transaktion enthält. Das Format wird als XML-Schema (siehe separate XSD-Datei *check_transactions_v2.xsd*) zur Verfügung gestellt.

6.3 Format für Dokumentenprüfungen

Das Format für optisch-physikalische und elektronische Dokumentenprüfungen wird als XML-Schema (siehe separate XSD-Dateien (*document_check_v2.xsd, document_check_optical_v2.xsd, document_check_electronic_v2.xsd, document_check_combined_v2.xsd*) zur Verfügung gestellt.

6.4 Format für biometrische Prüfungen

Das Protokollierungsformat für biometrische Prüfungen ist in der Technischen Richtlinie für Biometrie in hoheitlichen Anwendungen TR-03121 [TR-03121] definiert. Diese definiert für die jeweiligen Einsatzszenarien (z. B. Fingerabdruckverifikation gegen das EU-Visa-Informationssystem, Gesichtsbildverifikation im Kontext semi-automatisierter Grenzkontrollsysteme, etc.) das Format und die Informationen der zu protokollierenden Daten.

Es gilt zu beachten, dass die in [TR-03121] definierten Formate auch die aufgenommenen biometrischen Live-Daten enthalten können. Diese sind jedoch ausdrücklich nur im Ausnahmefall als Protokollierungsdaten für biometrische Prüfungen zu übernehmen. Im Standardfall DÜRFEN

18 Siehe Algorithmenkatalog auf https://www.bsi.bund.de/Algorithmenkatalog.- Der Algorithmenkatalog spezifiziert im eigentlichen Sinne zwar nur Signaturanwendungen, es wird jedoch EMPFOHLEN, die dort vorgeschlagenen Kryptoalgorithmen auch für die Verschlüsselung zu verwenden.

diese Daten NICHT übernommen werden (siehe *record*-Elemente in den entsprechenden Modulen von [TR-03121]).

Bibliografische und demografische Daten, welche von den Protokollformaten der [TR-03121] gefordert werden, müssen von der aufrufenden Applikation nachträglich eingefügt werden.

6.5 Format für Anfragen in Auskunftssystemen

Das Format für Anfragen in Auskunftssystemen wird als XML-Schema (siehe separate XSD-Datei (*background_check_v2.xsd*) zur Verfügung gestellt.

6.6 Format für applikationsspezifische Daten

Der Technologiehersteller KANN bei Bedarf weitere Daten protokollieren. Der Technologiehersteller legt dem Bedarfsträger gegenüber das von ihm zu diesem Zweck verwendete XML-Schema offen, welches Bestandteil des globalen von der jeweiligen Anwendung verwendeten XML-Schemas wird. Die Regelungen von 6.1 zum Schutz personenbezogener Daten gelten entsprechend.

Der Technologiehersteller KANN Teile der protokollierten Daten verschlüsseln. Bei der Festlegung des Umfanges der herstellerspezifischen Daten SOLLTEN die Datenschutzbeauftragten des Bedarfsträgers und des Technologieherstellers hinzugezogen werden. Über die verschlüsselten Inhalte MUSS der Technologiehersteller dem Bedarfsträger auf Anfrage Auskunft erteilen.

Der Technologiehersteller erhält in Abstimmung mit dem Bedarfsträger Zugriff auf mindestens diesen Teil der protokollierten Daten, es sei denn, eine entsprechende Einstufung dieser Daten verbietet das.

6.7 Beispiele der Protokollierung

Die folgenden Beispiele sollen einen Überblick über das Format der Protokollierung geben, sie werden als separate XML-Dateien zur Verfügung gestellt.

6.7.1 ePass-Prüfung Standardfall

Dieses Beispiel (*Example_ePassCheck_Basic.xml*) beschreibt eine Grenzkontrollsituation, bei welcher der elektronische Reisepass eines Reisenden optisch-physikalisch und elektronisch geprüft wird. Die aus dem Reisepass ausgelesenen biometrischen Daten werden dann verwendet, um den Inhaber mittels Gesichts- und Fingerabdruckerkennung zu verifizieren. Zusätzlich kann eine Fahndungsabfrage durchgeführt werden.

6.7.2 ePass- und Visa-Prüfung Standardfall

Dieses Beispiel (*Example_ePassAndVisaCheck_Basic.xml*) beschreibt eine Grenzkontrollsituation, bei welcher der elektronische Reisepass eines Reisenden optisch-physikalisch und elektronisch geprüft wird. Zusätzlich wird auch das Visum des Reisenden optisch-physikalisch geprüft. Das aus dem Reisepass ausgelesene Gesichtsbild wird mit dem Gesichtsbild des Reisenden verglichen. Zusätzlich werden Fingerabdrücke aufgenommen und für eine Verifikation des Reisenden gegen das Visa-Informationssystem verwendet. Auch eine Fahndungsabfrage wird durchgeführt.

6.7.3 ePass-Prüfung Ausnahmefall

Dieses Beispiel (*Example_ePassCheck_Extended.xml*) zeigt eine Ausnahmesituation (personenbezogene Daten sind verschlüsselt), bei der sämtliche Daten des Reisepasses des Reisenden protokolliert werden. Auch die biometrischen Daten werden hier übermittelt. Das Beispiel in *Example_ePassCheck_Extended_Decrypted.xml* zeigt das XML, in dem die personenbezogenen Daten entschlüsselt sind (z. B. zur Analyse der Daten).

6.8 Änderungshistorie

In den folgenden Abschnitten werden Änderungen am XML-Format gegenüber älteren Versionen dieser Technischen Richtlinie dokumentiert.

