Bundesanzeiger
Herausgegeben vom
Bundesministerium der Justiz
und für Verbraucherschutz
www.bundesanzeiger.de

Bekanntmachung
Veröffentlicht am Montag, 15. Dezember 2014
BAnz AT 15.12.2014 B9

Kraftfahrt-Bundesamt

Bekanntmachung des Standards für Internetbasierte Fahrzeugzulassung (i-Kfz) – Mindest-Sicherheitsanforderungen an dezentrale Portale – Stand: 13. November 2014 Version 1.0

Vom 14. November 2014

Mit Inkrafttreten der

- Ersten Verordnung zur Änderung der Fahrzeug-Zulassungsverordnung und der Gebührenordnung für Maßnahmen im Straßenverkehr sowie der
- Zweiten Verordnung zur Änderung der Fahrzeug-Zulassungsverordnung und anderer straßenverkehrsrechtlicher Vorschriften

am 1. Januar 2015 wird die erste Stufe des Projekts Internetbasierte Fahrzeugzulassung (im weiteren „i-Kfz“ genannt) umgesetzt. Ab diesem Zeitpunkt kann ein Fahrzeug auch dadurch außer Betrieb gesetzt werden, indem der Halter oder der Verfügungsberechtigte dies

- direkt (über ein dezentrales, kommunales Portal) oder
- über ein vom Kraftfahrt-Bundesamt betriebenes informationstechnisches System (zentrales Portal)

bei der Zulassungsbehörde elektronisch beantragt (internetbasierte Außerbetriebsetzung).

Dezentrale Portale greifen dabei über ein unsicheres Netzwerk (hier: Internet) auf die abgesicherte KBA-Infrastruktur zu. Dabei ist der Zugriff auf die im Kraftfahrt-Bundesamt vorhandene IT-Infrastruktur so zu gestalten, dass definierte Mindest-Sicherheitsanforderungen an die Informationssicherheit eingehalten werden. Soweit für diese internetbasierte Außerbetriebsetzung auf Systembestandteile zurückgegriffen wird, die einen Zugang zu den Daten des Kraftfahrt-Bundesamtes ermöglichen, hat nach § 14 Absatz 2 Satz 10 FZV (in der ab 1. Januar 2015 geltenden Fassung) die Übermittlung der Daten nach Maßgabe eines vom Kraftfahrt-Bundesamt im Bundesanzeiger und nachrichtlich im Verkehrsblatt veröffentlichten Standards zu erfolgen.

Der Standard ist von Betreibern dezentraler Portale verbindlich einzuhalten. Dieser Standard wird im Verlaufe der Fortentwicklung der internetbasierten Fahrzeugzulassung fortgeschrieben. Der für die Außerbetriebsetzung geltende Standard mit Mindest-Sicherheitsanforderungen wurde abgestimmt mit Vertretern

- der kommunalen Spitzenverbände (DLT und DST),
- der Entwickler der in Zulassungsbehörden eingesetzten Fachverfahren,
- des Bundesamtes für Sicherheit in der Informationstechnik (BSI),
- der für Zulassungsbehörden arbeitenden Rechenzentren,
- der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister (VITAKO),
- der für die Zulassung von Fahrzeugen zum Straßenverkehr zuständigen obersten Landesbehörden,
- von Zulassungsbehörden,
- der Versicherer (vertreten durch die GDV Dienstleistungs-GmbH & Co. KG),
- dem Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) sowie
- dem Kraftfahrt-Bundesamt (KBA)
- und wird im Folgenden im Bundesanzeiger und nachrichtlich im Verkehrsblatt bekannt gegeben. Dazu gehören folgende Dokumente:

  1. „Internetbasierte Fahrzeugzulassung (i-Kfz) – Mindest-Sicherheitsanforderungen an dezentrale Portale –“, Version 1.0, Stand: 13. November 2014 (Anlage 1)
  2. „Internetbasierte Fahrzeugzulassung (i-Kfz) – Anlage Penetrationstests –“, Version 1.0, Stand: 13. November 2014 (Anlage 2)

Die vorgenannten Dokumente werden zusätzlich im geschützten Bereich der Internetseiten des KBA veröffentlicht. Dort können die Dokumente digital aufgerufen werden unter:

http://www.kba.de/DE/GeschuetzterBereich/ZentraleRegister/I_KFZ/MindestSichAnforderungen_dez_Portale/mindest-sicherheitsanforderungen_inhalt.html?nn=644958

Die Zugangsdaten sind beim KBA zu erfragen.

Der Standard mit den Mindest-Sicherheitsanforderungen an dezentrale Portale, zusammen mit der bekannt gegebenen Anlage, gilt ab 1. Januar 2015.

Flensburg, den 14. November 2014

Kraftfahrt-Bundesamt

Der Präsident
Zinke

Anlage 1

Internetbasierte
Fahrzeugzulassung (i-Kfz)
– Mindest-Sicherheitsanforderungen an dezentrale Portale –

Version: 1.0
Stand: 13. November 2014

Dokumenttitel: Mindestsicherheitsanforderungen an dezentrale Portale
Projektname: Internetbasierte Fahrzeugzulassung
Freigegebene Version: 1.0

Änderungsverzeichnis

Version	Datum	Geänderte Kapitel	Grund der Änderung	Name
0.1	7. Juli 2014	alle	Ersterstellung	BPT
0.5	16. Juli 2014	alle	Vervollständigung der Inhalte	BPT
0.6	21. Juli 2014	alle	Einarbeitung der Kommentare, Einführung des Kapitels 6	BPT
0.8	25. Juli 2014	alle	Einarbeitung der KBA-Kommentare, Vervollständigung Kapitel 6 und 7	BPT
0.8.2	30. Juli 2014	alle	Einarbeitung der Ergebnisse des 1. WS beim KBA	BPT
0.9	20. August 2014	alle	Einarbeitung der Ergebnisse des 2. WS beim KBA	BPT
0.9.1	27. August 2014	alle	Einarbeitung der Ergebnisse des 3. WS Entwurf des Kapitels 7	BPT
0.9.2	08. September 2014	alle	Einarbeitung der Ergebnisse des 4. Workshops	KBA
0.9.3	20. September 2014	alle	Einarbeitung der Ergebnisse des 4. Workshops	BPT
0.9.4/ 0.9.5	1. Oktober 2014	alle	Allgemeine redaktionelle Korrekturen	KBA
0.9.6	15. Oktober 2014	alle	Einarbeitung der Ergebnisse der UAG-Sitzung vom 9. Oktober 2014	BPT
0.9.6.1	11. November 2014	5.1	Hinweis auf Seite 11 – Einfügen des Wortes „idealerweise“. Herstellung der Konsistenz zu Kapitel 7 ID: A-6.1-11	KBA
1.0	13. November 2014	alle	Vorbereitung der Veröffentlichung (Layout)	KBA

Tabelle 1: Änderungsverzeichnis

Inhaltsübersicht

1 Allgemeines

1.1 Mitgeltende Dokumente

– Internetbasierte Fahrzeugzulassung (i-Kfz) – Anlage Penetrationstest
– Internetbasierte Fahrzeugzulassung (i-Kfz) – Grobkonzept – Version 2.0.2

Hinweis:

Es wird ausschließlich auf die Teile des zitierten Dokumentes verwiesen, welche die Umsetzung der 1. Stufe des i-Kfz-Projektes betreffen.

– Informationen zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt

1.2 Abkürzungsverzeichnis

API	Application Programming Interface
ALG	Application-Level Gateway
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-ISI	BSI Standards zur Internet-Sicherheit
BSI-TR	BSI Technische Richtlinie
BSI-ITG	BSI IT-Grundschutz
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BPT	Bearing Point
cnn	Connector
DMZ	Demilitarisierte Zone
DOI	Deutschland Online Infrastruktur
ESP	Encapsulated Security Payload
FZV	Fahrzeugzulassungsverordnung
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
i-Kfz	Internetbasierte Fahrzeugzulassung
ID	Identifikator/Kennung
IKEv1	Internet Key Exchange Protocol version 1
IP	Internet Protocol
IPSec	Internet Protocol Security
ISMS	Information Security Management System (Informationssicherheitsmanagementsystem)
IT	Informationstechnologie
KBA	Kraftfahrt-Bundesamt
KBAG	Gesetz über die Einrichtung eines Kraftfahrt-Bundesamtes
Kom-Modul	Kommunikation-Modul
MAC	Message Authentication Code
OpenFT	Open File Transfer
PFS	Perfect Forward Secrecy

SiKo	Sicherheitskonzept
SW	Software-Einheit
TLS	Transport Level Security
UAG	Unterarbeitsgruppe
URL	Uniform Resource Locator
VBN-Nr.	Verfügungs-Berechtigungs-Nachweis-Nummer
VG	Verpflichtungsgrad
VPN	Virtual Private Network
WS	Web Service
XML	Extended Markup Language
ZFZR	Zentrales Fahrzeugregister

Tabelle 2: Abkürzungsverzeichnis

1.3 Abbildungsverzeichnis

1.4 Tabellenverzeichnis

2 Ziel und Zweck des Dokuments

Im Verfahren internetbasierte Fahrzeugzulassung (i-Kfz) werden schutzbedürftige Daten verarbeitet, insbesondere bei der Kommunikation mit den zentralen Registern des Kraftfahrt-Bundesamtes (KBA). Mit diesem Dokument werden Mindestanforderungen an die Informationssicherheit bei der Anbindung dezentraler Portale definiert, die zwingend zu erfüllen sind.

Im Zuge der Umsetzung der ersten Stufe i-Kfz zum 1. Januar 2015 kann die Antragstellung auf Außerbetriebsetzung eines Fahrzeugs – neben dem zentralen Zugang über das beim KBA betriebene i-Kfz-Portal – auch über dezentrale kommunale Portale erfolgen. In Diskussionen zwischen BMVI, KBA, BSI, Vertretern von kommunalen Spitzenverbän-

den, kommunalen IT-Dienstleistern und Zulassungsbehörden wurde eine grundlegende Architektur für die Kommunikationswege bei der Anbindung dezentraler Portale festgelegt („Hamburger Kompromiss“).

Die dezentralen Portale greifen über das Internet (unsicheres Netz) auf die KBA-Infrastruktur zu. Die Anforderung zur Öffnung der KBA-Netze für diese Kommunikation stellt eine neue Art des Zugriffs auf das Zentrale Fahrzeugregister (ZFZR) dar und bringt damit Gefahren in Bezug auf Sicherheit und Datenschutz mit sich.

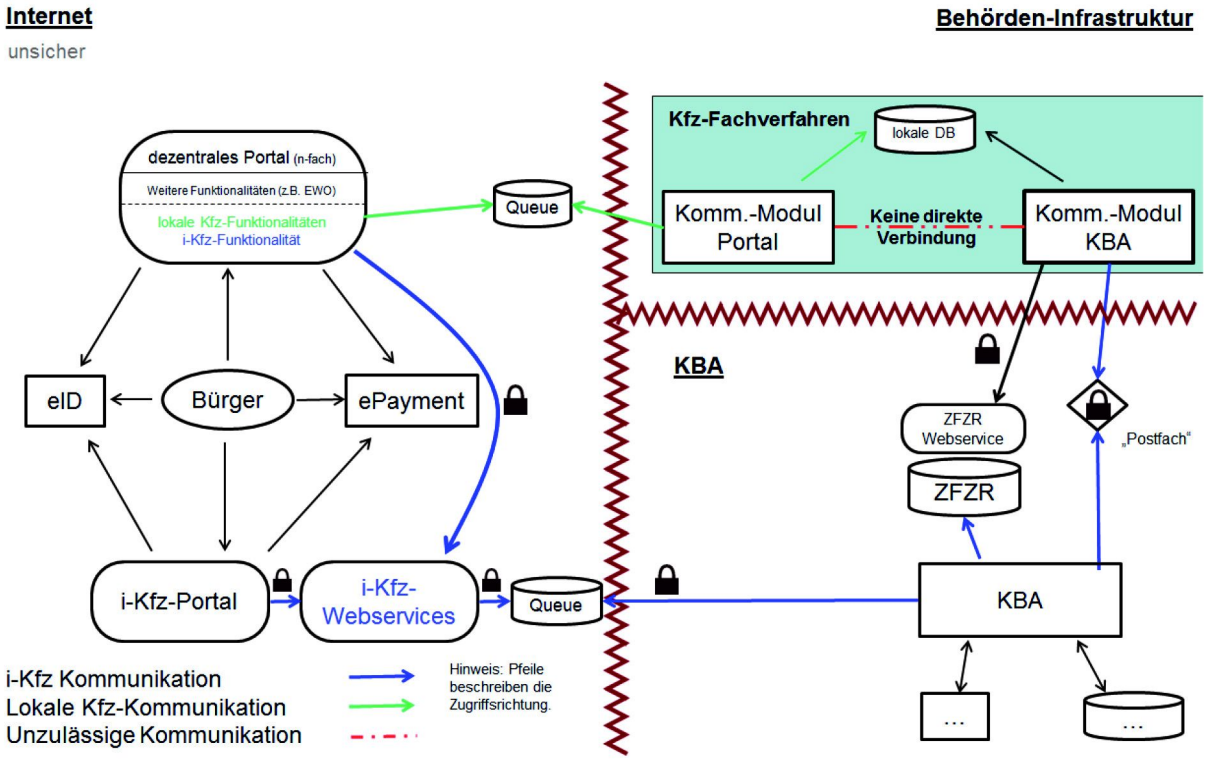

Abbildung 1: Kommunikationswege zur internetbasierten Außerbetriebsetzung („Hamburger Kompromiss“; Stand: 30. Juli 2014)

Vor diesem Hintergrund ist die Datensicherheit der zentralen Register beim KBA sicherzustellen. Um dies zu gewährleisten, hat das KBA Mindestanforderungen an die Informationssicherheit für die Anbindung dezentraler Portale in Stufe 1 i-Kfz festgelegt.

Die Mindestanforderungen orientieren sich zunächst grundsätzlich am Schutzbedarf „normal“ jeweils für die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit, z. T. gehen sie aufgrund spezifischer i-Kfz-Funktionalitäten darüber hinaus. Der Schutzbedarf für das i-Kfz-Verfahren wurde noch nicht abschließend bestimmt und die Vollständigkeit der Mindestanforderungen zur Erfüllung des Schutzbedarfes noch nicht geprüft. Ein entsprechendes Sicherheitskonzept mit ggf. integrierter Risikoanalyse existiert nicht. Somit ist eine ganzheitliche Betrachtung der Verfahrenssicherheit zum jetzigen Zeitpunkt noch nicht möglich.

Aus Sicht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind die vorliegenden Mindestanforderungen sinnvoll und angemessen und decken die wichtigsten Aspekte zur Informationssicherheit des i-Kfz-Verfahrens ab. Die Mindestanforderungen werden im weiteren Projektverlauf, abhängig von den Ergebnissen der UAG Datensicherheit, gegebenenfalls ergänzt und fortgeschrieben.

3 Rechtliche Regelungen

In diesem Kapitel wird der für das Projekt i-Kfz gegebene rechtliche Rahmen skizziert. Insbesondere wird auf die Rolle des KBA in Bezug auf die Ausgestaltung der Kommunikation zwischen KBA und Dritten eingegangen.

Es wurden folgende für das Projekt relevanten rechtlichen Grundlagen identifiziert:

- Gesetz über die Errichtung eines Kraftfahrt-Bundesamts (KBAG)
- Fahrzeug-Zulassungsverordnung (FZV)
- Viertes Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze (4. StVGuaÄndG)
- Bundesdatenschutzgesetz (BDSG)

Weiterführende geltende Regelungen:

– Information zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden (vergleiche [IznAaKBAfB]).

Das KBA nimmt gemäß [KBAG], [FZV] und [StVGuaÄndG] eine zentrale Rolle in der Gestaltung der Schnittstellen für die Kommunikation zwischen KBA und Dritten ein. Die Vorgaben für die betroffenen Schnittstellen sowie alle damit verbundenen Modalitäten werden vom KBA festgelegt.

„Das Kraftfahrt-Bundesamt übernimmt […] für Zwecke der Zulassung von Fahrzeugen und der Zuteilung von Kennzeichen die Errichtung und den Betrieb informationstechnischer Systeme für eine zentrale elektronische, auch internetbasierte Verarbeitung von für diesen Zweck erforderlichen Daten und deren Weiterleitung an die für den Vollzug zulassungsrechtlicher Vorschriften zuständigen Behörden und Stellen“, gemäß § 2 Absatz 1 Nummer 2a KBAG.

Weiterhin gilt es gemäß Artikel 2 Nummer 6 Buchstabe b [FZVuGebOStÄndV]:

„(2) Erfüllen die abgestempelten Kennzeichenschilder die Anforderungen des § 10 Absatz 3 Satz 2 bis 4 und die Zulassungsbescheinigung Teil I eines Fahrzeugs die Anforderungen des § 11 Absatz 1 Satz 1 und 2, so kann das Fahrzeug auch dadurch außer Betrieb gesetzt werden, dass der Halter oder der Verfügungsberechtigte dies bei der Zulassungsbehörde elektronisch über ein vom Kraftfahrt-Bundesamt betriebenes informationstechnisches System beantragt, das sicherstellt, dass

1. eine sichere Identifizierung des Antragstellers erfolgt und
2. die vom Halter oder Verfügungsberechtigten an das Kraftfahrt-Bundesamt übermittelten Daten vom Kraftfahrt-Bundesamt vollständig und plausibel an die Zulassungsbehörde übermittelt werden (internetbasierte Außerbetriebsetzung).“

Für die Gestaltung der Schnittstelle zwischen KBA und Dritten wurde dem Bundesrat ein Vorschlag zur entsprechenden Ergänzung der FZV im Herbst 2014 zugeleitet:

„Soweit für die internetbasierte Außerbetriebsetzung auf Systembestandteile zurückgegriffen wird, die einen Zugang zu den Daten des Kraftfahrt-Bundesamtes ermöglichen, hat die Übermittlung der Daten nach Maßgabe eines vom Kraftfahrt-Bundesamt im Bundesanzeiger und nachrichtlich im Verkehrsblatt veröffentlichten Standards zu erfolgen.“

4 Abgrenzung

Das vorliegende Dokument definiert die Mindestsicherheitsanforderungen, die zwingend bei der Umsetzung der 1. Stufe des i-Kfz-Projektes (Beginn zum 1. Januar 2015) zu berücksichtigen sind.

Dieses Dokument beinhaltet darüber hinaus Anforderungen, bzw. Teile von Anforderungen, die für die 1. Stufe nicht verpflichtend sind. Sie sind gesondert durch eine entsprechende Fußnote gekennzeichnet. Ab der 2. Stufe des i-Kfz-Projektes (Beginn zum 1. Januar 2016) sind die gekennzeichneten Anforderungen (bzw. deren Teile) als muss-Kriterien anzusehen und somit auch zwingend zu erfüllen.