6.8.1 Änderungen in Version 1.2

Check_transactions_v2.xsd:

- schemaVersion=2
- Neues optionales CheckTransaction-Header-Element ExternalKey
- Einzelne CheckTransaction als eigenständiges Root-Element erlaubt
- Klarstellung der Dokumentation zu TransactionID; jede einzelne TransactionID MUSS eindeutig sein.

document_check_v2.xsd:

- Update der Dokumentation zu YearOfBirth

background_check_v2.xsd:

- schemaVersion=2
- neues optionales Element BackgroundCheckType
- neuer möglicher Ergebniswert „partial“ für teilweise durchgeführte Prüfungen; Update der Dokumentation

6.8.2 Änderungen in Version 1.2.1

background_check_v2.xsd:

- schemaVersion=3
- neue Attribute returnCode, returnText, errorID in BackgroundCheckResult
- neue Attribute causeText und purposeText im Element Hit

7 Sende- und Empfangsspezifikation

Zur Übertragung von XML-Dokumenten gemäß Kapitel 6 definiert dieses Kapitel eine Web-Service-Schnittstelle durch eine WSDL-Beschreibung sowie weitere Anforderungen an die kryptographische Absicherung der Übertragung.

7.1 Web-Service-Schnittstelle

Die WSDL „*ReceiveTransaction.wsdl*“ definiert für den Logdatentransfer einen Web-Service-Port-Typ „*ReceiveTransactionPortType*“ mit SOAP 1.1 *HTTP-Binding*. Dieser enthält in der Input-Nachricht das zu übertragende XML-Dokument (*CheckTransactions*-Element), eine Rückantwort und eine Fehlerantwort. Die Semantik der Antworten ist durch Tabelle 48 festgelegt.

Rückantwort des Web-Service	***Anforderung***
received_ok	Der Service hat das XML-Dokument erfolgreich entgegengenommen.
invalid_transaction	Der Service hat das XML-Dokument entgegengenommen, es entspricht aber nicht den Anforderungen (z. B. bzgl. Schema-Korrektheit oder implementierter Schema-Version). Das XML-Dokument SOLLTE korrigiert werden und erneut übermittelt werden.[19]
internal_error	Es ist serverseitig ein technischer Fehler bei der Verarbeitung aufgetreten. Das XML-Dokument wurde nicht verarbeitet. Der Client MUSS das XML-Dokument zu einen späteren Zeitpunkt erneut senden.

Tabelle 48: Rückgabewerte der Web-Service-Schnittstelle „ReceiveTransactionService“

Die Schnittstelle erzwingt keine strikte Bindung an das XML-Schema. Der empfangende Server MUSS die Datei auf Schema-Korrektheit und Korrektheit der implementierten Schema-Version prüfen.

7.2 Absicherung der Kommunikationsstrecke

Für die Absicherung der Kommunikationsstrecke wird die Nutzung von TLS [RFC5246] EMPFOHLEN. Vorgaben zur Zertifikats- und Schlüsselspeicherung sind nicht im Regelungsbereich dieser Richtlinie.

19 Abhängig vom Implementierungsszenario ist dies nicht immer möglich, in diesem Fall kann der Service auch das fehlerhafte Dokument speichern und einer manuellen Fehlerbeseitigung zuführen. Es wird empfohlen, durch Testmaßnahmen dafür zu sorgen, dass der Fehlercode „*invalid_transaction*“ aufgrund des damit verbundenen organisatorischen Aufwands in der Praxis nicht auftritt.

8 Konformität

Kontrollwendungen für maschinell gestützte Dokumentenprüfungen in hoheitlichen Kontrollinfrastrukturen, die konform zu dieser Technischen Richtlinie sind, MÜSSEN alle normativen Anforderungen dieser Richtlinie für die in Kapitel 2 definierten Anwendungsszenarien umsetzen und erfüllen.

Sende- und Empfangssysteme, die konform zu dieser Technischen Richtlinie sind, müssen alle normative Anforderungen von Kapitel 7 umsetzen und erfüllen.

Zusätzlich MÜSSEN verwendete Dokumentenlesegeräte gemäß [TR-03105-4] zertifiziert sein und den darin enthaltenen Anforderungen entsprechen.

9 Abkürzungsverzeichnis und Glossar

Abkürzung	*Beschreibung*
AA	Active Authentication
ABC	Automated Border Control (automatisierte Grenzkontrolle in Form von Self-Service-/Schleusen-Systemen)
BAC	Basic Access Control
CA	Chip Authentication
CAN	Card Access Number
Container-Format	Unter einem Container-Format versteht man eine Datenstruktur, die als Container für weitere Daten dient, welche sich ähnlich wie in einem Verzeichnis, innerhalb des Containers befinden.
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CSCA-Link-Zertifikat	Ein Link-Zertifikat ist ein Zertifikat, welches sich über das zuvor gültige Zertifikat verifizieren lässt und damit eine vertrauenswürdige Kette bildet.
CVCA	Country Verifying Certification Authority
DG1	enthält biografische Daten des Dokumenteninhabers
DG14	Chip Authentication Public Key
DG15	Active Authentication Public Key
DG2	enthält das Gesichtsbild des Dokumenteninhabers
DG3	enthält ggf. Fingerabdrücke des Dokumenteninhabers
DS	Document Signer
DV	Document Verifier – Technische Umsetzung der DVCA, hier ist demnach eine DV-Instanz gemeint, mit der z. B. das IS kommuniziert.
DVCA	Document Verifier Certificate Authority – Im Kontext der PKI spricht man von der DVCA, während bei der technischen Umsetzung von der DV gesprochen wird.
EAC	Extended Access Control
eAT	Elektronischer Aufenthaltstitel

Abkürzung	*Beschreibung*
EF.CardAccess	Sicherheitsinformationen gemäß [TR-03110]
EF.CardSecurity	Sicherheitsinformationen gemäß [TR-03110]
EF.ChipSecurity	Sicherheitsinformationen gemäß [TR-03110]
EF.COM	Index, der angibt, welche Datengruppen im Tag gespeichert sind.
EF.CVCA	Country Verifying Certification Authority
EF.SOD	Hashwerte aller Datengruppen sowie elekt. Signatur über diese Hashwerte.
EMC	Elektromagnetische Verträglichkeit (engl. Electromagnetic Compatibility)
eMRTD	Elektronische, maschinenlesbare Reisedokumente (engl. Electronic Machine Readable Travel Documents)
ePass	Elektronischer Reisepass
Hash(wert)	Unter einem Hashwert versteht man das Ergebnis einer mathematischen nicht injektiven Abbildung, die zu einer Eingabe aus einer oft großen Quellmenge eine Ausgabe aus einer kleineren Zielmenge generiert, den sogenannten Hashcode bzw. Hashwert. Eine kryptologische Hashfunktion oder kryptographische Hashfunktion ist eine spezielle Form der Hashfunktion, welche insbesondere kollisionsresistent ist und/oder eine Einwegfunktion darstellt.
HSM	Hardware-Sicherheitsmodul (engl. Hardware Security Module)
ICAO	International Civil Aviation Organization
INPOL	Informationssysteme der Polizei
IR	Infrarot
IS	Inspektionssystem
ISO	International Organization for Standardization
MRTD	Maschinenlesbare Reisedokumente (engl. Machine Readable Travel Documents)
MRZ	Maschinenlesbare Zone (engl. Machine Readable Zone)
nPA	Neuer deutscher (elektronischer) Personalausweis
NPKD	National Public Key Directory

Abkürzung	*Beschreibung*
PA	Passive Authentication
PACE	Password Authentication Connection Establishment
PC	Personal Computer
PC/SC	Personal Computer / Smart Card Schnittstelle
PKD	Public Key Directory
PKI	Public Key Infrastructure
ppi	Pixels per inch
RF	Drahtlose Übertragung (engl. Radio Frequency)
SIS	Schengener Informationssystem
TA	Terminal Authentication
TCC	Terminal Control Centre
TR	Technische Richtlinie
UND/ODER	Option A *und/oder* Option B bedeutet in diesem Kontext: Entweder Option A oder Option B oder beide, aber in jedem Falle eine der beiden Optionen muss genutzt werden.
UUID	Universally Unique Identifier
UV	Ultraviolett
VIZ	Sichtbare Informationen auf der Personaldatenseite, auch unter dem Begriff biografische Datenseite bekannt (engl. Visual Inspection Zone).
VIS-Bild	Bild der Ausweisdatenseite aufgenommen unter Beleuchtung im sichtbaren Lichtwellenlängenbereich (Weißlichtbild).
XML	Extended Markup Language
XSD	XML Schema Definition

10 Literatur

[BSI-CVCA] Bundesamt für Sicherheit in der Informationstechnik (BSI): Certificate Policy für die ePass-Anwendung der hoheitlichen Dokumente, 2010.

[FRONTEX] European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX): "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", "Best Practice Operational Guidelines for Automated Border Control (ABC) Systems", 2012, Version 2.0.

[ICAO9303] International Civil Aviation Organization (ICAO): Doc 9303 – Machine Readable Travel Documents, Part 1 Vol. 1 and 2, Part 2 and Part 3 Vol. 1 and 2.

[ICAOMADSV] International Civil Aviation Organization (ICAO): Doc 9303 – Technical Report on Machine Assisted Document Security Verification.

[ICAO-ML] International Civil Aviation Organization (ICAO): Technical Report – CSCA countersigning and Master List issuance, 2009.

[ICAO-LDS-PKI] International Civil Aviation Organization (ICAO): Technical Report – LDS and PKI Maintenance, 2011, Version 1.0.

[ICAOSAC] International Civil Aviation Organization (ICAO): ICAO Technical Report Supplemental Access Control, 2010, Version 1.01.

[ISO1831] International Organization for Standardization (ISO) 1831: Printing specifications for optical character recognition, 2008.

[ISO10918-1] International Organization for Standardization ISO/IEC 10918-1: Digital compression and coding of continuous-tone still images: Requirements and guidelines, 2011.

[ISO3166-1] International Organization for Standardization ISO 3166-1: Codes for the representation of names of countries and their subdivisions – Part 2: Country subdivision code

[ISO14443] International Organization for Standardization ISO/IEC 14443: Identification cards – Contactless integrated circuit cards – Proximity cards, 2008.

[ISO/IEC18745-2] International Organization for Standardization ISO/IEC CD 18745-2: "Test methods for machine readable travel documents (MRTD) – Part 2: Test methods for the contactless interface". (Ed. 2013)

[RFC1485] Request For Comments Editor (RFC), S. Hardcastle-Kille: A String Representation of Distinguished Names (OSI-DS 23 (v5)) RFC 1485, 1993.

[RFC2119] Request For Comments Editor (RFC), Bradner, Scott: Key words for use in RFCs to indicate requirement levels, RFC 2119, 1997.

[RFC4120] Request For Comments Editor (RFC), Neuman, Yu, Hartman, Raeburn: The Kerberos Network Authentication Service (V5) RFC 4120, 2005.

[RFC4122] Request For Comments Editor (RFC), Leach P., Mealling M., Salz R.: A Universally Unique Identifier (UUID) URN Namespace RFC 4122, 2005.

[RFC5246] Request For Comments Editor (RFC), Dierks, Rescorla: The Transport Layer Security (TLS) Protocol. RFC 5246, 2008, Version 1.2.

[TR-03105-4] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03105 Part 4 – Test plan for ICAO compliant Proximity Coupling Device (PCD) on Layer 2-4, 2010, Version 2.2.

[TR-03110] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03110 – Advanced Security Mechanisms for Machine Readable Travel Documents, 2012, Version 2.10.

[TR-03121] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03121 - Biometrics in public sector applications, 2013, Version 3.0.1.