5 Architektur des i-Kfz-Systems

Zur Beschreibung der Kommunikation innerhalb des i-Kfz-Systems wird in den folgenden Kapiteln eine Architektur definiert. Ausgehend von einer funktional gehaltenen Beschreibung der Informationsflüsse zwischen beteiligten Akteuren und Anwendungen (vergleiche Kapitel 5.1) wird eine technische Sicht auf das Gesamtsystem dargestellt (vergleiche Kapitel 5.2), in der die relevanten Netzwerkbereiche (vergleiche Kapitel 5.3), die darin enthaltenen Komponenten (vergleiche Kapitel 5.4), sowie die Schnittstellen (vergleiche Kapitel 5.5) untereinander benannt und beschrieben werden.

Hinweis:

Die in diesem Kapitel vorgestellte Architekturbetrachtung bezieht sich ausschließlich auf das i-Kfz-System. Im Kapitel 6 sind zusätzliche Einflussfaktoren (z. B. bereits existierende Kommunikationsverbindungen) auf die i-Kfz-Architektur dargestellt und beschrieben.

5.1 Kommunikationsarchitektur innerhalb des i-Kfz-Systems

Die Abbildung 2 stellt die Anwendungen, die primären Akteure und die zulässigen Kommunikationsflüsse aus funktionaler Sicht dar[1]. Es sind drei primäre Akteure beteiligt:

– Antragsteller Bürger,
– Antragsteller Großkunde,
– Sachbearbeiter in der Zulassungsbehörde.

[1] Gemäß der Stufe 1 der Realisierung.

Weiterhin werden (gemäß Stufe 1 des i-Kfz-Projektes) folgende Anwendungen genutzt:

– dezentrales Portal,
– zentrales Portal,
– Fachverfahren der Zulassungsbehörde,
– KBA-Dienste.

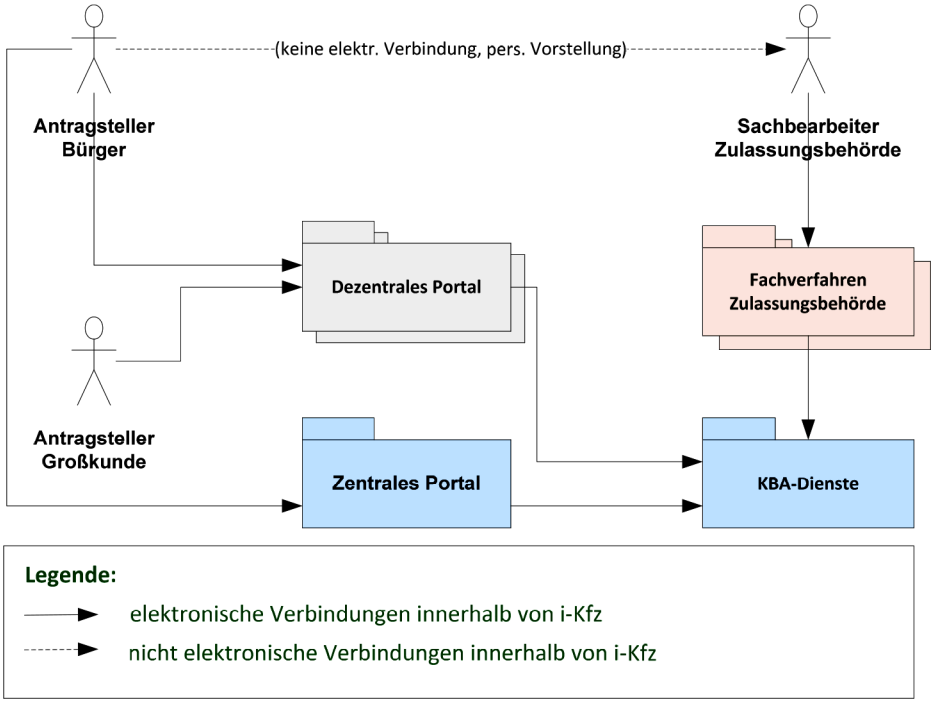

Abbildung 2: Primäre Akteure und Anwendungen sowie Kommunikationsflüsse im i-Kfz-System

Antragsteller Bürger

Die Rolle „Antragsteller Bürger“ bildet alle Personen ab, die die Dienste des zentralen oder eines dezentralen Portals über die graphische Benutzeroberfläche (GUI) in Anspruch nehmen.

Es ist zu beachten, dass darüber hinaus die Möglichkeit besteht, dass die antragstellende Person über bereits heute schon existierende Schnittstellen mit dem Fachverfahren der Zulassungsbehörde kommuniziert, z. B. um einen Termin mit der Zulassungsbehörde zu vereinbaren, ein Wunschkennzeichnen zu reservieren oder auch die benötigten Eingaben vorerfassen. Diese Anwendungen gehören nicht zum Funktionsumfang des i-Kfz-Projektes und sind nicht Betrachtungsgegenstand dieses Kapitels, sondern werden gesondert bei den externen Einflussfaktoren auf die i-Kfz-Architektur (Kapitel 6) berücksichtigt.

Antragsteller Großkunde

Die Rolle „Antragsteller Großkunde“ bezeichnet alle Antragsteller, die anstatt der graphischen Benutzerschnittstelle eine maschinen-verarbeitbare Schnittstelle zur Übermittlung der Antragsdaten nutzen. In der Regel handelt sich hier um Antragsteller, die eine relativ große Anzahl an Zulassungsvorgängen auf einmal erledigen müssen, z. B. Autohändler, Autovermietungen oder Flottenbetreiber.

Diese Schnittstelle dient dabei ausschließlich der Nutzung durch einen spezifischen Antragsteller in einem nicht-öffentlichen Bereich. Die Sicherheit kann bei einem Zugang über kaskadierende Portale nicht kontrolliert werden, diese sind daher im Verfahren nicht zuzulassen.

Da eine Großkundenschnittstelle im zentralen Portal nicht vorgesehen ist, erfolgt die Kommunikation ausschließlich über die dezentralen Portale. Eine alternative Kommunikationsbeziehung (z. B. zum Fachverfahren der Zulassungsbehörde) ist im Rahmen des Projektes i-Kfz nicht zulässig.

Sachbearbeiter in der Zulassungsbehörde

Innerhalb der Zulassungsbehörden bearbeiten die Sachbearbeiter die seitens der Antragsteller (Bürger und Großkunden) beantragten Leistungen.

Zentrales Portal

Das KBA stellt Bürgerinnen und Bürgern, deren zuständige Zulassungsbehörde kein dezentrales Portal anbietet, die internetbasierte Außerbetriebsetzung über ein zentrales Portal zur Verfügung. Diese Komponente ist nur für die erste Stufe des i-Kfz-Projektes vorgesehen und wird mit der Realisierung der vollständigen Abdeckung durch die dezentralen Portale ab Stufe 2 des i-Kfz-Verfahrens entfallen.

Das „zentrale Portal“ nimmt die Anfragen des Akteurs „Antragsteller Bürger“ entgegen und kommuniziert mit der Anwendung „KBA-Dienste“.

Dezentrales Portal

Im Auftrag der Zulassungsbehörden werden dezentrale Portale betrieben, welche analog zum zentralen Portal für die Bürgerinnen und Bürger eine internetbasierte Außerbetriebsetzung anbieten. Darüber hinaus bietet ein dezentrales Portal ggf. eine Webservice-Schnittstelle für die Benutzung durch die Großkunden an.

Ein dezentrales Portal kommuniziert im Rahmen des i-Kfz-Projektes ausschließlich mit den vom KBA hierzu bereitgestellten Diensten, sofern die KBA-Infrastruktur berührt wird. Von einem „dezentralen Portal“ können weitere lokale Funktionalitäten genutzt werden, die aber keine primäre i-Kfz-Funktionalität darstellen (z. B. ePayment, elektronischer Identitätsnachweis oder lokale Kfz-Funktionalitäten) und mit Hilfe von Schnittstellen in Anspruch genommen werden. Auf die Betrachtung dieser Wege wird im Dokument verzichtet.

Hinweis:

Nicht alle ca. 420 momentan existierenden Zulassungsbehörden werden ein eigenes dezentrales Portal betreiben. Es können sich Cluster bilden, in denen mehrere Zulassungsbehörden ein dezentrales Portal, angeboten durch einen Dienstanbieter (z. B. ein Landesrechenzentrum), gemeinsam nutzen. In solchen Fällen ist idealerweise auf eine Mandantentrennung in Verbindung mit einer sicheren Virtualisierung bezogen auf die einzelnen Zulassungsbehörden innerhalb des Clusters zu achten. Insbesondere sind eindeutige Zuständigkeiten im Bereich des Service Managements und der Administration sicherzustellen und zu dokumentieren.

Fachverfahren Zulassungsbehörde

Ein Fachverfahren in einer Zulassungsbehörde stellt eine Anwendung dar, in der die Anträge auf Außerbetriebsetzung eines Fahrzeugs durch einen Mitarbeiter der Zulassungsbehörde bearbeitet werden. Das Fachverfahren kommuniziert auf zweierlei Weise mit den KBA-Diensten:

- die im Rahmen des i-Kfz-Projektes gestellten Anträge werden seitens KBA dem Fachverfahren in der Zulassungsbehörde zur Verfügung gestellt und von der Zulassungsbehörde abgeholt (Kommunikationsverbindung: KBA-Dienste → Fachverfahren),
- das Fachverfahren liefert die Ergebnisse der Vorgangsverarbeitung an das KBA (Kommunikationsverbindung: Fachverfahren → KBA-Dienste).

Diese Kommunikationsverbindungen sind bereits heute technisch realisiert und werden durch die Zulassungsbehörden (außerhalb des i-Kfz-Projektes) benutzt, um die vor Ort durchgeführten Zulassungsvorgänge an das KBA zu übermitteln.

Hinweis:

Innerhalb der Zulassungsbehörden werden Fachverfahren unterschiedlicher Hersteller eingesetzt.

KBA-Dienste

Diese Anwendung symbolisiert die vom KBA angebotenen Dienste, unter anderem die Registerführung des ZFZR.

Ein Teil der KBA-Dienste wird bereits von den Zulassungsbehörden benutzt.

Hinweis:

Es ist zu beachten, dass im Rahmen der 1. Stufe des i-Kfz-Projektes jegliche Kommunikation zwischen dem Antragsteller und den Zulassungsbehörden über die Portale (hier sowohl zentral als auch dezentral) und das KBA (hier die KBA-Dienste) erfolgen muss. Es ist nicht zulässig, dass Antragsteller oder die Portale direkt über die Fachverfahren der Zulassungsbehörden mit dem KBA kommunizieren.

5.2 Technische Architektur des i-Kfz-Systems

Auf Basis der in Kapitel 5.1 beschriebenen Kommunikationsarchitektur wurde folgende technische Architektur für das i-Kfz-System definiert (vergleiche Abbildung 3), an der sich die Anbieter dezentraler Portale bei der Umsetzung der dezentralen Portale halten müssen.

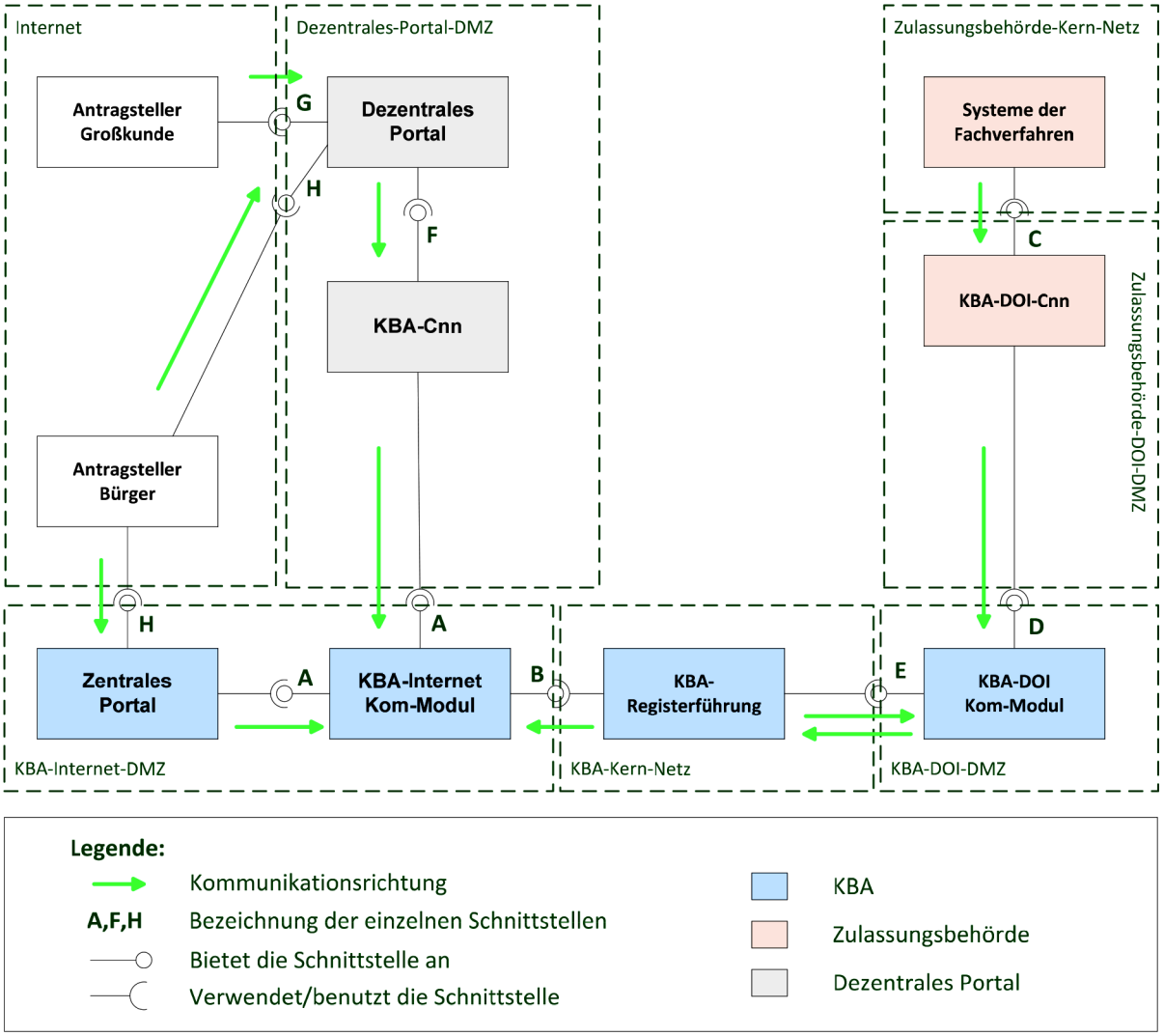

Abbildung 3: Technische Architektur des i-Kfz-Systems – das Gesamtbild

Im Folgenden werden die in der Architektur definierten Netzwerk-Bereiche und Komponenten sowie deren Schnittstellen beschrieben.

5.3 Netzwerkbereiche innerhalb des i-Kfz-Systems

Die im i-Kfz-System agierenden Kommunikationspartner sind unterschiedlichen Netzwerken (oder auch Netzwerksegmenten) zugeordnet. Eine Zuordnung der einzelnen Komponenten und Schnittstellen zu den Netzwerkbereichen ist der Abbildung 3 zu entnehmen.

In den folgenden Abschnitten werden die einzelnen Netzwerkbereiche, sowie deren Rolle im Gesamtverbund definiert. Die daraus abgeleiteten Sicherheitsanforderungen sind im Kapitel 7 beschrieben.

In der Abbildung 4 werden die identifizierten Netzwerkbereiche bzw. Netzwerke dargestellt und bezogen auf die untereinander auftretenden Kommunikationsflüsse in Relation gestellt.

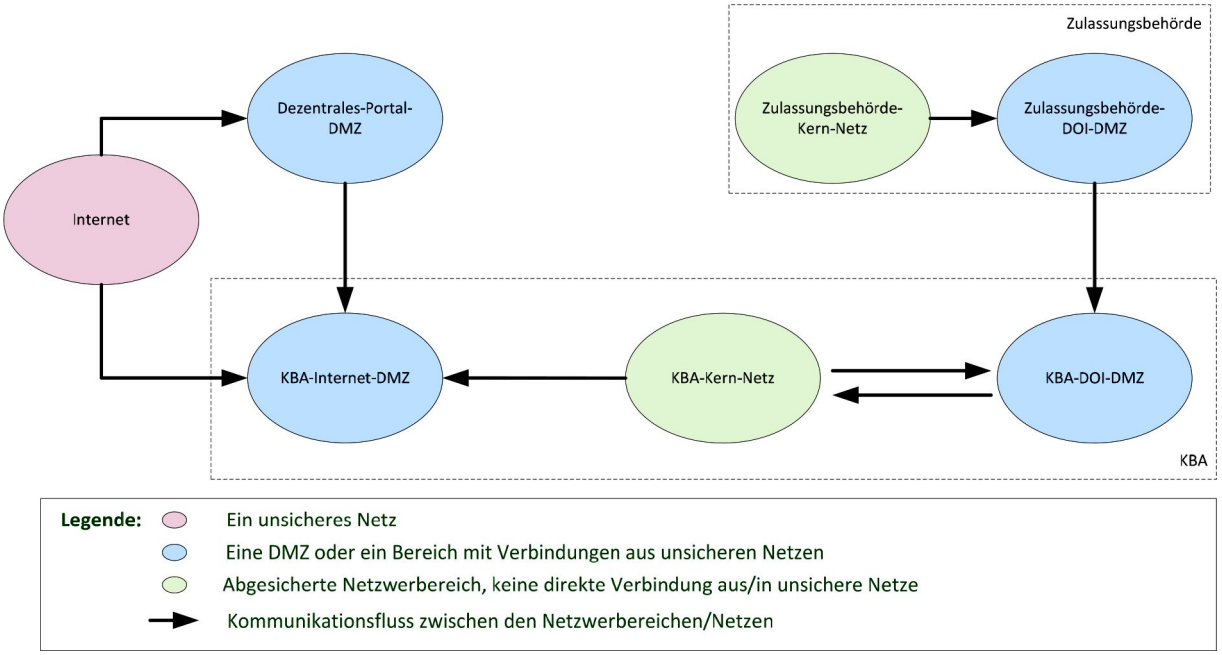

Abbildung 4: Netzwerkbereiche der definierten Architektur innerhalb i-Kfz

Hinweis:

Gemäß [BSI-ISI-LANA] wird eine Demilitarisierte Zone (DMZ) wie folgt definiert:

„Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein Netz dar, das weniger stark gesichert, aber vom äußeren Netz aus besser erreichbar ist als das eigentlich zu schützende interne Netz. Die DMZ dient der Schaffung eines zusätzlichen Sicherheitsbereichs für Dienste (z. B. E-Mail, Web) oder Proxys, die von externen Netzen aus nutzbar sein sollen, aber aus Sicherheitsgründen nicht im internen Netz platziert werden dürfen."

Mindestanforderungen an eine DMZ mit normalem Schutzbedarf sind die Verwendung von einem Paketfilter, von einem Application-Level-Gateway und von einem weiteren Paketfilter (die PAP-Struktur) für den Aufbau eines sogenannten Sicherheits-Gateways (vergleiche [BSI-ISI-LANA] und [BSI-ISI-WEB-SVR]).

5.3.1 KBA-Internet-DMZ

Die „KBA-Internet-DMZ" stellt ein separates Netzwerksegment innerhalb der KBA-Infrastruktur dar. Innerhalb dieses Netzwerksegmentes werden die Komponenten vom KBA zur Verfügung gestellt, die eine Abwicklung der i-Kfz-Szenarien über das Internet erlauben:

- „KBA-Internet-Kom-Modul" (vergleiche Kapitel 5.4.2),
- Das „zentrale Portal" (vergleiche Kapitel 5.4.1).

5.3.2 KBA-Kern-Netz

Die Kerndienste des KBA (hier KBA-Registerführung genannt, vergleiche Kapitel 5.4.3) werden innerhalb des Netzwerkbereiches „KBA-Kern-Netz" angeboten. Es handelt sich hierbei insbesondere um das ZFZR. Das „KBA-Kern-Netz" stellt einen geschützten Bereich dar, der von externen Netzwerken durch die Verwendung einer sogenannten DMZ separiert ist.

Es besteht keine Möglichkeit aus einer Internet-DMZ in das „KBA-Kern-Netz" eine Verbindung aufzubauen.

Es besteht auch keine Möglichkeit aus dem „KBA-Kern-Netz" eine Verbindung in ein externes Netzwerk (z. B. Internet oder auch DOI) zu eröffnen, ohne dass diese Verbindung über die korrespondierende DMZ (entsprechend „KBA-Internet-DMZ" oder „KBA-DOI-DMZ") verläuft.

Die innerhalb dieses Segmentes untergebrachten Dienste können mit Hilfe eines Puffer-Mechanismus (z. B. einer Nachrichtenschlange) mit den DMZ-Netzwerksegmenten kommunizieren.

5.3.3 KBA-DOI-DMZ

Die Zulassungsbehörden kommunizieren bereits heute aus der Komponente „Systeme der Fachverfahren"[2] heraus mit dem KBA über das Behördennetzwerk DOI. Diese Kommunikation ist entsprechend der Anforderungen des KBA formuliert innerhalb des Dokumentes „Information zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden" abzusichern.

[2] Der Name „Systeme der Fachverfahren" wurde stellvertretend gewählt und steht für alle für die Zulassungszwecke von den Zulassungsbehörden verwendeten Fachverfahren unterschiedlicher Hersteller. Es ist nicht eine besondere Fachanwendung gemeint.

Die im Rahmen des i-Kfz-Projektes zusätzlich geplante Kommunikation zwischen KBA und Zulassungsbehörden unter Verwendung eines Postfachs wird auf die bereits implementierten Transport-Mechanismen zurückgreifen.

5.3.4 Dezentrales-Portal-DMZ

Der Bereich „Dezentrales-Portal-DMZ“ beinhaltet die über das unsichere Medium Internet zugängliche Komponente „dezentrales Portal“ (vergleiche Kapitel 5.4.7) und die für die Kommunikation des dezentralen Portals mit dem KBA benutzte Komponente „KBA-Cnn“ (vergleiche Kapitel 5.4.8).

Es sind eingehende Kommunikationsverbindungen der Antragsteller (Großkunde und Bürger) erlaubt. Eine ausgehende Kommunikation ist nur in den Bereich „KBA-Internet-DMZ“ zulässig.

5.3.5 Zulassungsbehörde-Kern-Netz

Dieser Bereich beinhaltet die Komponente „Systeme der Fachverfahren“ der Zulassungsbehörde. Es ist keine direkt eingehende Kommunikation in diesen Bereich hinein zulässig. Es dürfen aus diesem Bereich ausgehende Verbindungen in den Bereich „Zulassungsbehörde-DOI-Netz“ hergestellt werden.

5.3.6 Zulassungsbehörde-DOI-DMZ

Die Komponenten, die die Kommunikation der Zulassungsbehörde mit dem KBA realisieren, werden im Bereich „Zulassungsbehörde-DOI-DMZ“ untergebracht. In diesem Bereich ist die eingehende Kommunikation aus dem Bereich „Zulassungsbehörde-Kern-Netz“ erlaubt. Weiterhin darf der Bereich ausgehend mit dem Bereich „KBA-DOI-DMZ“ über das DOI-Netz kommunizieren.

5.3.7 Internet

Dieser Bereich umfasst die Komponenten der Antragsteller:

– Bürger (vergleiche Kapitel 5.4.10)

– Großkunden (vergleiche Kapitel 5.4.9)

Außer der Abwicklung von Einzelanträgen über das zentrale bzw. über die dezentralen Portale kann es eine Möglichkeit für die sogenannten Großkunden (hier z. B. große Autohäuser, Flottenbetreiber oder Autovermietungsfirmen etc.) geben, über dezentrale Portale die Anträge nicht direkt über die graphische Benutzerschnittstelle des Portals einzugeben, sondern über eine maschinenlesbare Schnittstelle (vergleiche Kapitel 5.5.7) zu übermitteln.

5.4 Komponenten der Architektur innerhalb des i-Kfz-Systems

Die vorgestellten Netzwerkbereiche beinhalten System-Komponenten, die über definierte Schnittstellen miteinander kommunizieren.

5.4.1 Zentrales Portal

Das zentrale Portal wird durch das KBA bereitgestellt und ermöglicht die internetbasierte Antragstellung für die Außerbetriebsetzung eines Fahrzeugs (Stufe 1 i-Kfz). Das Portal ist dem Netzwerkbereich „KBA-Internet-DMZ“ zugeordnet. Die Kommunikation mit der übrigen KBA-Infrastruktur wird analog zu den dezentralen Portalen über das „KBA-Internet-Kom-Modul“ abgewickelt (vergleiche Kapitel 5.4.2).

5.4.2 KBA-Internet-Kom-Modul

Eine zentrale Rolle bei der Kommunikation aus dem Internet in das KBA-Netz übernimmt die Komponente „KBA-Internet-Kom-Modul“. Dieses Modul bietet zwei Schnittstellen an:

– Schnittstelle A – erreichbar aus dem Internet durch die dezentralen Portale, sowie aus dem der KBA-Internet-DMZ durch das zentrale Portal (vergleiche Kapitel 5.5.1),

– Schnittstelle B – erreichbar nur aus dem Intranet des KBA („KBA-Kern-Netz“), (vergleiche Kapitel 5.5.2).

Der interne Aufbau der Komponente „KBA-Internet-Kom-Modul“ ist der Abbildung 5 zu entnehmen. Das Modul nimmt die über die Schnittstelle A eingehenden Nachrichten entgegen und speichert diese über eine interne Schnittstelle k in einer Nachrichtenschlange, bis die Nachrichten über die Schnittstelle B abgeholt werden.

Die über die Schnittstelle B zurückgeschriebenen Antworten werden über die interne Schnittstelle k abgeholt und dann über die Schnittstelle A an die aufrufende Instanz als Antwort auf die Anfrage zurückgeschickt.

Eine logische synchrone Kommunikation über die Kommunikationsverbindung „dezentrales/zentrales Portal“ → „KBA-Internet-Kom-Modul“ → „KBA-Registerführung“ wird physikalisch durch den asynchronen Ansatz (die Verwendung der Nachrichtenschlange) auf der Kommunikationsverbindung „KBA-Internet-Kom-Modul“ → „KBA-Registerführung“ transparent für die aufrufende Instanz umgesetzt.

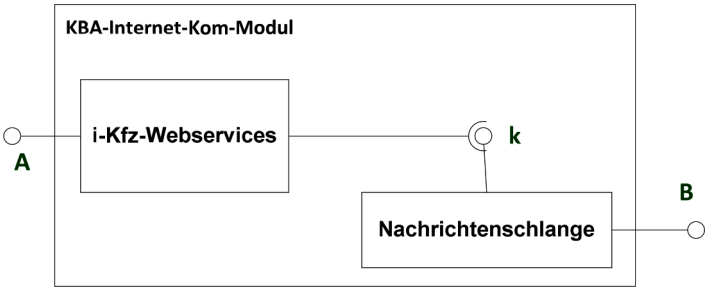

Abbildung 5: interner Aufbau der Komponente „KBA-Internet-Kom-Modul“ (schematische Darstellung)

5.4.3 KBA-Registerführung

Unter der „KBA-Registerführung“ werden Software-Komponenten (z. B. Verarbeitungsmodule, Datenbanken, ZFZR etc.) zusammengefasst, die innerhalb des Netzwerkbereiches „KBA-Kern-Netz“ in einer abgesicherten Umgebung ablaufen.

5.4.4 KBA-DOI-Kom-Modul

Die bereits zur Verfügung stehende Kommunikationsmöglichkeit zwischen einer Zulassungsbehörde und dem KBA über sichere Netze der öffentlichen Verwaltung (insbesondere DOI) wird in der Architektur durch die Komponente „KBA-DOI-Kom-Modul“ dargestellt.

Die eingehende Kommunikation von den Zulassungsbehörden wird mit Hilfe der Schnittstelle D (vergleiche Kapitel 5.5.4) und von der KBA-Registerführung mit Hilfe der Schnittstelle E (vergleiche Kapitel 5.5.5) entgegengenommen.

Die Kommunikation vom KBA an die Zulassungsbehörden wird analog umgesetzt. Die an eine Zulassungsbehörde adressierten Nachrichten werden mithilfe der Schnittstelle E von der KBA-Registerführung abgelegt und über die Schnittstelle D den Zulassungsbehörden zur Verfügung gestellt.

Das „KBA-DOI-Kom-Modul“ wickelt die Kommunikation dabei für zwei Anwendungsfälle ab, die bereits heute technisch implementiert sind und außerhalb der Funktionalität des i-Kfz-Projektes genutzt werden (vergleiche Abbildung 6)[3]:

– Die Zugriffe seitens der Zulassungsbehörde auf das Zentrale Fahrzeugregister (ZFZR-Webservice) – hier fragen die Behörden synchron einen Web-Service ab,

– die Zugriffe der Zulassungsbehörden auf das für die Zulassungsbehörden seitens KBA zur Verfügung gestellte Postfach – in dem Falle werden die Nachrichten asynchron (durch die Zulassungsbehörden) abgeholt und die Antwortnachrichten abgelegt.

[3] Die beiden Anwendungsfälle werden über die gleiche Schnittstelle bedient. Innerhalb des Moduls wird entschieden, welcher Anwendungsfall vorliegt. Anschließend wird eine entsprechende innere Komponente angesprochen.

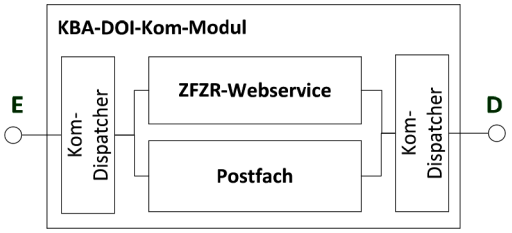

Abbildung 6: Interner Aufbau der Komponente „KBA-DOI-Kom-Modul“

5.4.5 KBA-DOI-Cnn

Dieses Modul stellt eine sichere Kommunikationsschnittstelle zwischen dem „Fachverfahren“ und dem „KBA-DOI-Kom-Modul“ über sichere Netze (insbesondere DOI) her. Die Komponente bietet die Aushandlung und Abwicklung einer abgesicherten Datenübertragung auf dem Transport-Level.

Das Modul bietet die Schnittstelle C (vergleiche Kapitel 5.5.3) an, die durch das Fachverfahren der Zulassungsbehörden bedient wird. Weiterhin spricht die Komponente die vom KBA betriebene Kommunikationsgegenstelle („KBA-DOI-Kom-Modul“) mit Hilfe der Schnittstelle D (vergleiche Kapitel 5.5.4) an.

Das Modul „KBA-DOI-Cnn“ bedient dabei zwei Anwendungsfälle:

– Bereits heute implementierter Zugriff seitens der Zulassungsbehörden auf den ZFZR-Webservice,

– der im Rahmen des i-Kfz-Projektes verwendete Zugriff auf das Postfach.

5.4.6 Systeme der Fachverfahren (Zulassungsbehörde)

Die Komponente „Systeme der Fachverfahren“[4] in der Zulassungsbehörde wird in dem sicheren Bereich „Zulassungsbehörde-Kern-Netz“ betrieben. Die Komponente „Systeme der Fachverfahren“ bietet keine Schnittstellen an, sondern bedient die von der Komponente „KBA-DOI-Cnn“ angebotene Schnittstelle C (vergleiche Kapitel 5.5.3).

[4] Der Name „Systeme der Fachverfahren“ wurde stellvertretend gewählt und steht für alle für die Zulassungszwecke von den Zulassungsbehörden verwendeten Fachverfahren unterschiedlicher Hersteller. Es ist nicht eine besondere Fachanwendung gemeint.

Die Komponente „Systeme der Fachverfahren“ ist immer eine Kommunikation initiierende Instanz und darf keine Kommunikationsanfragen entgegennehmen.

5.4.7 Dezentrales Portal

Die Komponente „dezentrales Portal“ bietet dem „Antragsteller Bürger“ die Schnittstelle H (vergleiche Kapitel 5.5.8) an und bedient die von der Komponente „KBA-Cnn“ (vergleiche Kapitel 5.4.8) angebotene Schnittstelle F (vergleiche Kapitel 5.5.6), über die die an das KBA adressierten Nachrichten weitergeleitet werden.

Eine Erweiterung gegenüber dem „zentralen Portal“ stellt die mit Hilfe der Schnittstelle G (vergleiche Kapitel 5.5.7) implementierte Möglichkeit der Abwicklung von Massenanfragen, die seitens sogenannter Großkunden abgesetzt werden können.

5.4.8 KBA-Cnn

Die Komponente „KBA-Cnn“ realisiert die Kommunikation zwischen einem „dezentralen Portal“ und dem KBA über die Komponente „KBA-Internet-Kom-Modul“ durch Aufbau einer gesicherten VPN-Verbindung. Der Informationsfluss verläuft stets vom „KBA-Cnn“ (Initiator) zum „KBA-Internet-Modul“ (Empfänger).

Der „KBA-Cnn“ bietet die Schnittstelle F (vergleiche Kapitel 5.5.6) gegenüber dem „dezentralen Portal“ an, welches die Nachrichten entgegennimmt. Die Nachrichten werden im nächsten Schritt an das „KBA-Internet-Kom-Modul“ über die Schnittstelle A (vergleiche Kapitel 5.5.1) weitergeleitet.

5.4.9 Antragsteller Großkunde

Eine Besonderheit des Systems stellen die sogenannten Großkunden dar, die beispielweise durch Autovermietungen, Flotten-Betreiber oder durch große Autohäuser vertreten sind. Die Fachverfahren der Großkunden kommunizieren über die Schnittstelle G (vergleiche Kapitel 5.5.7) mit einem dezentralen Portal.

Die Benutzung der Schnittstelle G ermöglicht eine performante Übertragung mehrerer Nachrichten (Massendaten). Eine Nutzung der graphischen Benutzerschnittstelle (GUI) des dezentralen Portals ist nicht notwendig.

5.4.10 Antragsteller Bürger

Die Antragstellergruppe „Bürger“ fasst die Bürgerinnen und Bürger zusammen, die mit Hilfe des zentralen Portals bzw. der dezentralen Portale eine Kfz-Angelegenheit abwickeln möchten. Es handelt sich hier um eine graphische Schnittstelle (GUI), die für Einzelangelegenheiten über einen Standardbrowser bedient werden kann. Die Kommunikation wird durch die Schnittstelle H (vergleiche Kapitel 5.5.8) charakterisiert.

5.5 Schnittstellen der Architektur innerhalb des i-Kfz-Systems

Die im Kapitel 5.4 vorgestellten Komponenten der Architektur werden über definierte Schnittstellen angesprochen. Es wurden insgesamt neun Schnittstellen definiert, die in den darauffolgenden Kapiteln detaillierter vorgestellt werden.

5.5.1 Schnittstelle A

Die Schnittstelle A wird vom „KBA-Internet-Kom-Modul“ angeboten und von den Komponenten „zentrales Portal“ (vergleiche Abbildung 7) und „dezentrales Portal“ (über das Modul „KBA-Cnn“, vergleiche Abbildung 8) genutzt.

Hinweis:

Die detaillierte technische Spezifikation der Schnittstelle ist in der seitens KBA zu Verfügung gestellten Information für Softwarehersteller und Verfahrensanbieter zu finden.

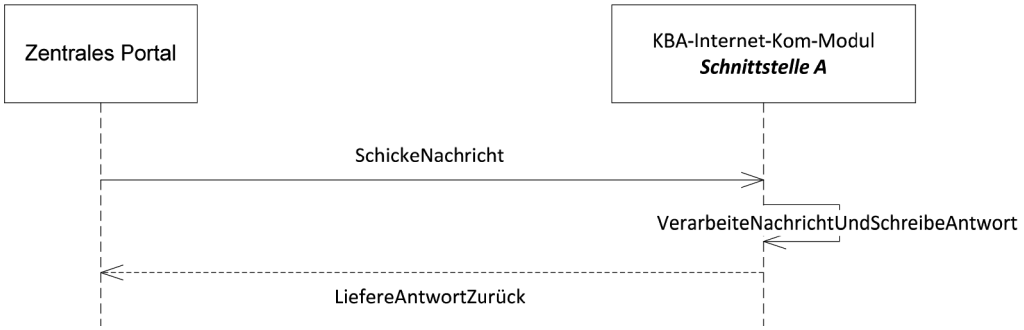

Abbildung 7: Verwendung der Schnittstelle A durch das zentrale Portal

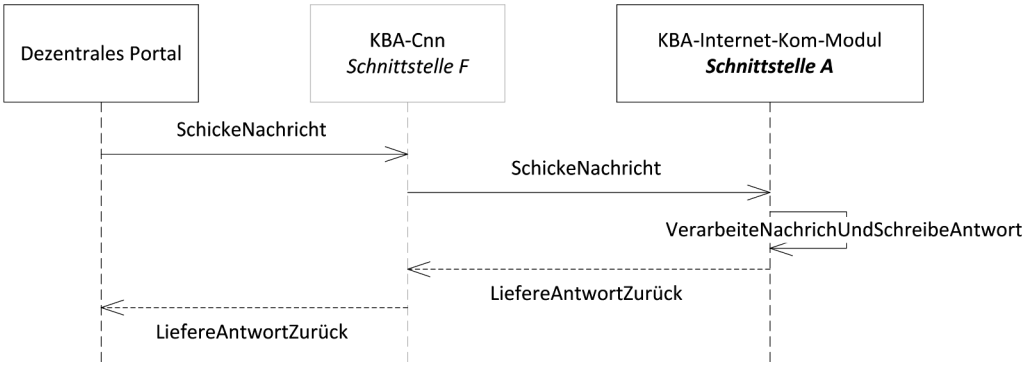

Abbildung 8: Verwendung der Schnittstelle A durch ein dezentrales Portal

Die Schnittstelle nimmt die für die weitere Verarbeitung durch die „KBA-Registerführung“ gedachten Nachrichten entgegen und puffert diese (z. B. in einer Nachrichten-Schlange) für die Abholung seitens der „KBA-Registerführung“. Auf dem gleichen Weg werden die Antworten der KBA-Registerführung in einen Puffer geschrieben, im nächsten Schritt aus dem Puffer ausgelesen und entsprechend über die Schnittstelle A an die aufrufende Instanz zurückgeliefert.