[TR-03129] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03129 – PKIs for Machine Readable Travel Documents – Protocols for the Management of Certificates and CRLs, 2009, Version 1.10.

[TR-03129-2] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03129-2 – Protocols for the Management of Certificates and CRLs - National Protocols for ePassport Application, 2013, Version 1.

[XMLENC] World Wide Web Consortium (W3C): XML Encryption Syntax and Processing. http://www.w3.org/TR/xmlenc-core, 2002.

11 Anhang A: Exemplarische Umsetzung des Kommunikationsablaufs (informativ)

Da im Gesamtkontext der maschinell gestützten Dokumentenprüfung im hoheitlichen Bereich mehrere Komponenten zum Einsatz kommen, wird empfohlen, die Kommunikationsabläufe der folgenden Abschnitte umzusetzen. Die Kontrollanwendung beinhaltet dabei ein Dokumenten-kontrollmodul, welches die Operationen zur Durchführung der Sicherheitsprotokolle ausführt. Als weitere Komponenten im Kontrollprozess sind das Dokumentenlesegerät mit dem elektronischen Dokument, das Terminal Control Centre (TCC) als vertrauenswürdige Stelle und ein Hardware-Sicherheitsmodul (HSM), welches direkt an das TCC angebunden ist, am Kommunikationsablauf beteiligt.

Die in den folgenden Abschnitten beschriebenen Kommunikationsabläufe umfassen das optisch-physikalische und elektronische Lesen der Dokumente, sowie die in den vorigen Abschnitten definierten optisch-physikalischen und elektronischen Dokumentenprüfungen. Wie in Abschnitt 5.4.2 beschrieben, hängt die Reihenfolge des Zugriffs auf die einzelnen Dateien und Datengruppen auf dem elektronischen Chip des Dokuments vom jeweiligen Dokument ab. Die unterschiedlichen Prozesse für den deutschen elektronischen Reisepass der 2. Generation (ePass) und den deutschen Personalausweis (nPA) sind beispielhaft in den folgenden Abschnitten beschrieben.

11.1 Elektronischer Reisepass (ePass)

Der Kommunikationsablauf für den elektronischen Reisepass ist in den Abbildungen 10 und 11 dargestellt. Dieser beginnt mit dem optischen Erfassen des Dokuments, um die MRZ, welche notwendig ist für den Zugriff auf die elektronischen Daten des Dokuments, und die Bilder der Datenseite zu extrahieren. Zusätzlich soll das Dokumentenlesegerät die in Abschnitt 5.3 definierten optisch-physikalischen Prüfungen des Dokuments durchführen. Die Ergebnisse dieser Prüfungen werden vom Dokumentenlesegerät an die Kontrollanwendung zurückgeliefert.

Mithilfe der optisch gelesenen MRZ versucht die Anwendung nun, die elektronischen Daten zu lesen und beginnt dabei mit dem Lesen der Datengruppe 1, welche die elektronische MRZ enthält. Es wird dann BAC durchgeführt, um eine sichere Kommunikationsverbindung zum Dokument aufzubauen. Da es auch Dokumente gibt, die nicht mit BAC geschützt sind, kann dieser Schritt gegebenenfalls ausfallen und die Kommunikation mit dem elektronischen Chip findet dann unverschlüsselt statt. Im nächsten Schritt wird EF.COM gelesen, um die auf dem Chip vorhandenen Datengruppen zu identifizieren. Um die Echtheit des Chips zu garantieren, wird Datengruppe 14 gelesen, welche die notwendigen Informationen für die Durchführung von CA (Version 1) enthält. Ist die Datengruppe 14 nicht vorhanden, wird AA durchgeführt (sofern vom Chip unterstützt). Dafür muss die Datengruppe 15 gelesen werden. AA kann optional auch zusätzlich zu CA1 durchgeführt werden. Im Anschluss an die Prüfung der Chipechtheit soll EF.SOD gelesen werden. Obwohl EF.SOD erst für die Prüfung der gelesenen Datengruppen (PA) benötigt wird, soll EF.SOD möglichst bald gelesen werden, um beim vorzeitigen Entfernen des Dokuments vom Lesegerät zumindest die bereits gelesenen Datengruppen auf deren Integrität und Echtheit prüfen zu können.

Da in Datengruppe 1 keine sensitiven Informationen stehen, kann diese nun gelesen werden und an die Kontrollanwendung übertragen werden. Auch Datengruppe 2, welche das digitale Gesichtsbild enthält, kann nun gelesen werden.

Um die Fingerabdrücke aus Datengruppe 3 auslesen zu können, muss TA (Version 1) durchgeführt werden. Dazu wird die Datei EF.CVCA vom Dokument gelesen, welche Informationen über die notwendigen Zertifikate für die TA enthält. Die Kontrollanwendung (bzw. das Dokumentenkontrollmodul) fordert nun vom TCC die passende Zertifikatskette an, welche dann an den Chip zur Prüfung gesendet wird. Dieser schickt das Ergebnis der Zertifikatsprüfung sowie den benötigten Public Key zurück. Zusätzlich werden vom Chip Zufallsdaten (sog. Challenge) angefordert, die zusammen mit dem Public Key zum TCC geschickt werden. Das TCC leitet diese Daten dann an das HSM weiter, wo diese mit dem dort gespeicherten privaten Schlüssel signiert werden. Die erstellte Signatur wird dann an die Kontrollanwendung retourniert, wo sie zum elektronischen Chip zur Prüfung geschickt werden kann. Nur wenn diese Signaturprüfung erfolgreich ist, wird der Zugriff auf Datengruppe 3 gewährt. Diese und andere auf dem Dokument vorhandenen Datengruppen (z. B. Datengruppe 4) können nun gelesen werden.

Nun kann die Kontrollanwendung vom Dokumentenkontrollmodul den Status der einzelnen Sicherheitsprotokolle (BAC, CA1, AA, TA1) abfragen und anzeigen.