Es darf über die Schnittstelle A nur die eingehende Kommunikation behandelt werden. Es darf keine ausgehende Kommunikation über die Schnittstelle A realisiert werden. Die Antwortnachrichten werden synchron als Rückgabewerte zurückgeschrieben.

Die Schnittstelle ist mit Hilfe der Webservice-Technologie (WS-Technologie) realisiert und bietet die im Rahmen des i-Kfz-Projektes entwickelten i-Kfz-Webservices an.

Die Schnittstelle realisiert eine synchrone Kommunikation, die intern asynchron abgewickelt wird.

Die Nachrichten werden in einem vom KBA definierten XML-Format realisiert. Entsprechende Schemadateien und WS-Beschreibungen sind im geschützten Bereich der KBA-Internetseite[5] veröffentlicht.

[5] Siehe http://www.kba.de/DE/GeschuetzterBereich/ZentraleRegister/I_KFZ/i_fkz_inhalt.html?nn=644958

5.5.2 Schnittstelle B

Bei der Schnittstelle B handelt es sich um eine weitere Schnittstelle, die vom „KBA-Internet-Modul“ angeboten wird. Es ist eine interne KBA-Schnittstelle, die von außerhalb des Bereichs „KBA-Internet-DMZ“ mit Ausnahme des „KBA-Kern-Netz“ nicht sichtbar ist. Die „KBA-Registerführung“ aus dem „KBA-Kern-Netz“ greift auf diese Schnittstelle zu, um die für diese Komponenten bestimmten Nachrichten abzuholen.

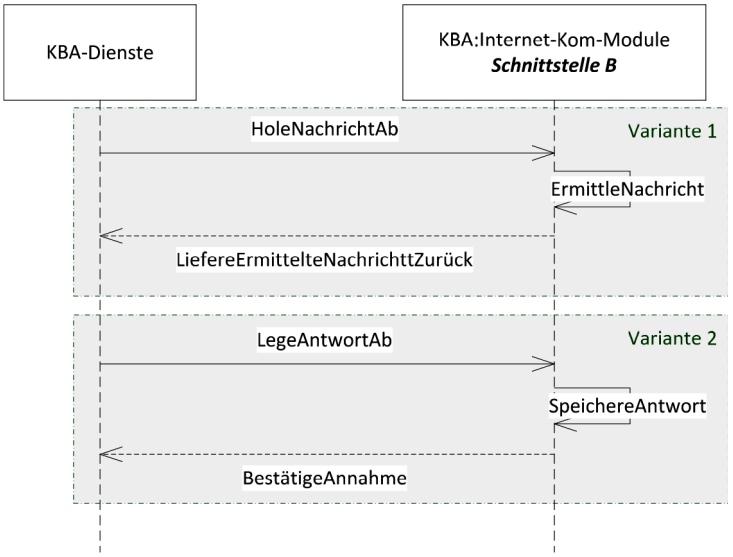

Abbildung 9: Verwendung der Schnittstelle B

Die Schnittstelle an sich wird im synchronen Modus betrieben, realisiert aber einen asynchronen Zugriff zwischen den Komponenten „KBA-Internet-Modul“ und „KBA-Registerführung“.

Die Nachrichten werden in einem vom KBA definierten XML-Format implementiert.

5.5.3 Schnittstelle C

Schnittstelle C definiert den Informationsfluss zwischen den Komponenten „Systeme der Fachverfahren“ und „KBA-DOI-Cnn“ und wird von der Komponente „KBA-DOI-Cnn“ angeboten. Die aus der Komponente „Systeme der Fachverfahren“ herausgehenden Nachrichten an die KBA-Infrastruktur, sowie das Abholen von aus der KBA-Infrastruktur herausgehenden Nachrichten an die Zulassungsbehörde (Postfach) werden über diese Schnittstelle realisiert.

Es werden zwei unterschiedliche Kommunikationsmodi unterschieden, die sich auf dem logischen Level unterscheiden, auf dem physikalischen Level jedoch gleich behandelt werden:

– Abschicken einer Nachricht aus der Komponente „Systeme der Fachverfahren“ an das KBA und Empfang einer Antwort – die Nachricht ist innerhalb der Komponente „Systeme der Fachverfahren“ erstellt worden und wird dann synchron an das KBA verschickt; die zeitnah generierte Antwort seitens KBA wird an die Komponente „Systeme der Fachverfahren“ als Rückgabewert zurückgeliefert (vergleiche Abbildung 10 – Variante 1),

– Abholen einer Nachricht des KBA an die Zulassungsbehörde und Ablegen einer Antwort durch die Zulassungsbehörde – in diesem Fall wird die Kommunikation seitens der Komponente „Systeme der Fachverfahren“ initiiert. Die Komponente „Systeme der Fachverfahren“ holt im ersten Schritt (erster Aufruf, vergleiche Abbildung 10 – Variante 2) die für sie bestimmte Nachricht ab, verarbeitet diese und legt ggf. die erzeugte Antwort an das KBA (zweiter Aufruf, vergleiche Abbildung 10 – Variante 3) ab.

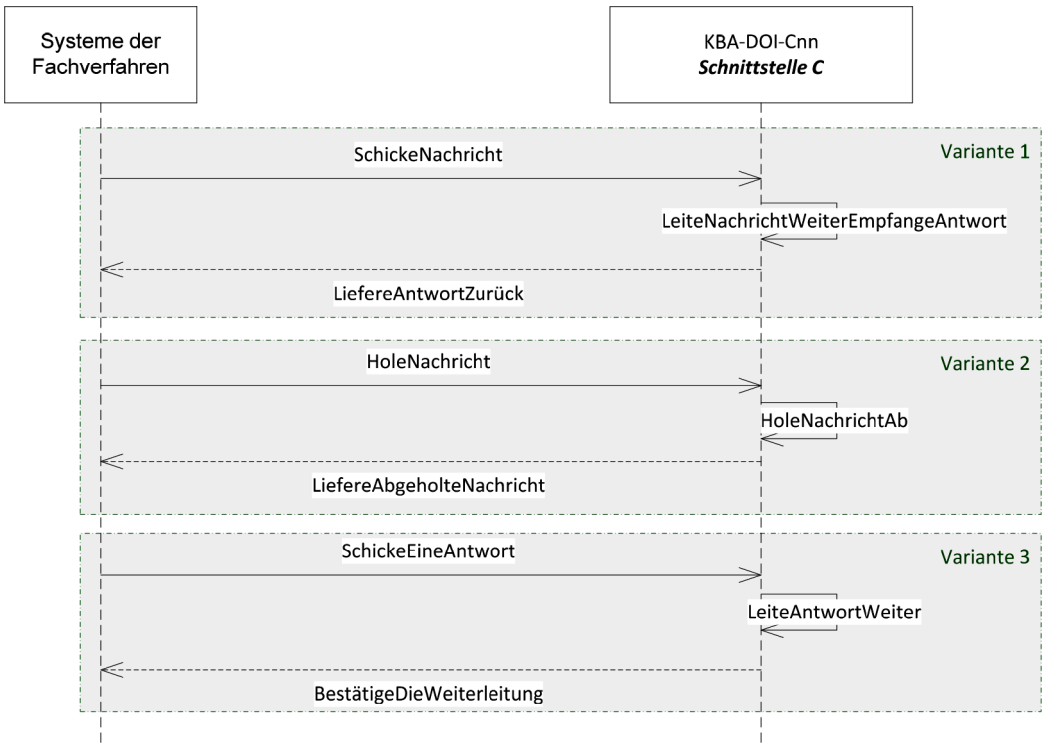

Abbildung 10: Verwendung der Schnittstelle C

Die Schnittstelle C leitet die Kommunikation transparent in den Bereich „KBA-DOI-DMZ“ weiter. Die Realisierung des zweiten Kommunikationsmodus (Zwischenspeicherung der Nachrichten) erfolgt im Bereich „KBA-DOI-DMZ“.

Hinweis:

Im Dokument „Informationen zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden“ (Kapitel 3) wird der Betrieb einer Kopfstelle innerhalb der Zulassungsbehörden beschrieben. Diese Kopfstelle bietet gegenüber der Komponente „Systeme der Fachverfahren“ die Schnittstelle C technisch an.

Die im Rahmen des i-Kfz-Projektes ausgetauschten Nachrichten sind in einem vom KBA festgelegten XML-Format implementiert.

5.5.4 Schnittstelle D

Die Kommunikation zwischen den Komponenten „KBA-DOI-Cnn“ und „KBA-DOI-Kom-Modul“ wird mit Hilfe der Schnittstelle D realisiert. Das funktionale Verhalten der Schnittstelle D entspricht dem Verhalten an der Schnittstelle C (vergleiche Kapitel 5.5.3). Die möglichen Nachrichten der Schnittstelle C sind genauso an der Schnittstelle D zu finden.

Es werden beide zur Schnittstelle C beschrieben Kommunikationsmodi unterstützt.

5.5.5 Schnittstelle E

Der Kommunikationsfluss zwischen den Modulen „KBA-Registerführung“ und „KBA-DOI-Kom-Modul“ wird durch die Schnittstelle E beschrieben. Die Komponente „KBA-Registerführung“ stellt dabei die aktive Instanz der Kommunikation dar und holt die eingehenden Nachrichten ab, bzw. legt die ausgehenden Nachrichten für die Weiterleitung an die Zulassungsbehörde ab.

Analog der Schnittstelle B ist diese Schnittstelle synchron implementiert, realisiert aber eine asynchrone Kommunikation zwischen den Komponenten „KBA-Registerführung“ und „KBA-DOI-Kom-Modul“.

5.5.6 Schnittstelle F

Die Schnittstelle F definiert die Gegebenheiten der Kommunikation zwischen einem „dezentralen Portal“ und dem „KBA-Cnn“. Der „KBA-Cnn“ nimmt die ausgehenden Nachrichten vom „dezentralen Portal“ entgegen und leitet diese an die KBA-Infrastruktur weiter, empfängt die eingehende Antwort und liefert diese an die aufrufende Instanz zurück.

Es ist eine synchrone Schnittstelle, die Nachrichten in einem vom KBA definierten XML-Format unterstützt.

Hinweis:

Es ist auch zulässig, dass die Schnittstelle F eine interne Schnittstelle innerhalb der Komponente „dezentrales Portal“ darstellt. In dem Fall ist die Komponente „KBA-Cnn“ in die Komponente „dezentrales Portal“ integriert.

5.5.7 Schnittstelle G

Mit Hilfe der Schnittstelle G wird die Kommunikation zwischen der Komponente „Antragsteller Großkunde“ und der Komponente „dezentrales Portal“ beschrieben. Es handelt sich um eine vollständig automatisierte Maschine-zu-Maschine-Schnittstelle (API), die ohne Mitwirkung von Menschen betrieben wird.

Die Komponente „Antragsteller Großkunde“ nimmt stets die Rolle des Initiators der Kommunikation an.

Im Rahmen des i-Kfz-Projektes findet keine Standardisierung der Schnittstelle G statt. Dieses Dokument legt allerdings allgemeine Sicherheitsmindestanforderungen fest (vergleiche Kapitel 7.2.7), die bei der Realisierung der Schnittstelle G beachtet werden müssen.

5.5.8 Schnittstelle H

Der Zugriff durch die antragstellende Person auf die dezentralen Portale und/oder auf das zentrale Portal wird durch die Schnittstelle H beschrieben. Die Schnittstelle H ist mit Hilfe der Web-Technologie realisiert und wird über einen Standardbrowser durch die Bürger bedient.

Form und Inhalt der auszutauschenden Informationen, sowie der Ablauf der einzelnen Schritte an der Schnittstelle sind im Rahmen des i-Kfz-Projektes spezifiziert worden. Eine genaue technologische Umsetzung ist nicht vorgeschrieben.

6 Externe Einflussfaktoren auf die Architektur des i-Kfz-Systems

Zusätzlich zu der im Kapitel 4 beschriebenen Architektur des i-Kfz-Systems können unterschiedliche außerhalb des i-Kfz-Projektes liegende Aspekte weitere Sicherheitsanforderungen notwendig machen. In diesem Kapitel werden zusätzliche Kommunikationsflüsse sowie deren Einfluss auf die Architektur dargestellt. Die identifizierten Sicherheitsanforderungen werden im Kapitel 7 beschrieben.

6.1 Zusätzliche Kommunikationsflüsse

Im Zuge der in den letzten Jahren innerhalb der Zulassungsfachverfahren durchgeführten Implementierungen sind insbesondere web-basierte Erweiterungen (z. B. Terminvereinbarung oder Reservierung eines Wunschkennzeichens, Vorerfassung von Zulassungsdaten) umgesetzt worden. Es ist daher davon auszugehen, dass die Zulassungsfachverfahren bereits einen direkten Zugang aus einem unsicheren Netzwerk in die lokalen Systeme der Zulassungsbehörden umgesetzt haben.

In Abbildung 11 ist dieser zusätzlich zu betrachtende Kommunikationsfluss zwischen einem dezentralen Portal und dem Fachverfahren in der Zulassungsbehörde mit einem rot gekennzeichneten Pfeil dargestellt.

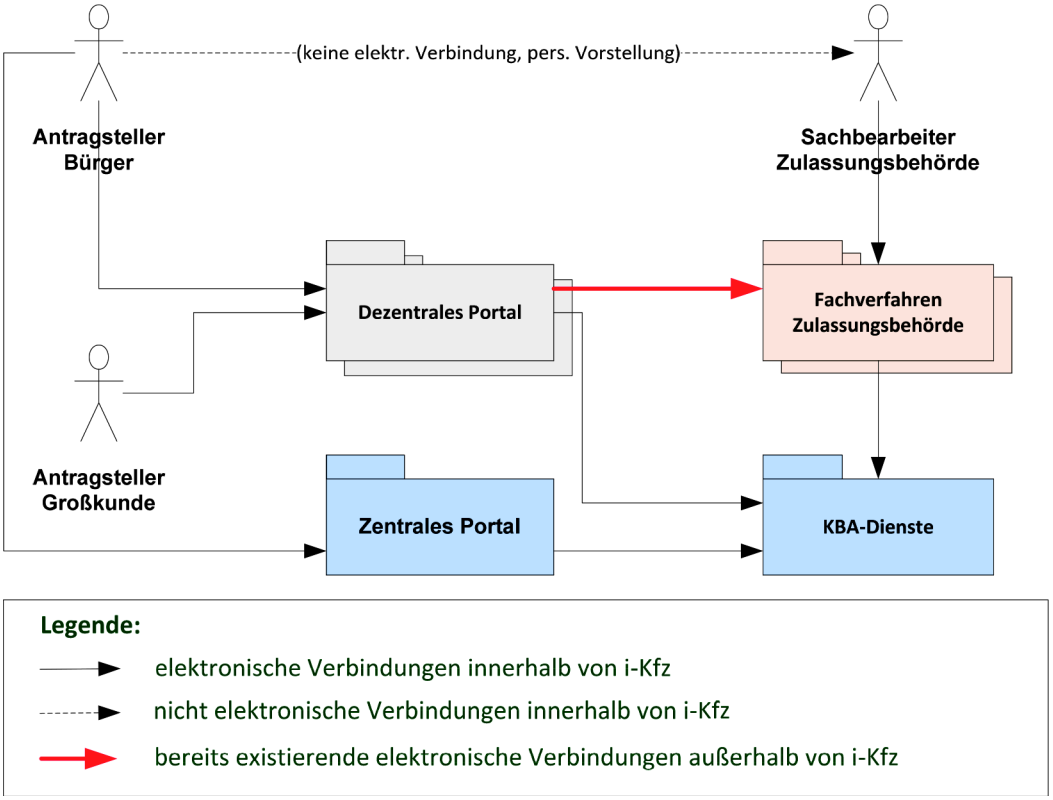

Abbildung 11: Zusätzliche Kommunikationsflüsse

6.2 Einfluss auf die technische Architektur des i-Kfz-Systems

Die im Kapitel 6.1 beschriebene zusätzliche Kommunikationsbeziehung zwischen den dezentralen Portalen und den Zulassungsbehörden bedingen eine Erweiterung der im Kapitel 5.2 definierten technischen Architektur. Insbesondere kommen folgende Elemente hinzu:

- zusätzlicher Netzwerkbereich – „Zulassungsbehörde-Internet-DMZ“
- zusätzliche Komponente – „Internet-Cnn“, die für die Abwicklung der aus dem Internet kommenden Kommunikation verantwortlich ist und
- zwei zusätzliche Schnittstellen – Schnittstelle X (zwischen Internet und dem Bereich „Zulassungsbehörde-Internet-DMZ“) und Schnittstelle Y (zwischen den Bereichen „Zulassungsbehörde-Internet-DMZ“ und „Zulassungsbehörde-Kern-Netz“).

Die zusätzlichen Elemente wurden in der Abbildung 12 rot umrahmt dargestellt und werden im weiteren Verlauf dieses Kapitels beschrieben.

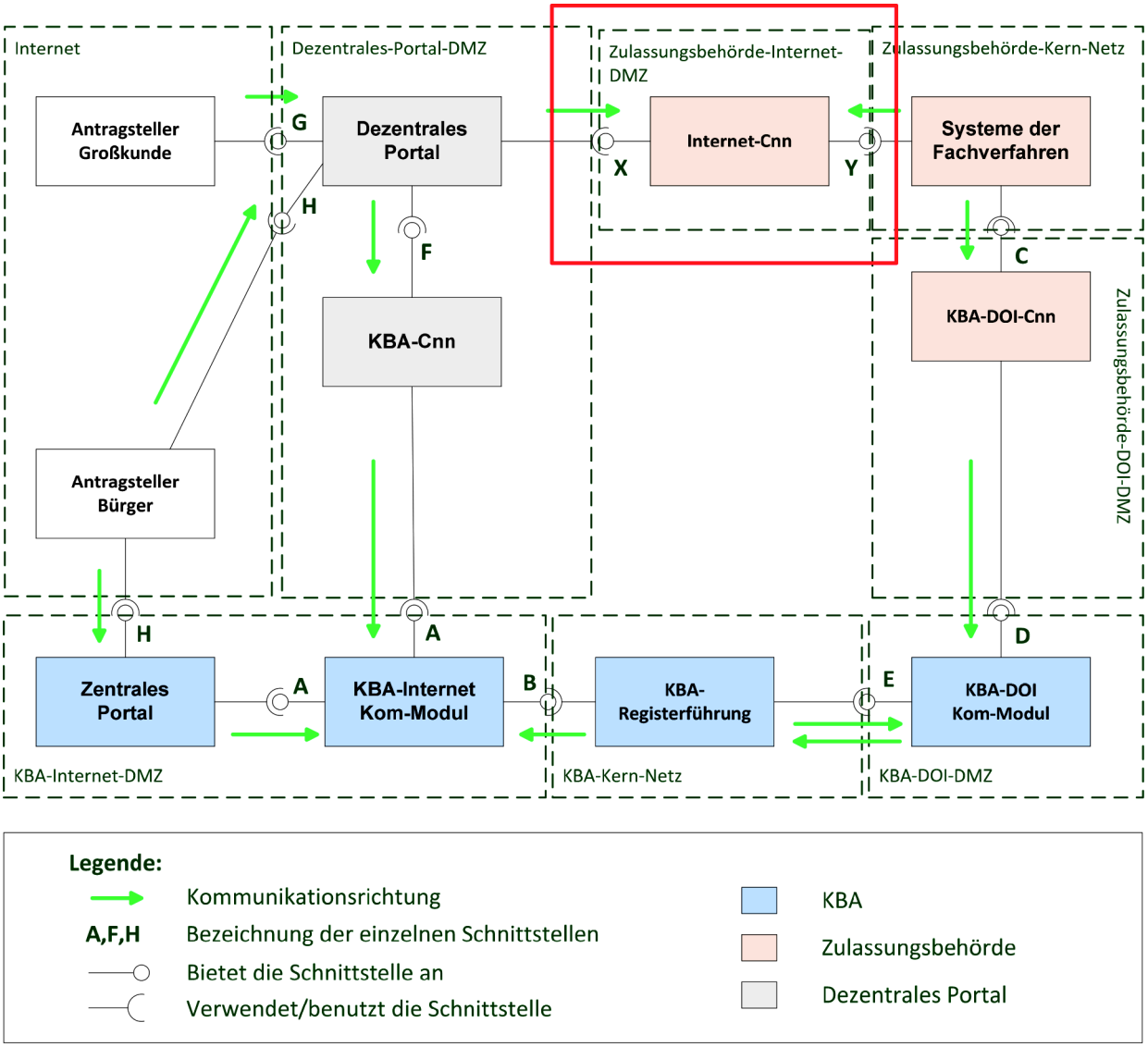

Abbildung 12: Erweiterte technische Architektur des i-Kfz-Systems

6.3 Zusätzliche Netzwerkbereiche

Mit der Öffnung des Zulassungsverfahrens für die Zugriffe aus einem unsicheren Netzwerkbereich (z. B. Internet) steigt die Gefahr des Kompromittierens eines Fachverfahrens. Da die Zulassungssoftware (die Komponente „Systeme der Fachverfahren“) über einen (insbesondere auch schreibenden) Zugriff auf das KBA-Register verfügt (Kommunikationsverbindung Systeme der Fachverfahren→KBA-DOI-Cnn→KBA-DOI-Kom-Modul→KBA-Registerführung), steigt somit auch die Gefahr eines unzulässigen Zugriffs auf die Kommunikationsverbindung Zulassungsbehörde-KBA (vergleiche Schnittstelle C, Kapitel 5.5.4).

Um dieser Gefahr entgegenzuwirken, wurde ein zusätzlicher Netzwerkbereich zwischen den unsicheren Netzen und dem abzusichernden Netzwerkbereich der Zulassungsbehörde geschaffen – „Zulassungsbehörde-Internet-DMZ“ (vergleiche dazu Kapitel 6.3.1).

In der Abbildung 13 wurde der zusätzliche Bereich rot umrahmt markiert.

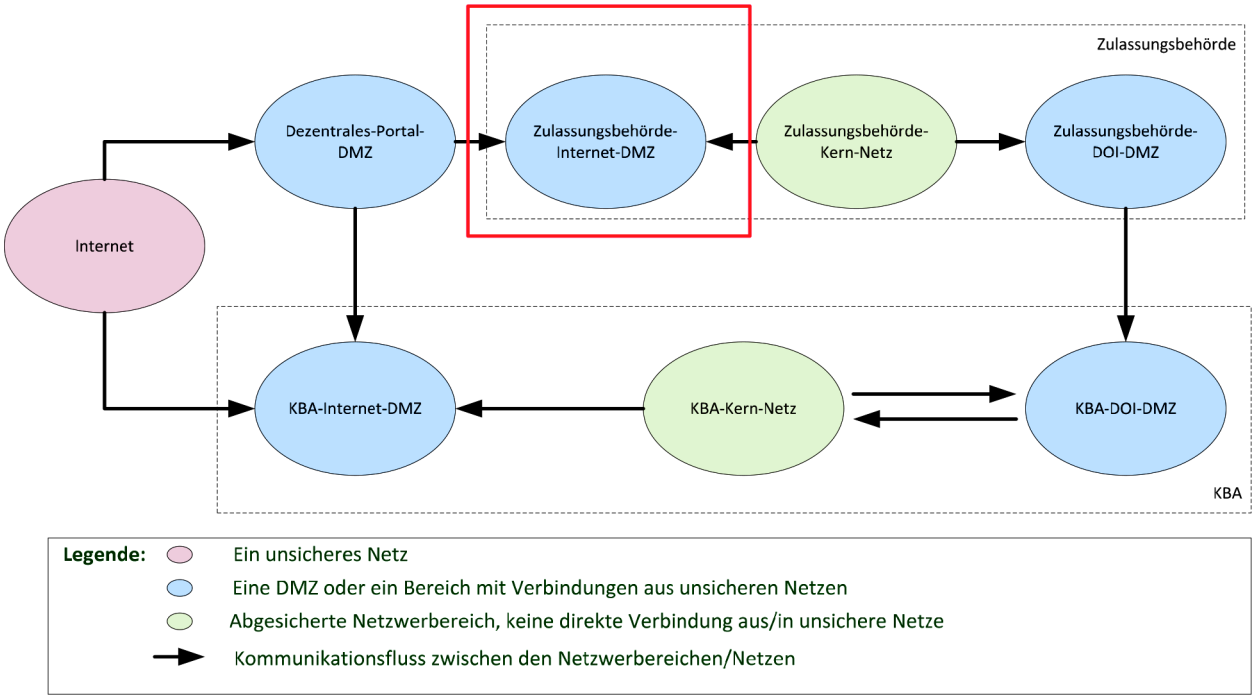

Abbildung 13: Erweiterte Zusammenstellung der Netzwerkbereiche

6.3.1 Zulassungsbehörde-Internet-DMZ

Die aus dem unsicheren Netzwerk (Internet) in den Bereich der Zulassungsbehörde eingehende Kommunikation wird in dem ersten Schritt im Netzwerkbereich „Zulassungsbehörde-Internet-DMZ“ empfangen.

Es handelt sich hier um die von den dezentralen Portalen ausgehende Kommunikation zur Zulassungsbehörde, die für die i-Kfz-Abwicklung benötigt wird (dezentrale i-Kfz-Funktionalität wie z. B. Gebührenrückstandsprüfung) oder um weitere Funktionen/Verfahren, die nicht innerhalb des i-Kfz-Verfahrens benötigt werden.

Eine weitere Kommunikationsmöglichkeit in dem Netzwerksegment „Zulassungsbehörde-Internet-DMZ“ besteht aus dem abgesicherten Netzwerkbereich der Zulassungsbehörde „Zulassungsbehörde-Kern-Netz“.

Hinweis:

Es ist zulässig, dass die beiden Bereiche „Dezentrales-Portal-DMZ“ (vergleiche dazu Kapitel 5.3.4) und „Zulassungsbehörde-Internet-DMZ“ zusammengelegt werden, wenn dies organisatorisch möglich ist (z. B. bei gleichem Betreiber). In einem solchen Fall wird die Komponente „dezentrales Portal“ innerhalb des Netzwerkbereiches „Zulassungsbehörde-Internet-DMZ“ betrieben.

Hinweis:

Es darf keine direkte, sowohl physikalische als auch logische, Verbindung zwischen den Komponenten aus dem Netzwerkbereich „Zulassungsbehörde-Internet-DMZ“ und den Komponenten aus dem Netzwerksegment „Zulassungsbehörde-DOI-DMZ“ existieren.

6.4 Zusätzliche Komponenten

Die beiden Kommunikationsflüsse im Netzwerkbereich „Zulassungsbehörde-Internet-DMZ“ werden durch die Komponente „Internet-Cnn“ abgewickelt (vergleiche Kapitel 6.4.1).

6.4.1 Internet-Cnn

Die Komponente „Internet-Cnn“ ist für den Empfang der aus dem Internet kommenden und an die Zulassungsbehörde adressierten Nachrichten sowie deren Angebot für die weitergehende Bearbeitung zuständig. Die Komponente bietet zwei Schnittstellen an:

- Schnittstelle X – über diese Schnittstelle wird die aus dem Internet kommende Kommunikation entgegengenommen (vergleiche Kapitel 6.5.1),
- Schnittstelle Y – mit Hilfe dieser Schnittstelle können die Komponenten aus dem Bereich „Zulassungsbehörde-Kern-Netz“ die an sie adressierten Nachrichten abholen und die generierten Antworten zur Verfügung stellen (vergleiche Kapitel 6.5.2).

Die beispielhafte schematische Darstellung der Komponente „Internet-Cnn“ ist in der Abbildung 14 dargestellt. Die logische synchrone Kommunikation zwischen den Komponenten „dezentrales Portal“ und „Systeme der Fachverfahren“ wird über folgende asynchrone Teilschritte abgebildet:

- Die interne Komponente „Internet-Server“ nimmt die Nachrichten (Anfragen) über die äußere Schnittstelle X entgegen (z. B. von der Komponente „dezentrales Portal“) und speichert diese über die interne Schnittstelle j in einem Nachrichtenpuffer (z. B. einer Nachrichtenschlange [Queue]).
- Die Komponente „Systeme der Fachverfahren“ greift über die Schnittstelle Y auf den Nachrichtenpuffer zu, liest die strukturierten Inhalte aus und prüft ihre Semantik. Anschließend holt sie die wartenden Nachrichten ab.
- Die abgeholten Nachrichten werden durch die Komponente „Systeme der Fachverfahren“ verarbeitet und die generierten Antwortnachrichten werden über die Schnittstelle Y in den Nachrichtenpuffer geschrieben.
- Die Komponente „Internet-Server“ holt die wartenden Antwortnachrichten über die interne Schnittstelle j ab und liefert diese als Antwort auf die korrespondierenden Anfragen, die zuvor über die Schnittstelle Y ankamen.

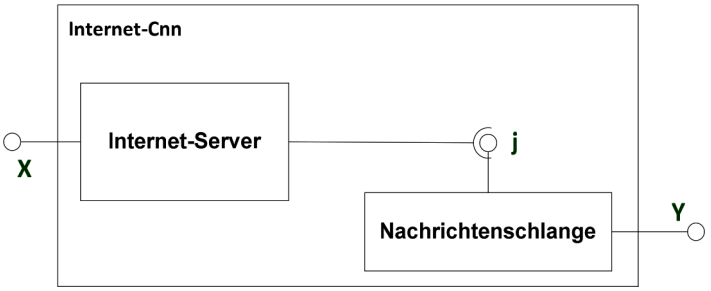

Abbildung 14: Schematische Darstellung des internen Aufbaus der Komponente „Internet-Cnn“

6.5 Zusätzliche Schnittstellen

6.5.1 Schnittstelle X

Die Kommunikation zwischen den Komponenten „dezentrales Portal“ und „Internet-Cnn“ (innerhalb der Zulassungsbehörde) wird über die Schnittstelle X realisiert. Der Initiator der Kommunikation ist dabei stets die Komponente „dezentrales Portal“. Die eingehenden Nachrichten werden von der Komponente „Internet-Cnn“ entgegengenommen und die Antworten an die aufrufende Instanz in einem synchronen Modus zurückgeliefert.

6.5.2 Schnittstelle Y

Die über das unsichere Netz (Internet) an die Zulassungsbehörden herangetragenen Nachrichten müssen in einem ersten Schritt von einem direkten Durchgriff auf das geschützte Kern-Netzwerk der Zulassungsbehörde separiert werden. Für diesen Zweck wurde der Netzwerk-Bereich „Zulassungsbehörde-Internet-DMZ“ geschaffen.

Die Komponente, die die eingehenden Nachrichten zwischenspeichert und die Schnittstelle Y anbietet, heißt „Internet-Cnn“. Die Schnittstelle wird von der Komponente „Systeme der Fachverfahren“ benutzt.

Die Kommunikation muss dabei stets von einer Komponente aus dem Bereich „Zulassungsbehörde-Kern-Netz“ initiiert werden.

Es darf keine Möglichkeit geben, dass die Kommunikation aus dem Bereich „Zulassungsbehörde-Internet-DMZ“ über die Schnittstelle Y im Bereich „Zulassungsbehörde-Kern-Netz“ initiiert werden kann.

7 Abgeleitete Sicherheitsanforderungen

In diesem Kapitel werden die allgemeinen und speziellen Sicherheitsanforderungen an die beschriebenen Schnittstellen der Architektur dargestellt.

Jede Anforderung besteht aus vier Teilen, die in Form einer Tabelle zusammengestellt sind (vergleiche Tabelle 3):

- ID – die im Rahmen dieses Dokumentes eindeutige Kennung der Anforderung: Die ID beginnt immer mit dem Großbuchstaben A, gefolgt von der Nummer des Kapitels, in dem die Anforderung beschrieben ist, gefolgt von der Nummer der Anforderung bezogen auf das jeweilige Kapitel (z. B. erhält die zweite Anforderung, die im Kapitel 6.2.6 beschrieben ist, die folgende ID: A-6.2.6-2),
- Anforderungstitel,
- Verpflichtungsgrad (VG),
- Anforderungsbeschreibung.

ID	Anforderungstitel	VG
Anforderungsbeschreibung		

Tabelle 3: Aufbau einer Sicherheitsanforderung

Der Verpflichtungsgrad einer Anforderung kann einen der folgenden Werte annehmen:

- „muss“ – eine „muss“-Anforderung ist unbedingt zu erfüllen,
- „soll“ – eine „soll“-Anforderung muss nicht unbedingt erfüllt werden, jedoch sind die Gründe im Falle einer Nichterfüllung zu dokumentierten,
- „kann“ – ist eine optionale Anforderung.

Hinweis:

Die Gruppe der „muss“-Anforderungen bildet die Mindestanforderungen, die erfüllt werden müssen.

7.1 Allgemeine Sicherheitsanforderungen

A-6.1-1	Kommunikationswege zwischen dezentralen Portalen und dem KBA	muss

Die Kommunikation zwischen den dezentralen Portalen und dem KBA darf nur über die vom KBA angebotene Schnittstelle A erfolgen.

A-6.1-2	Härtung ausgewählter Komponenten	muss

Einige Komponenten der Architektur müssen besonderen Härtungsmaßnahmen unterzogen werden, um die geforderte Resistenz gegenüber potentiellen Angriffen aufweisen zu können. Es handelt sich dabei um die folgenden Komponenten aus der Architektur:

- „dezentrales Portal“ (vergleiche Kapitel 5.4.7), insbesondere im Hinblick auf die Implementierung der Schnittstellen H und G sowie die Verwendung der Schnittstelle F,
- „Systeme der Fachverfahren“[6] (vergleiche Kapitel 5.4.6), insbesondere in Bezug auf die Verwendung der Schnittstellen C und Y.

Zur Bestätigung der erfolgreichen Härtung sind Penetrationstests durchzuführen. Die Ausgestaltung dieser Tests wird in dem Dokument „Anlage Penetrationstest“ durch das KBA zur Verfügung gestellt werden.

Diese Tests müssen durch unabhängige Experten durchgeführt werden. Eine Durchführung z. B. durch den Anwendungsentwickler, Betreiber oder Betriebsverantwortlichen ist nicht zulässig. Das beauftragte Unternehmen muss in dem Umfeld etabliert sein (z. B. durch Fachpublikation, vergleichbare Referenzen für Kunden).

Die während der Durchführung der Maßnahmen gefundenen Mängel müssen behoben und deren Beseitigung muss durch Nachtests nachgewiesen werden.

Die Einzelheiten des Vorgehens, insbesondere die Form und der Umfang der Mitteilung, werden durch das Zulassungsverfahren geregelt.

[6] Optional für die 1. Stufe, verpflichtend ab der 2. Stufe des i-Kfz-Projektes.

A-6.1-3	Organisatorische Sicherheit	muss

Es müssen mindestens folgende organisatorische Maßnahmen konzipiert und umgesetzt werden:

- Die Rolle des Sicherheitsbeauftragten muss besetzt werden[7].
- Ein ISMS muss etabliert und implementiert werden.
- Ein Zutrittskonzept muss erstellt und implementiert werden (vergleiche Anforderung A-6.1-5).
- Ein Zugangs- und Zugriffskonzept muss erstellt und implementiert werden (vergleiche Anforderung A-6.1-13).
- Die Fachkunde und Zuverlässigkeit des eingesetzten Personals muss gewährleistet werden (vergleiche Anforderung A-6.1-4).
- Ein Konzept für das Incident Management muss erstellt und implementiert werden (vergleiche Anforderung A-6.1-7).

[7] Die geforderte Rolle kann durch eine Einzelperson bzw. durch eine Gruppe Personen bekleidet werden. Es muss dabei gewährleistet sein, dass eine eindeutige Ansprechinstanz benannt ist.

A-6.1-4	Fachkunde und Zuverlässigkeit des Personals	muss

Der Betreiber der Komponenten „dezentrales Portal“ und „Systeme der Fachverfahren“ (Zulassungsbehörde) muss die erforderliche Fachkunde und Zuverlässigkeit nachweisen. In diesem Zusammenhang ist von besonderer Wichtigkeit, dass die Mitarbeiter im ausreichenden Maße geschult wurden.

Eine Schulung muss insbesondere eine Einarbeitung/Einweisung in die implementierten Funktionalitäten als auch eine Sensibilisierung hinsichtlich der sicherheitsrelevanten sowie datenschutzrechtlichen Aspekte der Anwendung beinhalten.

A-6.1-5	Räumliche Sicherheit	muss

Die räumliche Sicherheit muss gewährleistet werden.

Der Zutritt zu den Serverräumen muss geregelt und kontrolliert werden. Die herrschenden Regeln müssen in Form eines Zutrittskonzepts beschrieben werden. Die Anzahl der Zutrittsberechtigten muss dabei auf das notwendige Minimum beschränkt werden.