Zusätzlich müssen die gelesenen Datengruppen allerdings noch auf deren Echtheit geprüft werden. Dazu gehört eine Integritätsprüfung aller gelesenen Datengruppen und eine Konsistenzprüfung der Inhalte von EF.SOD und EF.COM. Die Prüfung von EF.SOD erfolgt über das TCC. Dazu sendet die Anwendung Document Signer Informationen an das TCC. Zu diesen Informationen gehört im Normalfall auch das DS-Zertifikat, welches geprüft werden muss. Das TCC führt die geforderten Prüfungen (siehe Abschnitt 5.4.5) durch und liefert die Ergebnisse an die Anwendung zurück. Nur wenn diese Prüfung erfolgreich ist, können die in den vorigen Schritten durchgeführten Protokolle und Sicherheitsprüfungen als gültig betrachtet werden. Zusätzlich zur PA müssen auch noch die Daten der DG1 und der optisch gelesenen MRZ geprüft sowie ein Vergleich der Ausstellerstaaten in DG1 und im DS-Zertifikat durchgeführt werden.

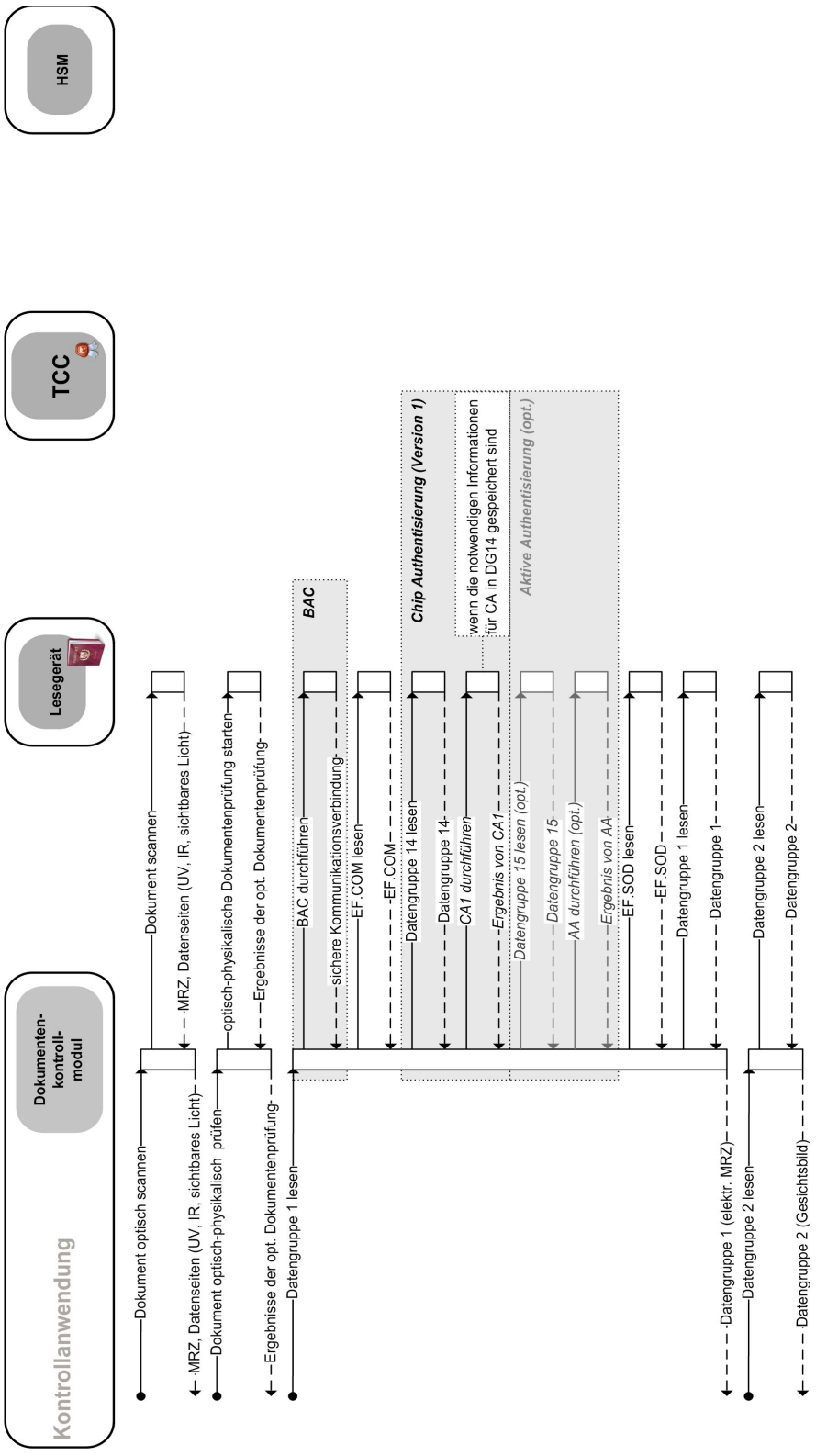

Abbildung 10: Kommunikationsablauf ePass Teil 1

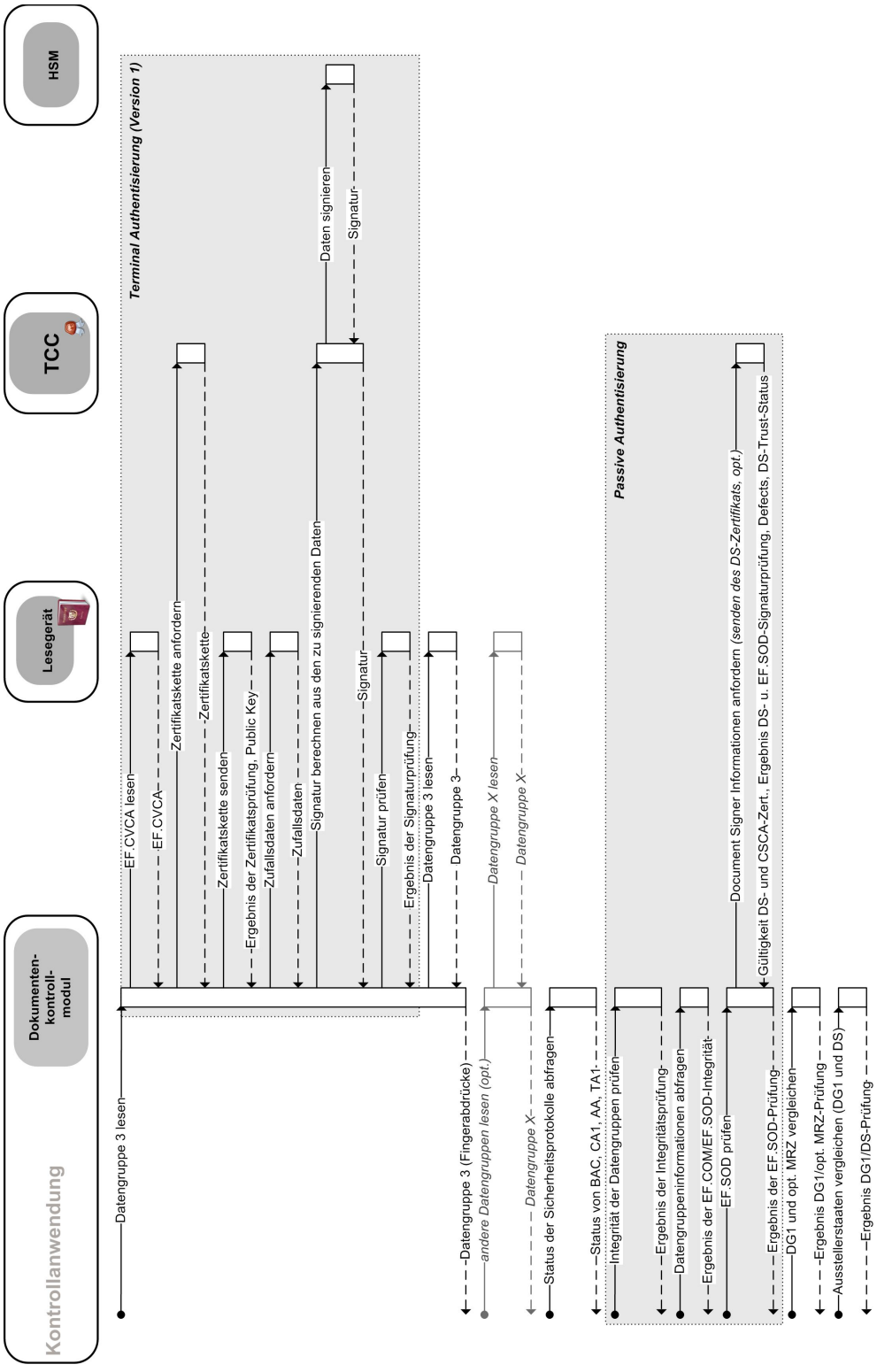

Abbildung 11: Kommunikationsablauf ePass Teil 2

11.2 Elektronischer Personalausweis (nPA)

Der Kommunikationsablauf für den elektronischen Personalausweis ist in den Abbildungen 12 und 13 dargestellt. Dieser beginnt ebenfalls mit dem optischen Erfassen des Dokuments, um die MRZ oder die CAN, welche notwendig sind für den Zugriff auf die elektronischen Daten des Dokuments, und die Bilder der Datenseite zu extrahieren. Zusätzlich soll das Dokumentenlesegerät die in Abschnitt 5.3 definierten optisch-physikalischen Prüfungen des Dokuments durchführen. Die Ergebnisse dieser Prüfungen werden vom Dokumentenlesegerät an die Kontrollanwendung zurückgeliefert.