Der Zugang zu kritischen systemtechnischen Komponenten, insbesondere zu:

- „KBA-Cnn“ – Realisierung des VPN-Tunnels in die KBA-Infrastruktur,
- „KBA-DOI-Cnn“ – Implementierung des DOI-Zugangs mit PrivateWire/OpenFT in die KBA-Infrastruktur,

darf nur autorisierten Personen gewährt werden.

Es sind räumliche und organisatorische Maßnahmen zu treffen und zu dokumentieren, die diese Anforderung umsetzen.

A-6.1-6	System- und netztechnische Sicherheit muss sichergestellt werden.	muss

Die System- und netztechnische Sicherheit der eingesetzten Komponenten, insbesondere der Komponenten, die einen Zugriff aus nicht sicheren Netzwerkbereichen erlauben, muss sichergestellt werden.

Die Umsetzung der Funktionalitäten des dezentralen Portals muss netztechnisch (z. B. durch Einsatz geeigneter Paketfilter) von anderen angebotenen Anwendungen des Betreibers separiert werden.

Die aktuellen stabilen Sicherheitspatches und -updates und die netztechnische Absicherung der Komponenten (z. B. Verwendung von Paketfiltern, Application Layer Gateways etc.) müssen erfolgen und müssen fortlaufend gepflegt werden (vergleiche auch Anforderung A-6.1-7). Die Verwendung von aktiven Netzkomponenten ist zu bevorzugen.

Insbesondere folgende Komponenten der Architektur müssen verstärkt unter diesen Aspekten betrachtet werden, die alle einem Zugriff aus einem unsicheren Netzwerkbereich (z. B. Internet etc.) ausgesetzt sind:

- „dezentrales Portal“,
- „zentrales Portal“,
- „KBA-Internet-Kom-Modul“,
- „Systeme der Fachverfahren“[8],
- und ferner „Internet-Cnn“.

Die Vorgaben und Empfehlungen des BSI insbesondere zum Thema „sicheres Bereitstellen von Web-Angeboten“ gemäß [BSI-ISI] müssen beachtet und umgesetzt werden.[9]

Die geplanten Regeln zur Umsetzung der Maßnahmen zusammen mit den Verantwortlichen für deren Umsetzung und dazugehörige Management-Prozess müssen innerhalb des Informationssicherheitskonzepts dargestellt werden.

[8] Optional in der 1. Stufe, ab der 2. Stufe des i-Kfz-Projektes verpflichtend.

[9] Vergleiche https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/ISi-Reihe/ISi-Web-Server/web_server_node.html

Hinweis:

Im Rahmen dieses Dokumentes gilt folgende Definition des Begriffes „Sicherheitsvorfall“.

Als Sicherheitsvorfall wird im Rahmen dieses Dokumentes ein Ereignis verstanden, das die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme bzw. IT-Anwendungen, die innerhalb des i-Kfz-Projektes zum Einsatz kommen, derart beeinträchtigt, dass ein großer Schaden für die beteiligten Akteure entstehen kann.

A-6.1-7	Incident Management	muss

Ein tragfähiges Incident Management muss konzipiert (Incident-Management-Konzept) und eingeführt werden, insbesondere im Hinblick auf den Umgang mit:

- Informationssicherheitsvorfällen,
- Patching-Policy.

Das Konzept muss insbesondere die Reaktion auf gemeldete Schwachstellen sowie festgestellte Sicherheitsvorfälle, sowie eine damit verbundene Patching-Strategie beinhalten. Weiterhin müssen die Verantwortlichkeiten und der zeitliche Rahmen für die Durchführung von diesbezüglichen Maßnahmen deutlich definiert werden.

A-6.1-8	Ein Informationssicherheitskonzept muss erstellt werden.	muss

Die im Rahmen der Architektur genannten Komponenten und Schnittstellen müssen einer Informationssicherheitskonzeption unterzogen werden, die sich am [BSI-ITG-100-2] (IT-Grundschutz) orientiert. Insbesondere die folgenden Komponenten müssen betrachtet werden:

- „dezentrales Portal“,
- „KBA-Cnn“,
- „Internet-Cnn“,
- „Systeme der Fachverfahren“,
- „KBA-DOI-Cnn“[10].

[10] Optional für die 1. Stufe, ab der 2. Stufe des i-Kfz-Projektes verpflichtend.

A-6.1-9	Kommunikation zwischen den Komponenten	muss

Jede Komponente darf ausschließlich über die ihr im Rahmen der technischen Architektur zugeordneten Komponenten kommunizieren.

Es ist nicht zulässig, dass eine direkte Weiterleitung von Nachrichten aus dem Netzwerkbereich „Zulassungsbehörde-Internet-DMZ“ über die Komponente „Systeme der Fachverfahren“ (in dem Netzwerkbereich „Zulassungsbehörde-Kern-Netz“) in den Netzwerkbereich „Zulassungsbehörde-DOI-DMZ“ (eine Art von 1-zu-1-Weiterleitung) implementiert ist.

A-6.1-10	Demilitarisierte Zonen	muss

Die in der vorgestellten Architektur abgebildeten demilitarisierten Zonen (DMZ) müssen gemäß der Vorgaben des BSI erstellt werden (vergleiche [BSI-ISI-LANA] und [BSI-ISI-SVR]).

Insbesondere muss durch einen geeigneten Einsatz von Paketfiltern und Application Layer Gateways die Trennung der Kern-Netze von den unsicheren Netzen realisiert werden.

Der Aufbau der benutzten DMZ muss zumindest der von BSI definierten PAP-Struktur (Paketfilter-Application Layer Gateway – Paketfilter) entsprechen.

A-6.1-11	Mandantentrennung	muss

Im Falle des Betriebs für mehrere Mandaten (z. B. dezentrale Portale für mehrere Zulassungsbehörden) muss eine Mandantentrennung konzipiert und implementiert werden.

Insbesondere die Administrationsebene (System-Management) muss mandantenfähig implementiert werden, hierbei sind u. a. die Zuständigkeiten der Administration für konkrete Mandanten festzulegen.

Wird die Mandantenfähigkeit mit Hilfe von Virtualisierung implementiert, dann muss die sogenannte IT-System-Virtualisierung (Virtualisierung von vollständigen Server-Systemen) verwendet werden. Die Aspekte der sicheren Virtualisierung müssen gemäß dem Baustein „B 3.304 Virtualisierung“ der IT-Grundschutzkataloge unter der Berücksichtigung der darin enthaltenen Maßnahmenempfehlungen implementiert werden. Insbesondere die Isolation und Kapselung der einzelnen Mandanten (sowohl auf Anwendungs- als auch Datenhaltungsebene) muss gewährleistet werden.

Eine eindeutige Zuordnung der personellen Zuständigkeiten und Ausgestaltung der Zugriffsrechte im administrativen Bereich, bezogen sowohl auf den Bereich eines einzelnen Mandanten, als auch auf die Virtualisierungsumgebung selbst (insbesondere die Beschränkung der Zugriffsrechte der Administratoren der Virtualisierungsumgebungen) muss gegeben sein.

Als Informationsquelle zum Thema Mandantenfähigkeit (insbesondere als Orientierungshilfe hinsichtlich der datenschutzrechtlichen Aspekte) kann [BFDI-OHM] genutzt werden.

A-6.1-12	Nachweispflicht gegenüber KBA	muss

Die Erfüllung der im Rahmen dieses Dokumentes verfassten Mindestanforderungen muss in Form eines schriftlichen Berichtes erstellt und dem KBA im Zuge des im Kapitel 8 beschriebenen Zulassungsverfahrens nachgewiesen werden.

Die genaue Ausgestaltung des Berichts wird im Zuge des Zulassungsverfahrens durch das KBA bereitgestellt werden.

A-6.1-13	Zugangs- und Zugriffskonzept	muss

Der Zugang und Zugriff auf die sicherheitskritischen IT-Systeme muss konzipiert und implementiert werden (der Zugang in Form des Aufbaus einer Verbindung zwischen einem Nutzer und einem IT-System).

Insbesondere der Zugriff von einzelnen Administratoren auf die IT-Systeme, bzw. deren Bereiche, muss berücksichtigt werden (vergleiche auch hierzu die Anforderung A-6.1-11).

Die Anzahl der Administratoren, die volle Administrationsrechte besitzen, muss auf wenige Personen reduziert werden.

Der administrative Zugang zu den IT-Systemen muss über ein separates logisches Administrationsnetzwerk implementiert werden.

7.2 Sicherheitsanforderungen an die Schnittstellen der Architektur

Basierend auf der Beschreibung des Verhaltens an den Schnittstellen werden in diesem Kapitel Sicherheitsanforderungen an die einzelnen Schnittstellen der Architektur definiert.

Die Anforderungen werden sowohl an die im Kapitel 4 aufgeführten Schnittstellen der Architektur des i-Kfz-Systems als auch an die im Kapitel 6 dargestellten Schnittstellen der erweiterten Architektur gerichtet.

7.2.1 Anforderungen an die Schnittstelle A

Das Verhalten der Schnittstelle A wurde im Kapitel 5.5.1 erläutert.

Es wurden folgende Anforderungen an die Schnittstelle A abgeleitet.

A-6.2.1-1	Die Verbindung muss mit Hilfe eines IPSec-Tunnels aufgebaut werden.	muss

Die Kommunikation muss über einen auf Basis von IPSec-Technologie basierenden VPN-Tunnel ablaufen. Die Transportverschlüsselung wird an der Schnittstelle A aufgelöst.

Die Verbindung muss in einem Tunnelmodus und mit Hilfe des Protokolls Encapsulated Security Payload (ESP) in Verbindung mit dem Protokoll IKEv1 aufgebaut werden.

Die von Bundesamt für Sicherheit in der Informationstechnik publizierten Vorgaben zur Verwendung von IPSec gemäß [BSI-TR02102-3] müssen eingehalten werden.

Die genaue Konfiguration der IPSec-Verbindung wird vom KBA im Zuge des Zulassungsverfahrens zur Verfügung gestellt.

A-6.2.1-2	Die IPSec-Kommunikationsteilnehmer müssen beiderseitig authentifiziert werden.	muss

Während des Verbindungsaufbaus muss die gegenseitige Authentifizierung der Kommunikationsparteien des IPSec-Tunnels stattfinden.

Die genaue Konfiguration des mit dem IPSec-Protokoll zusammenhängenden Mechanismus wird vom KBA im Zuge des Zulassungsverfahrens bereitgestellt.

A-6.2.1-3	Die Vertraulichkeit der Daten muss gewährleistet werden.	muss

Die Verschlüsselung der Datenübertragung auf dem Transport-Level muss gewährleistet werden.

Die Daten müssen über den aufgebauten VPN-Tunnel empfangen werden. Die Verwendung des vorgeschriebenen Protokoll ESP sichert die Vertraulichkeit zu.

Es müssen die Vorgaben des BSI gemäß [BSI-TR02102-3] erfüllt werden.

Die genaue Auflistung der benutzten Parameter wird vom KBA im Zuge des Zulassungsverfahrens bereitgestellt.

A-6.2.1-4	Die Integrität der Daten muss gewährleistet werden.	muss

Die während der Übertragung ggf. von Dritten an den transportierten Daten vorgenommenen Änderungen müssen vom Empfänger erkannt werden.

Die Daten müssen über den aufgebauten VPN-Tunnel empfangen werden. Die Verwendung des vorgeschriebenen Protokolls ESP sichert die Integrität der Daten zu.

A-6.2.1-5	Authentifizierung des i-Kfz-WS-Clients	muss

Der vom Portal kommende Aufruf des i-Kfz-Webservices muss authentifiziert werden.

Die genauen Eingaben zum benutzten Mechanismus werden vom KBA im Zuge des Zulassungsverfahrens bereitgestellt.

7.2.2 Anforderungen an die Schnittstelle B

Interne Schnittstelle des KBA.

7.2.3 Anforderungen an die Schnittstelle C

Die Schnittstelle C ist im Kapitel 5.5.3 vorgestellt worden. Es wurden folgende Anforderungen an die Schnittstelle C abgeleitet.

A-6.2.3-1	Verwendung der Schnittstelle C	muss

Die Schnittstelle C muss von einer Komponente aus dem Bereich „Zulassungsbehörde-DOI-DMZ“ angeboten werden und darf nur von Komponenten aus dem Bereich „Zulassungsbehörde-Kern-Netz“ verwendet werden.

Insbesondere ist es explizit verboten, dass eine Komponente aus dem Bereich „Zulassungsbehörde-Internet-DMZ“ über einen Zugriff auf die Schnittstelle C verfügt.

Weiterhin müssen die beiden Bereiche „Zulassungsbehörde-Internet-DMZ“ und „Zulassungsbehörde-DOI-DMZ“ gänzlich voneinander getrennt werden.

Ergänzend ist in diesem Zusammenhang die Anforderung A-6.2.10-1 zu beachten.

A-6.2.3-2	Die Integrität und Vertraulichkeit der Daten.	muss

Die im Dokument „Informationen zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden“ enthaltenen Vorgaben zum sicheren Betrieb müssen eingehalten werden.

Die Vorgaben aus [BSI-TR02102-1] zu Algorithmen und Schlüssellängen müssen beachtet werden.

A-6.2.3-3	Die Nachvollziehbarkeit muss gewährleistet werden.	muss

Die Nachvollziehbarkeit der Kommunikation durch die Schnittstelle C ist von großer Bedeutung. Die Zugriffe auf der Schnittstelle C müssen sicher protokoliert werden. Die Protokolldaten unterliegen einer engen Zweckbindung und dürfen ausschließlich dem Zweck der Entdeckung und Erörterung der Gründe von potentiell aufkommenden Unregelmäßigkeiten in der Kommunikation dienen (Sicherstellung des ordnungsgemäßen Betriebs).

Die Protokolldaten müssen die Identität der zugreifenden Instanz sowie systemtechnische Daten (z. B. IP-Adresse und Port etc.) beinhalten.

Die Protokolldaten müssen für mindestens 6 Monate, auf einen begründenden Wunsch des KBA (z. B. im Falle der Untersuchung eines Vorfalls) auch länger, aufbewahrt werden.

7.2.4 Anforderungen an die Schnittstelle D

Die Anforderungen an die Schnittstelle D sind in [IznAaKBAfB] beschrieben. Die Eigenschaften der Schnittstelle D sind im Kapitel 5.5.4 zu finden.

Bezogen auf die im Rahmen von i-Kfz definierte zusätzliche Kommunikation über das Postfach ergeben sich weitere Anforderungen an die Schnittstelle D.

A-6.2.4-1	Die Kommunikation zwischen Zulassungsbehörden und dem KBA darf nur über definierte Verbindungen stattfinden.	muss

Die Kommunikation zwischen den Zulassungsbehörden und dem KBA darf nur über die Schnittstelle D erfolgen.

Es müssen die für die Schnittstelle D in diesem Dokument definierten Sicherheitsanforderungen befolgt werden.

A-6.2.4-2	Zugriff auf das Postfach an der Schnittstelle D muss authentifiziert werden.	muss

Es darf nur ein authentifizierter Zugriff auf das Postfach durch die Zulassungsbehörden (OpenFT) möglich sein.

Die notwendigen Zugangsdaten werden der Behörde im Rahmen des Zulassungsprozesses durch das KBA mitgeteilt.

Es gelten die Empfehlungen aus [BSI-TR02102-1] bezüglich der Authentisierung.

7.2.5 Anforderungen an die Schnittstelle E

Interne Schnittstelle des KBA.

7.2.6 Anforderungen an die Schnittstelle F

Die Schnittstelle F wurde im Kapitel 5.5.6 beschrieben.

A-6.2.6-1	Die Benutzung der Schnittstelle F	muss

Die Schnittstelle F muss von einer Komponente aus dem Bereich „Dezentrales-Portal-DMZ“ zur Verfügung gestellt werden und darf nur von Komponenten aus dem gleichen Bereich angesprochen werden.

A-6.2.6-2	Die Integration der Schnittstelle F	kann

Die Schnittstelle F kann durch die Komponente „dezentrales Portal“ als eine interne Schnittstelle realisiert werden.

In diesem Fall muss (z. B. durch den Einsatz von geeigneten Paketfiltern) gewährleistet werden, dass nur ausgewählte Komponenten auf die Schnittstelle F zugreifen dürfen.

A-6.2.6-3	Die Nachvollziehbarkeit muss gewährleistet werden.	muss

Die Zugriffe auf die Schnittstelle F müssen protokolliert werden.

Die Protokolldaten müssen die Identität der zugreifenden Instanz sowie systemtechnische Daten (z. B. IP-Adresse und Port etc.) beinhalten.

Die Protokolldaten müssen für mindestens 6 Monate, auf einen begründenden Wunsch des KBA (z. B. im Falle der Untersuchung eines Vorfalls) auch länger, aufbewahrt werden.

Insbesondere sind die Vorgaben und Empfehlungen des BSI zur Erstellung und Verwaltung der sicheren Protokolldaten in den Dokumenten der ISI-Reihe (vergleiche Anforderung A-6.2.3-3) einzuhalten.

7.2.7 Anforderungen an die Schnittstelle G

Die Schnittstelle G ist im Kapitel 5.5.7 vorgestellt.

A-6.2.7-1	Die Kommunikationspartner müssen gegenseitig authentifiziert werden.	muss

Die beiden Seiten der Kommunikation müssen sich gegenseitig authentifizieren.

Es ist nur Kommunikation mit einem authentifizierten Portal/Großkunden zulässig.

A-6.2.7-2	Die Integrität der Inhaltsdaten muss geschützt werden.	muss

Die Inhalte der Nachrichten müssen mit Hilfe einer digitalen Signatur bzw. einer MAC gegen Manipulation geschützt werden.

Es gelten die in [BSI-TR02102-1] enthaltenen Eingaben zu Algorithmen und Schlüssellängen.

A-6.2.7-3	Die Vertraulichkeit der Inhaltsdaten muss geschützt werden.	muss

Die Vertraulichkeit der Inhaltsdaten muss sichergestellt werden, indem die Daten für die Übertragung verschlüsselt werden.

Die Benutzung der Transport-Verschlüsselung bis zum Portal ist an der Stelle ausreichend. Die Daten müssen über eine authentifizierte HTTPS-Verbindung verschickt werden.

Es gelten die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik bezüglich der Verwendung von TLS gemäß [BSI-TR02102-2] und [BSI-MS-TLS] sowie ferner gemäß [BSI-TR02102-1] für die Authentifizierung.

A-6.2.7-4	Die Nachvollziehbarkeit muss gewährleistet werden.	muss

Die Zugriffe auf die Schnittstelle G müssen protokolliert werden.

Die Protokolldaten müssen die Identität der zugreifenden Instanz sowie systemtechnische Daten (z. B. IP-Adresse und Port etc.) beinhalten.