Mithilfe der optisch gelesenen MRZ oder der CAN versucht die Anwendung nun, die elektronischen Daten zu lesen und beginnt dabei mit dem Lesen der Datengruppe 1, welche die elektronische MRZ enthält. Nach dem Lesen von EF.CardAccess wird PACE durchgeführt, um eine sichere Kommunikationsverbindung zum Dokument aufzubauen. Im nächsten Schritt muss TA (Version 2) durchgeführt werden. Die Kontrollanwendung (bzw. das Dokumentenkontrollmodul) fordert nun vom TCC die passende Zertifikatskette an, welche dann an den Chip zur Prüfung gesendet wird. Dieser schickt das Ergebnis der Zertifikatsprüfung sowie den benötigten Public Key zurück. Zusätzlich werden vom Chip Zufallsdaten (Challenge) angefordert, die zusammen mit dem Public Key zum TCC geschickt werden. Das TCC leitet diese Daten dann an das HSM weiter, wo diese mit dem dort gespeicherten privaten Schlüssel signiert werden. Die erstellte Signatur wird dann an die Kontrollanwendung retourniert, wo sie zum elektronischen Chip zur Prüfung geschickt werden kann. Nur wenn diese Signaturprüfung erfolgreich ist, wurde TA erfolgreich durchgeführt.

Um die Echtheit des Chips zu garantieren, wird EF.ChipSecurity (oder EF.CardSecurity, wenn EF.ChipSecurity nicht vorhanden ist) gelesen, welche die notwendigen Informationen für die Durchführung von CA (Version 2) enthält. Im Anschluss an die Prüfung der Chipechtheit soll EF.SOD gelesen werden. Obwohl EF.SOD erst für die Prüfung der gelesenen Datengruppen (PA) benötigt wird, soll EF.SOD möglichst bald gelesen werden, um beim vorzeitigen Entfernen des Dokuments vom Lesegerät zumindest die bereits gelesenen Datengruppen auf deren Integrität und Echtheit prüfen zu können. Nun können alle Datengruppen vom Dokument gelesen werden.