Die Protokolldaten müssen für mindestens 6 Monate, auf einen begründenden Wunsch des KBA (z. B. im Falle der Untersuchung eines Vorfalls) auch länger, aufbewahrt werden.

Insbesondere sind die Vorgaben und Empfehlungen des BSI zur Erstellung und Verwaltung der sicheren Protokolldaten in den Dokumenten der ISI-Reihe (vergleiche Anforderung A-6.2.3-3) einzuhalten.

A-6.2.7-5	Absicherung des Kommunikationsclients des Nutzers.	muss

Der mit dem Portal über die Schnittstelle G kommunizierende Client muss gemäß der BSI-Vorgaben abgesichert werden.

Es gelten insbesondere die Vorgaben, die im Rahmen von [BSI-ISI-CLT] bzw. [BSI-ISI-WEB-CLT] formuliert sind.

Im Falle einer Server-zu-Server-Kommunikation muss der Server des Nutzers gemäß der von BSI herausgegebenen Vorgaben in [BSI-ISI-SVR] abgesichert werden.

Der Nutzer muss die an das Portal gerichteten Anforderungen A-6.2.7-1, A-6.2.7-2 und A-6.2.7-3 als Kommunikationspartner entsprechend erfüllen.

7.2.8 Anforderungen an die Schnittstelle H

Die Ausgestaltung der Schnittstelle H ist dem Kapitel 5.5.8 zu entnehmen.

A-6.2.8-1	Implementierung des elektronischen Identitätsnachweises.	muss

Die Identität ist durch die Online-Ausweisfunktion (nPA/eAT) oder vergleichbar sicher nachzuweisen.

Um Missbrauch auszuschließen muss der Antragsteller sicher identifiziert werden. Dies kann anhand des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes oder anhand geeigneter technischer Verfahren mit gleichwertiger Sicherheit geschehen. Als solche Verfahren kommen insbesondere eine Identifizierung des Antragstellers mittels De-Mail oder eine Identifizierung über sogenannte E-Payment-Systeme in Betracht (vergleiche § 14 Absatz 2 FZV).

Die Funktion des elektronischen Identitätsnachweises mit Hilfe der Online-Ausweisfunktion muss an der Schnittstelle H durch die Komponente „dezentrales Portal“ unterstützt werden.

A-6.2.8-2	Die Authentizität der Daten.	muss

Im Rahmen der Integrität muss insbesondere die Authentizität der Daten sichergestellt werden.

Die Benutzung von einem sicheren Transportkanal (TLS) zusammen mit der Durchführung des elektronischen Identitätsnachweises sichert die Bestätigung der Identität der beiden Instanzen: Antragsteller Bürger (Personalausweis/eAT und dazugehörige PIN) und Portal (Vorlage des Berechtigungszertifikates) (vergleiche [BSI-TR-03107-1], BSI-TR-02102 zu sicheren Kryptoverfahren).

A-6.2.8-3	Die Vertraulichkeit der Daten.	muss

Die Daten müssen zwischen dem Browser des Antragstellers und dem Web-Server des Portals stets verschlüsselt übertragen werden.

Im Rahmen des durchgeführten elektronischen Identitätsnachweises mit Hilfe der Online-Ausweisfunktion (nPA/eAT) wird eine TLS-geschützte Verbindung zwischen dem Web-Browser und dem Web-Server aufgebaut (vergleiche [BSI-TR.03107-1] und [BSI-TR-03124-1]). Diese Verbindung muss für die Übertragung der Antragsdaten benutzt werden.

A-6.2.8-4	Die Nachvollziehbarkeit muss gewährleistet werden.	muss

Die Zugriffe auf die Schnittstelle H müssen protokolliert werden.

Die Protokolldaten müssen die Identität der zugreifenden Instanz sowie systemtechnische Daten beinhalten.

Die Protokolldaten müssen für mindestens 6 Monate, auf einen begründenden Wunsch des KBA (z. B. im Falle der Untersuchung eines Vorfalls) auch länger, aufbewahrt werden.

Insbesondere sind die Vorgaben und Empfehlungen des BSI zur Erstellung und Verwaltung der sicheren Protokolldaten in den Dokumenten der ISI-Reihe (vergleiche Anforderung A-6.2.3-3) einzuhalten.

Weiterhin müssen insbesondere für die Protokollierung des stattgefundenen elektronischen Identitätsnachweises mit Hilfe der Online-Ausweisfunktion die Vorgaben und Empfehlungen des BSI gemäß [BSI-TR03107-2] befolgt werden.

7.2.9 Anforderungen an die Schnittstelle X

Die Ausgestaltung der Schnittstelle X ist nicht im Fokus dieses Dokumentes, da diese Schnittstelle im Rahmen des i-Kfz-Projektes nicht direkt benutzt wird (vergleiche Grobkonzept2).

Hinweis:

Es wird empfohlen die Schnittstelle gemäß den geltenden Sicherheitsanforderungen für einen Zugriff aus dem Internet abzusichern (vergleiche [BSI-ISI]).

7.2.10 Anforderungen an die Schnittstelle Y

Im Zuge der Umsetzung der ersten Stufe des i-Kfz-Projektes ist keine Kommunikation an der Schnittstelle Y vorgesehen. Aus diesem Grund ergibt sich keine Notwendigkeit den Schutzbedarf der Schnittstelle zu ermitteln. Basierend auf der Gesamtarchitektur des Systems ergeben sich aber weitere Anforderungen, die im Folgenden beschrieben werden.

A-6.2.10-1[11]	Verwendung der Schnittstelle Y	muss

Die Schnittstelle Y muss von einer Komponente aus dem Bereich „Zulassungsbehörde-Internet-DMZ“ angeboten werden und darf nur von einer Komponente aus dem Bereich „Zulassungsbehörde-Kern-Netz“ verwendet werden.

Eine Komponente aus dem Bereich „Zulassungsbehörde-Kern-Netz“ muss dabei die Kommunikation initiierende Instanz sein.

[11] Optional für die 1. Stufe, ab der 2. Stufe des i-Kfz-Projektes verpflichtend.

8 Zulassungsverfahren für die Anbindung an die KBA-Infrastruktur

Die Kommunikation mit der KBA-Infrastruktur ist nur den zugelassenen Kommunikationspartnern gestattet. Über die Zulassung eines Kommunikationspartners entscheidet ausschließlich das KBA, die entsprechenden Zulassungsformalitäten als Kommunikationspartner werden in diesem Kapitel beschrieben. Die Prüfung einer Zulassung muss stets von einem Kommunikationspartner (hier die Zulassungsbehörde) beantragt werden. Bereits erteilte Kommunikationszulassungen sind in regelmäßigen Abständen zu erneuern.

Im Folgenden wird zunächst ein Überblick über den Lebenszyklus einer Zulassung gegeben, gefolgt von der Beschreibung der einzelnen Zustände und der möglichen Übergänge zwischen den Zuständen. Nachfolgend werden die Eigenschaften der durchzuführenden Audits und Penetrationstests, die Besonderheiten der Beantragung/Kündigung einer Zulassung sowie des angewandten Mahnverfahrens skizziert.

8.1 Lebenszyklus einer Zulassung

Ein Lebenszyklus einer Zulassung zur Kommunikation mit der KBA-Infrastruktur im Rahmen des i-Kfz-Projektes (im weiteren Verlauf auch nur Zulassung genannt) wird in der Abbildung 15 dargestellt.

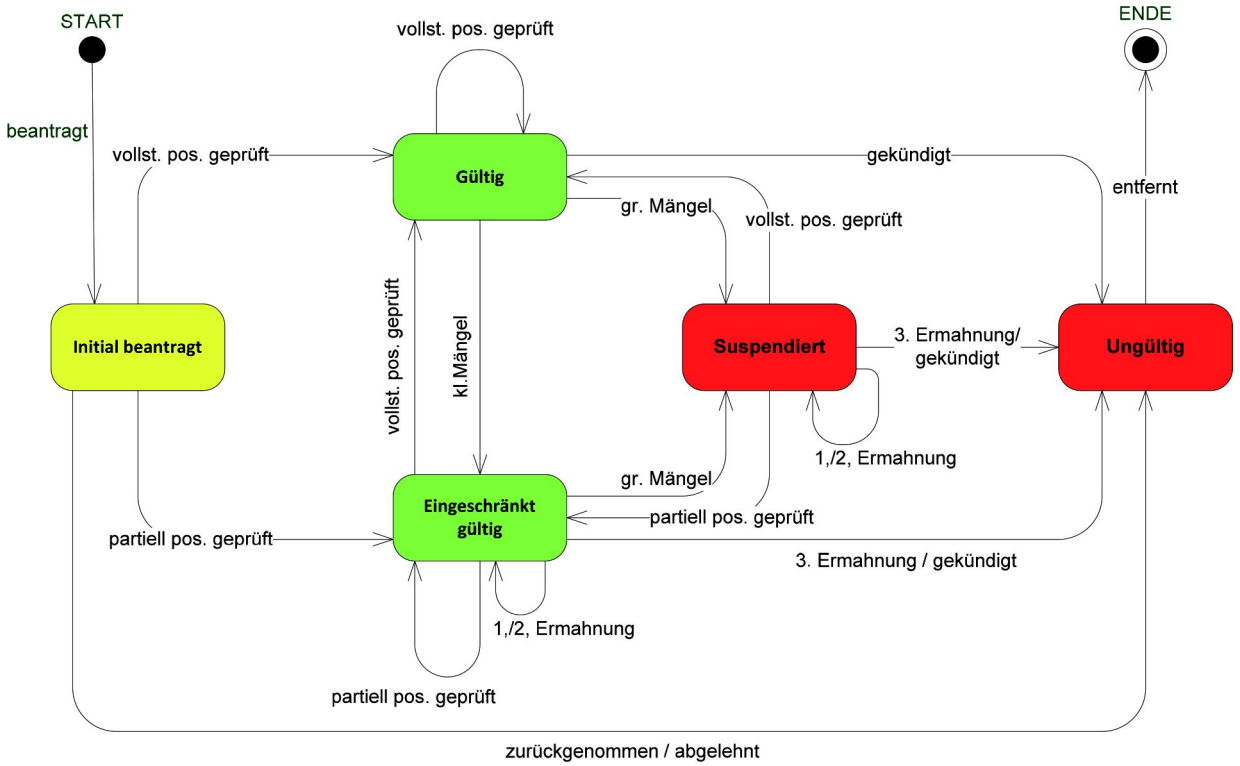

Abbildung 15: Der Lebenszyklus einer Zulassung

Außer den Pseudozuständen „START“ und „ENDE“ sind fünf weitere Zustände einer Zulassung möglich:

– „initial beantragt“ – die Zulassung wurde beantragt, befindet sich in der Prüfung, ist noch nicht gültig,

– „gültig“ – die Zulassung ist gültig, die Kommunikation mit der KBA-Infrastruktur kann erfolgen,

– „eingeschränkt gültig“ – die Zulassung wurde mit Auflagen versehen, die fristgerecht erfüllt werden müssen, die Kommunikation mit der KBA-Infrastruktur kann (befristet) erfolgen,

– „suspendiert“ – die Zulassung ist suspendiert worden, die Auflagen müssen fristgerecht erfüllt werden, die Kommunikation mit der KBA-Infrastruktur wurde unterbrochen,

– „ungültig“ – die Zulassung wurde terminiert, die Kommunikation mit der KBA-Infrastruktur findet nicht statt, die Zugangsdaten der Behörde wurden endgültig gesperrt, um die Kommunikation wiederaufnehmen zu können muss erneut eine Zulassung beantragt werden.

Nachstehend werden die einzelnen Zustände einer Zulassung mit den dazugehörigen Übergängen beschrieben. Jeder Übergang ist durch folgenden fünf Attribute charakterisiert:

– „Art“ – es werden drei unterschiedliche Arten der Zustandsübergänge (Aktivitäten) definiert. Ein Übergang bezieht sich stets auf einen Zustand und kann gegenüber diesem Zustand eine der genannten Arten zugewiesen bekommen:

  – „in“ – ein eingehender Übergang, bedeutet mit Hilfe von diesem Übergang wird der betrachtende Zustand erreicht (z. B. „gültig“ – [kleine Mängel] → „gültig“),

  – „out“ – ein ausgehender Übergang, bedeutet mit Hilfe von diesem Übergang kann der betrachtende Zustand verlassen werden (z. B. „eingeschränkt gültig“ – [vollständig positiv geprüft] → „gültig“),

  – „in/out“ – ein ein- und ausgehender Übergang, bedeutet mit Hilfe von diesem Übergang kann der betrachtende Zustand verlassen aber gleichzeitig auch wieder betreten werden (z. B. „eingeschränkt gültig“ – [1. Ermahnung] → „eingeschränkt gültig“).

– „Name“ – der Name eines Übergangs (z. B. „1. Ermahnung“),

– „Start“ – Anfangszustand einer Übergangs,

– „Ziel“ – Zielzustand eines Übergangs,

– „Beschreibung“ – eine textuelle Beschreibung des Übergangs.

8.1.1 Eine „initial beantragte“ Zulassung

In dem Zustand „initial beantragt“ befindet sich eine Zulassung wenn sie neu beantragt wurde. Dieses trifft auf folgende Fälle zu:

– Die Zulassung wird erstmalig beantragt,

– oder die Zulassung wurde bereits beantragt und erteilt, hat aber ihre Gültigkeit im Rahmen des Zulassungsprozesses verloren und muss daher erneut beantragt werden.

Um eine Zulassung zu beantragen müssen generell die Bedingungen einer „gültigen“ Zulassung erfüllt werden (vergleiche Kapitel 8.1.2).

Eine Zulassung befindet sich in dem Zustand „initial beantragt“, wenn der Beantragungsprozess erfolgreich abgeschlossen wurde (vergleiche Kapitel 8.5).

Eine „initial beantragte“ Zulassung ermächtigt noch nicht zur Kommunikation mit der KBA-Infrastruktur.

Die Aktivitäten (Übergänge) die eine Zulassung in den Zustand „initial beantragt“ überführen, oder auf eine Zulassung im Zustand „initial beantragt“ anwendbar sind, werden in der Tabelle 4 aufgelistet:

Übergänge				
Art	Name	Start	Ziel	Beschreibung
in	„beantragt“	„START“	„initial beantragt“	Die Zulassung wurde beantragt und im nächsten Schritt findet die Prüfung der vorgelegten Beantragungsunterlagen seitens des KBA statt.
out	„vollst. positiv geprüft“	„initial beantragt“	„gültig“	Die Prüfung der Unterlagen im Rahmen der Beantragung ist vollständig positiv abgeschlossen worden. Eine uneingeschränkt gültige Zulassung wurde erteilt.
	„partiell positiv geprüft“		„eingeschränkt gültig“	Die Prüfung der bei der Beantragung vorgelegten Unterlagen konnte nicht vollständig positiv abgeschlossen werden. Es ergaben sich einige wenige Unstimmigkeiten (kleine Mängel). Es wurde eine eingeschränkt gültige Zulassung mit Auflagen, die zeitnah erfüllt werden müssen, erteilt.
	„zurückgenommen/ abgelehnt“		„ungültig“	Der Antrag wurde seitens des Antragstellers zurückgenommen oder durch das KBA abgelehnt. Es wurde keine Zulassung erteilt.

Tabelle 4: Zulassungsverfahren – Übergänge des Zustands „initial beantragt“

8.1.2 Eine „gültige“ Zulassung

Eine Zulassung ist uneingeschränkt „gültig“ (auch nur „gültig“ genannt), wenn folgende Eigenschaften gelten:

1. Der Beantragungsprozess wurde erfolgreich abgeschlossen (vergleiche Kapitel 8.5).

2. Die in diesem Dokument definierten Mindestanforderungen (vergleiche Kapitel 7) sind vollständig erfüllt (die Einhaltung/Erfüllung konnte vollständig positiv geprüft werden).

3. Die Erfüllung der Mindestanforderungen wurde im Rahmen eines Audits (vergleiche Kapitel 8.2) durch einen unabhängigen Dritten (im weiteren Verlauf Auditor genannt) überprüft und bestätigt.

4. Es sind mehr als zwei Monate bis zur Fälligkeit eines Re-Audits (Hinweis: Sobald es weniger als zwei Monate bis zur Vorlage der Ergebnisse des Re-Audits sind, ist die Zulassung automatisch „eingeschränkt gültig“).

Eine gültige Zulassung ermächtigt zur Kommunikation mit der KBA-Infrastruktur.

In der Tabelle 5 werden die möglichen Aktivitäten (Übergänge) und der damit verbundenen Änderungen des Status einer Zulassung, bezogen auf eine „gültige“ Zulassung, dargestellt:

Übergänge				
Art	Name	Start	Ziel	Beschreibung
in	„vollständig positiv geprüft“	„initial beantragt“	„gültig“	Die Unterlagen einer „initial beantragten“ Zulassung konnten vollständig positiv geprüft werden, somit ergibt sich eine uneingeschränkt „gültige“ Zulassung.
		„eingeschränkt gültig“		Die im Rahmen des Zulassungsprozesses gestellten Auflagen wurden vollständig erfüllt (die festgestellten kleinen Mängel wurden beseitigt), somit ist die Zulassung uneingeschränkt „gültig“.
		„suspendiert“		Die festgestellten großen Mängel (z. B. ein schwerwiegender Informationssicherheitsvorfall) wurden vollständig behoben, die Prüfung der Unterlagen der Zulassung konnte vollständig positiv durchgeführt werden, die Zulassung wird uneingeschränkt „gültig“.
in-out		„gültig“		Ein besonderer Fall, z. B. erneute rechtzeitige Vorlage aktualisierter Zulassungsdokumente.
out	„kleine Mängel“		„eingeschränkt gültig“	Kleine Mängel (z. B. die Ergebnisse der erneuten positiven Durchführung der Penetrationstests sind nicht fristgemäß vorgelegt worden) wurden festgestellt. Es werden an die Zulassung Auflagen geknüpft, die Mängel sind in einer festgelegten Frist zu beseitigen und entsprechend zu dokumentieren. Die Zulassung wird somit „eingeschränkt gültig“.
	„große Mängel“		„suspendiert“	Mindestens ein großer Mangel wurde festgestellt. Die Zulassung wurde „suspendiert“, eine Auflage wurde generiert und die Kommunikation mit der KBA-Infrastruktur ist nicht mehr möglich. Der Mangel muss schnellstmöglich beseitigt und dokumentiert werden.
	„gekündigt“		„ungültig“	Die Zulassung wurde seitens des Kommunikationspartners gekündigt.

Tabelle 5: Zulassungsverfahren – Übergänge des Zustands „gültig“

8.1.3 Eine „eingeschränkt gültige“ Zulassung

Eine „gültige“ Zulassung, die kleine Mängel aufweist gilt als „eingeschränkt gültig“.