Die Kontrollanwendung kann dann vom Dokumentenkontrollmodul den Status der einzelnen Sicherheitsprotokolle (PACE, CA2, TA2) abfragen und anzeigen.

Zusätzlich müssen die gelesenen Datengruppen allerdings noch auf deren Echtheit geprüft werden. Dazu gehört eine Integritätsprüfung aller gelesenen Datengruppen. Die Prüfung der Sicherheitsobjekte (EF.SOD, EF.ChipSecurity, EF.CardSecurity) erfolgt über das TCC. Dazu sendet die Anwendung Document Signer Informationen an das TCC. Zu diesen Informationen gehört im Normalfall auch das DS-Zertifikat, welches geprüft werden muss. Das TCC führt die geforderten Prüfungen (siehe Abschnitt 5.4.5) durch und liefert die Ergebnisse an die Anwendung zurück. Nur wenn diese Prüfung erfolgreich ist, können die in den vorigen Schritten durchgeführten Protokolle und Sicherheitsprüfungen als gültig betrachtet werden. Zusätzlich zur PA müssen auch noch die Daten der DG1 und der optisch gelesenen MRZ geprüft sowie ein Vergleich der Ausstellerstaaten in DG1 und im DS-Zertifikat durchgeführt werden.

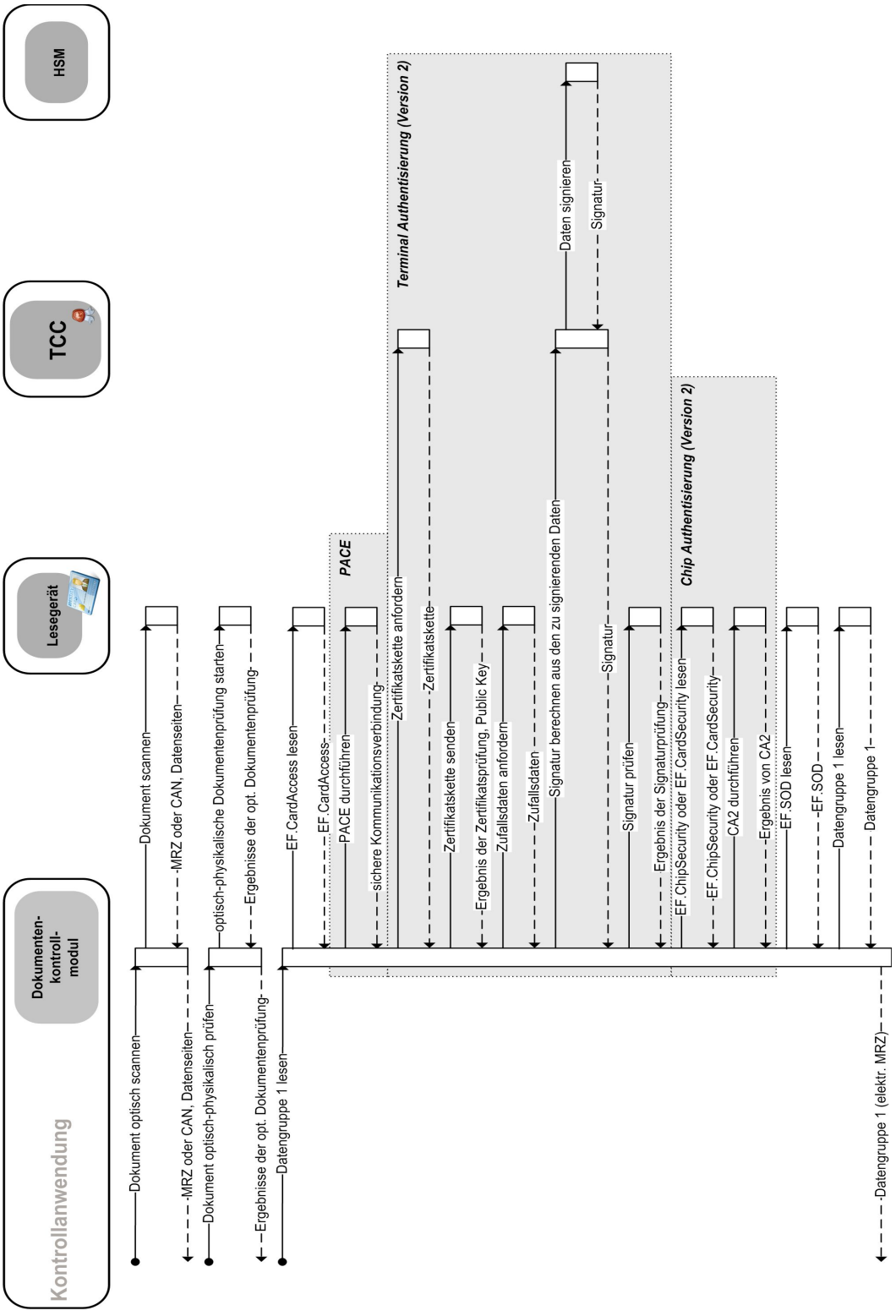

Abbildung 12: Kommunikationsablauf nPA Teil 1

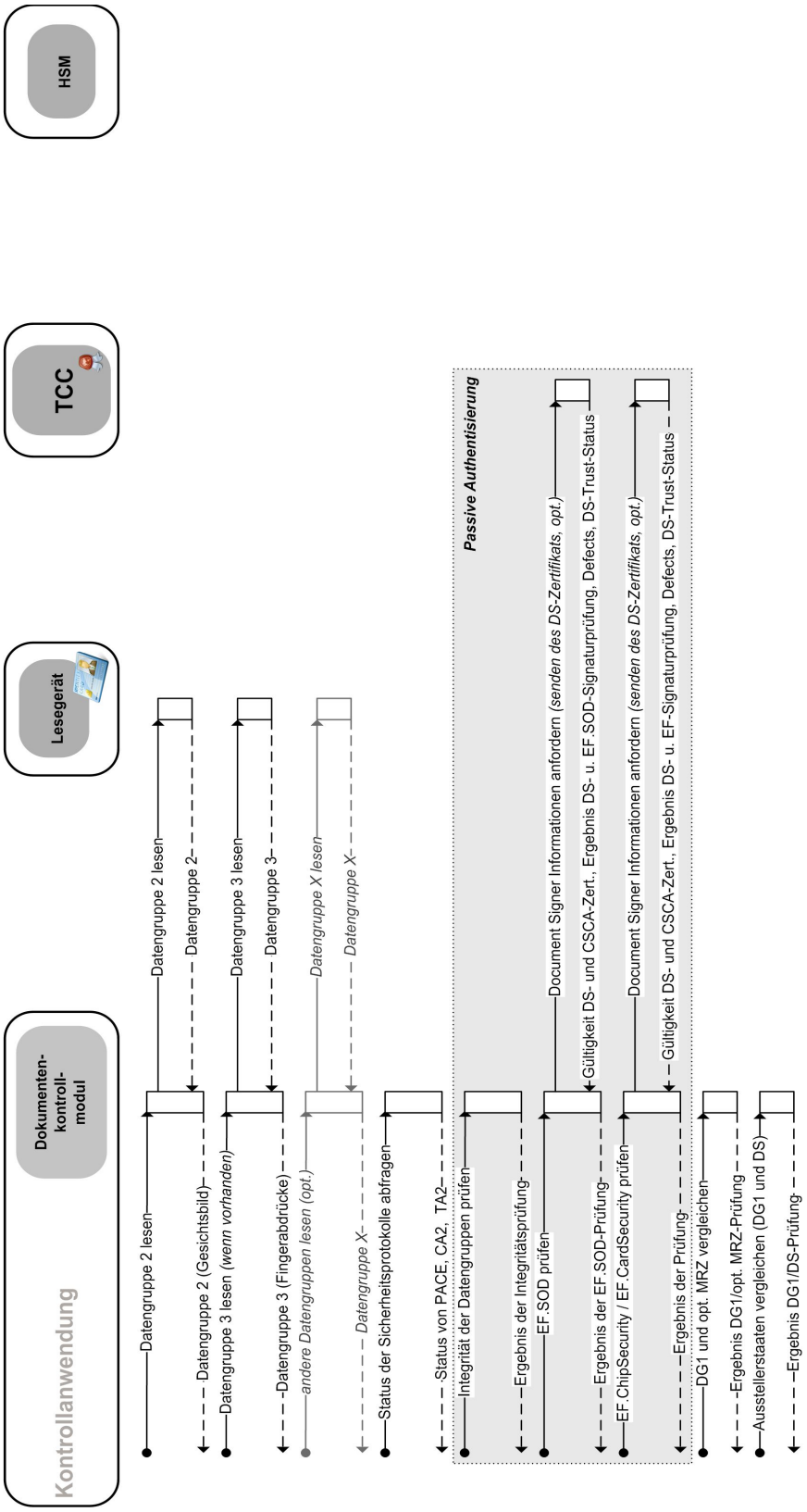

Abbildung 13: Kommunikationsablauf nPA Teil 2

12 Anhang B: Dokumentenunterstützung (informativ)

Die folgende Tabelle gibt einen Überblick über die verfügbaren Dokumente und deren möglicher Unterstützung der einzelnen Protokollabläufe beim Lesen der elektronischen Inhalte:

Dokument	***BAC/PACE***	***Protokolle***
ePass EU Stufe 1	BAC	Passive Authentication – PA ([ICAO 9303]) Terminal Authentication Version 1 gemäß ([TR-03110]) Chip Authentication Version 1 gemäß ([TR-03110])
ePass EU Stufe 2	PACE	Passive Authentication– PA ([ICAO 9303]) Terminal Authentication Version 1gemäß ([TR-03110]) Chip Authentication Version 1 gemäß ([TR-03110])
Deutscher nPA	PACE	Terminal Authentication Version 2 – TA2 ([TR-03110]) Passive Authentication – PA ([ICAO 9303]) Chip Authentication Version 2 – CA2 ([TR-03110])
Nicht-deutscher eAT	BAC	Passive Authentication – PA ([ICAO 9303]) Terminal Authentication Version 1 gemäß ([TR-03110]) Chip Authentication Version 1 gemäß ([TR-03110])
Deutscher eAT	BAC	Passive Authentication – PA ([ICAO 9303]) Terminal Authentication Version 1 gemäß ([TR-03110]) Chip Authentication Version 1 gemäß ([TR-03110])
	PACE	Terminal Authentication Version 2 gemäß ([TR-03110]) Chip Authentication Version 2 gemäß ([TR-03110])

Tabelle 49: Dokumententypen mit den von ihnen unterstützten Protokollen

Dokument	***Mögliche unterstützte Protokollabläufe***
ePass	Version 1 (gemäß Abschnitt 5.4.2.1) Version 2 (gemäß Abschnitt 5.4.2.2)
Deutscher nPA	Version 3 (gemäß Abschnitt 5.4.2.3)
Nicht-deutscher eAT	Version 1 (gemäß Abschnitt 5.4.2.1)
Deutscher eAT	Version 1 (gemäß Abschnitt 5.4.2.1) Version 3 (gemäß Abschnitt 5.4.2.3)

Tabelle 50: Unterstützte Protokollabläufe der einzelnen Dokumente