Folgende Eigenschaften definieren einen kleinen Mangel:

- Ein Nachweis der Wiederholung der Penetrationstests steht aus (überfällig),
- Ein Nachweis der Wiederholung des Audits steht aus (überfällig),
- Ein Nachweis der Wiederholung des Audits muss spätestens in zwei Monaten vorgelegt werden (die Zulassung steht kurz vor dem Ablauf).

Eine eingeschränkte Zulassung wird normalerweise durch eine oder mehrere Auflagen begleitet, die innerhalb einer vorgegebenen Frist erfüllt werden müssen und deren Erfüllung nachgewiesen werden muss.

Ein wiederholtes Nichtbeachten der angesetzten Erfüllungs- und Nachweisfristen kann zur Ungültigkeit der Zulassung führen (vergleiche Kapitel 8.7).

Eine eingeschränkte Zulassung ermächtigt zur Kommunikation mit der KBA-Infrastruktur.

In der Tabelle 6 werden, bezogen auf eine „eingeschränkt gültige“ Zulassung, die Aktivitäten (Übergänge) und der damit verbundenen Änderungen des Status einer Zulassung gezeigt:

Übergänge				
Art	Name	Start	Ziel	Beschreibung
in	„kleine Mängel“	„gültig“	„eingeschränkt gültig“	Bei einer „gültigen“ Zulassung wurden kleine Mängel festgestellt (z. B. der ausstehende Nachweis der durchgeführten Penetrationstests wurde nicht rechtzeitig vorgelegt). Die Zulassung wechselt den Zustand in „eingeschränkt gültig“. Es werden bestimmte Auflagen definiert, die in vorgegebener Zeit erfüllt werden müssen.
	„partiell positiv geprüft“	„suspendiert“		Eine suspendierte bzw. erneut beantragte Zulassung konnte partiell positiv geprüft werden. Bei der Prüfung wurden kleine Mängel festgestellt und in Form von Auflagen beanstandet. Die Auflagen müssen in einem festgelegten Zeitfenster erfüllt werden.
		„initial beantragt“		
in/out		„eingeschränkt gültig“		Eine erneute Prüfung hatte weiterhin kleine Mängel nachgewiesen. Die Zulassung bleibt „eingeschränkt gültig“, die Mängel müssen innerhalb der vorgegebenen Frist beseitigt werden.
	„1./2. Ermahnung“			Die vollständige Erfüllung der Auflagen ist nicht rechtzeitig erfolgt. Nachfolgend wird die erste oder bereits die zweite Ermahnung ausgesprochen. Die Auflagen müssen in vorgegebener Zeit erfüllt werden. Die Zulassung bleibt „eingeschränkt gültig“.
out	„vollständig positiv geprüft“		„gültig“	Die vorhandenen kleinen Mängel wurden beseitigt, die erneute Prüfung wurde positiv abgeschlossen, die Zulassung ist „gültig“.
	„große Mängel“		„suspendiert“	Große Mängel wurden festgestellt (z. B. schwerwiegender Informationssicherheitsvorfall). Die Zulassung wurde suspendiert. Die Mängel müssen in vorgegebener Zeit beseitigt werden. Es findet keine Kommunikation mit der KBA-Infrastruktur statt.
	„3. Ermahnung/ gekündigt“		„ungültig“	Die Zulassung wurde vom Kommunikationspartner gekündigt, oder aufgrund nicht erfüllter Auflagen eine dritte Ermahnung seitens des KBA ausgesprochen. Die Zulassung ist „ungültig“. Die Kommunikation mit der KBA-Infrastruktur wird beendet. Um die Kommunikation wiederaufzunehmen muss eine Zulassung erneut beantragt werden.

Tabelle 6: Zulassungsverfahren – Übergänge des Zustands „eingeschränkt gültig“

8.1.4 Eine „suspendierte“ Zulassung

Eine Zulassung kann aufgrund der festgestellten großen Mängel suspendiert werden. Zu der Gruppe der großen Mängel gehören u. a.:

- Ein schwerwiegender Informationssicherheitsvorfall wurde beim Kommunikationspartner festgestellt (z. B. Teile des Portals wurden kompromittiert).
- Festgestellter Verstoß gegen die in diesem Dokument definierten Mindestsicherheitsanforderungen.

Eine suspendierte Zulassung wird normallerweise von zeitlich befristeten Auflagen begleitet, die vom Kommunikationspartner erfüllt werden müssen und deren Erfüllung dem KBA rechtzeitig (vor dem Ablauf der Auflagefrist) angezeigt werden müssen.

Eine wiederholte Nichtbeachtung der angesetzten Erfüllung- und Nachweisfristen kann zur Ungültigkeit der Zulassung führen (vergleiche Kapitel 8.7).

Eine suspendierte Zulassung ermächtigt nicht zur Kommunikation mit der KBA-Infrastruktur (die Zugangsdaten werden seitens KBA gesperrt).

In der Tabelle 7 werden die Aktivitäten (Übergänge) und daraus resultierende neue Zustände der Zulassung, bezogen auf eine „suspendierte“ Zulassung, dargestellt:

Übergänge				
Art	Name	Start	Ziel	Beschreibung
in	„große Mängel“	„gültig“	„suspendiert“	Es wurde zumindest einen großer Mangel festgestellt (z. B. ein schwerwiegender Informationssicherheitsvorfall). Es werden bestimmte Auflagen auferlegt, die in einer Frist vom Kommunikationspartner erfüllt werden müssen.
		„eingeschränkt gültig“		
in/out	„1./2. Ermahnung“	„suspendiert“		Die Erfüllung der Auflagen wurde zum ersten oder zum zweiten Mal angemahnt. Die Zulassung bleibt „suspendiert“.
out	„partiell positiv geprüft“		„eingeschränkt gültig“	Die Prüfung einer „suspendierten“ Zulassung konnte partiell positiv durchgeführt werden. Es wurden kleine Mängel festgestellt, die in einer vorgegebenen Frist beseitigt werden müssen. Die Zulassung wird als „eingeschränkt gültig“ klassifiziert und die Kommunikation mit der KBA-Infrastruktur wird freigeschaltet.
	„vollständig positiv geprüft“		„gültig“	Die Prüfung einer „suspendierten“ Zulassung konnte vollständig positiv erfolgen. Somit ist die Zulassung uneingeschränkt „gültig“. Die Kommunikation mit der KBA-Infrastruktur wurde wieder aufgenommen.
	„3. Ermahnung/ gekündigt“		„ungültig“	Die Zulassung wurde vom Kommunikationspartner gekündigt, oder aufgrund der Nichterfüllung von Auflagen wurde eine dritte und endgültige Mahnung seitens des KBA ausgesprochen. Die Zulassung ist „ungültig“. Um die Kommunikation mit KBA wieder aufzunehmen muss erneut eine Zulassung beantragt werden.

Tabelle 7: Zulassungsverfahren – Übergänge des Zustands „suspendiert“

8.1.5 Eine „ungültige“ Zulassung

Eine ungültige Zulassung kann nicht in einen anderen Statuswert geändert werden. Um zur Kommunikation mit der KBA-Infrastruktur erneut zugelassen zu werden, muss der Kommunikationspartner die entsprechende Zulassung erneut beantragen.

Eine ungültige Zulassung ermächtigt nicht zur Kommunikation mit der KBA-Infrastruktur.

Übergänge				
Art	Name	Start	Ziel	Beschreibung
in	„zurückgenommen/ abgelehnt“	„initial beantragt“	„ungültig“	Der Antragsteller nimmt den Antrag zurück, oder der Antrag wurde abgelehnt.
	„gekündigt“	„gültig“		Die Zulassung wurde seitens des Antragstellers gekündigt.
	„3. Ermahnung/ gekündigt“	„eingeschränkt gültig“		Die Erfüllung einer Auflage wurde zum dritten Mal angemahnt. Die Zulassung verliert die Gültigkeit, oder die Zulassung wurde seitens des Antragstellers gekündigt.
		„suspendiert“		
out	„entfernt“	„ungültig“	„ENDE“	Die Zulassungsdaten wurden endgültig entfernt.

Tabelle 8: Zulassungsverfahren – Übergänge des Zustands „ungültig“

8.2 Audit

Die Erfüllung der in diesem Dokument definierten Mindestsicherheitsanforderungen muss im Rahmen eines Audits durch einen unabhängigen Dritten überprüft und bestätigt werden (vergleiche hierzu [BSI-ITG-ZERT]).

Die Überprüfung (Audit) ist alle drei Jahre zu wiederholen. Die Ergebnisse sind dem KBA vorzulegen.

Der Umfang des durchzuführenden Audits besteht aus einer Überprüfung der Anforderungen, die im Kapitel 7 definiert sind.

Im Falle einer bestehenden IT-Grundschutz-Zertifizierung sind im Audit nur die i-Kfz-spezifischen Anforderungen zu prüfen, welche über die IT-Grundschutzprüfung hinausgehen.

8.3 Prüfung der zusätzlichen Anforderungen[12]

Dieses Dokument spezifiziert einige Anforderungen, die über den Rahmen der IT-Grundschutz-Stufe hinausreichen. Insbesondere diese Anforderungen müssen im Zuge des Audits überprüft werden. Zu diesen Anforderungen gehören:

- Die erfolgreiche Durchführung der vorgeschriebenen Härtungsmaßnahmen der ausgewählten Komponenten (vergleiche Anforderung A-6.1-2) ist zu überprüfen. Der erfolgreiche Abschluss der im Kapitel 8.4 beschriebenen Penetrationstests muss geprüft und dokumentiert werden.
- Die Erfüllung der Anforderung A-6.1-2 muss überprüft und das Ergebnis dokumentiert werden.
- Die netztechnische Abschottung der Portal-Anwendung (vergleiche Anforderung A-6.1-6) muss überprüft und das Ergebnis dokumentiert werden.
- Die Anforderung A-6.1-9, insbesondere die 1-zu-1-Kommunikation (direkte Weiterleitung der Nachrichten), muss überprüft und das Ergebnis dokumentiert werden.

8.4 Penetrationstests[12]

Im Zuge der Maßnahmen zur Härtung der kritischen Anwendungen müssen an den Komponenten (vergleiche hierzu die Anforderung A-6.1-2 in Kapitel 7.1)

- „dezentrales Portal“
- und „Systeme der Fachverfahren“

sogenannte Penetrationstests durchgeführt werden. Der positive Ausgang der Penetrationstests muss dem KBA mitgeteilt werden. Im Falle des negativen Ausgangs der Penetrationstests müssen die aufgezeigten Mängel unverzüglich beseitigt werden sowie deren Beseitigung muss durch eine erfolgreiche Nachprüfung gegenüber dem KBA nachgewiesen werden.

[12] Optional für die 1. Stufe, verpflichtend ab der 2. Stufe des i-Kfz-Projektes.

Die Penetrationstests sind jährlich erfolgreich zu wiederholen und das Ergebnis ist im Rahmen des Zulassungsverfahrens dem KBA mitzuteilen.

In bestimmten Fällen kann eine außerordentliche Durchführung von Penetrationstests notwendig sein. Zu diesen Fällen gehören:

- Feststellung eines scherwiegenden Informationssicherheitsvorfalls und Beseitigung dessen Ursachen – abhängig von den Gegebenheiten, sind im Nachgang die Penetrationstests vollständig, oder punktuell abgestimmt auf die relevanten Bereiche durchzuführen und der positive Ausgang ist dem KBA mitzuteilen.
- Einsatz einer neuen Hauptversion der Anwendung – es handelt sich hier generell nicht um einen Minor-Update bzw. Sicherheitspatch, sondern um ein Major-Release der Software (z. B. von der Version 2.0 auf die Version 3.0).
- Durchführung der Änderungen an den kritischen Schnittstellen, insbesondere an den Außenschnittstellen (hier auch im Falle von kleinen Updates und Sicherheitspatches). Begründet können die Penetrationstests partiell innerhalb des betroffenen Bereiches durchgeführt werden.
- Durchführung von Änderungen an anderen involvierten und sicherheitskritischen Infrastrukturkomponenten – z. B. ein Switch oder ein Paketfilter werden ausgetauscht oder einem Update/Sicherheitspatch unterzogen.

Sollte eine partielle Durchführung des Penetrationstests stattgefunden haben, dann gilt für die nächste vollständige Durchführung die Periode gemessen vom Datum der Durchführung des letzten vollständigen Penetrationstests.

8.5 Beantragung einer Zulassung

Nur zugelassene Kommunikationspartner dürfen im Rahmen des i-Kfz-Projektes mit der KBA-Infrastruktur kommunizieren. Die für die Kommunikation notwendige Zulassung muss von jedem Kommunikationspartner beantragt werden. Der Antragsteller ist dabei stets die korrespondierende Zulassungsbehörde[13].

[13] Im Falle, dass die Zulassungsbehörde nicht selbstständig das Portal betreibt, sind die im Rahmen dieses Dokumentes geforderten Aktivitäten (z. B. Penetrationstest, Audit) durch die Zulassungsbehörde zu koordinieren.

Für das Jahr 2015 und im Rahmen der Stufe 1 (Außerbetriebsetzung) des i-Kfz-Projektes gelten folgende Sonderregelungen:

- Zur initialen Beantragung einer Zulassung muss das Ergebnis des Audits bereits vorliegen. Alternativ muss seitens des Antragstellers erklärt werden, dass die Sicherheitsanforderungen umgesetzt sind und die Penetrationstests sowie das Audit bereits beauftragt wurden (unter Angabe des beauftragten Unternehmens). Die Ergebnisse sind dem KBA dann bis spätestens Ende 2015 vorzulegen.
- Im Falle bereits bestehender BSI-Grundschutz-Zertifizierung, welche durch ein jährliches Wiederholungsaudit aufgefrischt wird, kann das vom KBA geforderte Audit mit dem Wiederholungsaudit bis Ende 2015 erfolgen.

Der Prozess der Beantragung wird gestartet indem der Antragsteller die Beantragungsdokumente bei der KBA-Kundenbetreuung bestellt. Im Folgenden wird der Beantragungsprozess grob skizziert.

Nr.	Initiator	Involvierte Instanz	Beschreibung
1	Antragsteller	KBA-Anwender-betreuung	Der Antragsteller (hier die Zulassungsbehörde) bestellt bei der KBA-Anwenderbetreuung einen Satz Antragsunterlagen zur Beantragung einer Zulassung zur Kommunikation mit der KBA-Infrastruktur im Rahmen des i-Kfz-Projektes. Der Antragsteller wählt entweder die Zusendung der Unterlagen per Post oder erhält die Zugangsdaten zum geschützten Bereich der KBA-Internetseite, in dem die Unterlagen heruntergeladen werden können.
2a[14]	KBA-Anwender-betreuung	Antragsteller	Ein kompletter Satz der Beantragungsunterlagen wird an die vom Antragsteller angegebene Adresse postalisch verschickt.
2b[15]	Antragsteller	KBA-Portal	Der Antragsteller lädt sich die Beantragungsunterlagen vom KBA-Portal herunter.
3	Antragsteller	Ggf. der Portal-Betreiber	Die Erfüllung der in diesem Dokument vorgelegten Mindestanforderungen wird seitens des Antragstellers und ggf. auch weiteren Akteuren (z. B. seitens des Portal-Betreibers) sichergestellt.
4	Antragsteller	Ggf. Portal-Betreiber, KBA-Technischer Support	Der Antragsteller führt selbst bzw. veranlasst die Durchführung der technischen Tests der Kommunikationsstrecke mit der KBA-Infrastruktur (insbesondere die Schnittstellen A und D sind zu testen, vergleiche Kapitel 5.5).
5[16]	Antragsteller	Penetrationstests ausführendes Unternehmen	Der Antragsteller beauftragt ein Unternehmen mit entsprechender Expertise, um die vorgeschriebenen Penetrationstests durchzuführen. Mit dem erfolgreichen Abschluss der Penetrationstests und Erstellung des Berichtes ist dieser Schritt abgeschlossen.
6[16]	Antragsteller	Auditor	Es wird durch den Antragsteller ein Auditor beauftragt, um die Überprüfung der Einhaltung der Mindestanforderungen zu bestätigen (vergleiche Kapitel 8.2).
7	Antragsteller	KBA-Anwender-betreuung	Die ausgefüllten Antragsunterlagen mit Anlagen: – Bericht zum erfolgreichen Abschluss des Penetrationstests, – Bericht zum erfolgreichen Abschluss des Audits, werden auf dem Postweg an die im Kapitel 8.8 genannte Anschrift gesendet. Die Zulassung befindet sich somit im dem Zustand „initial beantragt“ und es folgt eine Prüfung der Unterlagen durch das KBA.

Tabelle 9: Grobe Schritte des Beantragungsprozesses einer Zulassung

[14] Dieser Schritt wird dann ausgeführt, wenn die Zusendung auf dem Postweg vereinbart wurde, sonst wird der Schritt 2b ausgeführt.

[15] Dieser Schritt wird nur dann ausgeführt, wenn das Abholen (Herunterladen) der Unterlagen vom KBA-Portal vereinbart wurde, sonst wird der Schritt 2a ausgeführt.

[16] Hier gelten die im Kapitel 8.5 formulierten Sonderregelungen für das Jahr 2015.

8.6 Kündigung einer laufenden Zulassung

Eine laufende Zulassung kann jederzeit seitens des Kommunikationspartners beim KBA schriftlich gekündigt werden. Eine eingegangene Kündigung wird durch das KBA schriftlich bestätigt und beinhaltet das Datum der Deaktivierung des Zugangs.

Die für die Kündigung benötigten Unterlagen können bei der KBA-Anwenderbetreuung erfragt werden (vergleiche Kapitel 8.8).

Eine gekündigte Zulassung, deren Kündigung bestätigt wurde, kann nicht reaktiviert werden. Zur Reaktivierung ist eine erneute initiale Beantragung notwendig.

8.7 Ermahnungsverfahren, Sperrung einer Zulassung

Um ein reibungsloses Zulassungsverfahren anzubieten zu können, müssen auch die Aspekte des Umgangs mit den ggf. auftretenden Versäumnissen geregelt werden. Insbesondere im Falle einer „eingeschränkt gültigen“ bzw. „suspendierten“ Zulassung muss ein Mechanismus definiert werden, welcher die Beseitigung der auferlegten Auflagen steuert und somit eine vollständige Erfüllung der Mindestanforderungen sichert.

Jede formulierte Auflage ist mit einer Erledigungsfrist versehen. Der Kommunikationspartner ist somit verpflichtet unter der Einhaltung dieser Frist die Auflage zu erfüllen.

Sollte keine fristgerechte Erfüllung der Auflage feststellbar sein, dann ist seitens des KBA eine schriftliche Mahnung an den Kommunikationspartner zu richten und eine Ersatzfrist zu nennen. Kommt es im weiteren Verlauf zum wiederholten

Verstreichen der Frist, so ist seitens des KBA eine erneute (zweite) Mahnung zu versenden inklusive einer zweiten (finalen) Ersatzfrist. Sollte auch die finale Frist nicht eingehalten werden und die Erfüllung der auferlegten Auflage nicht feststellbar ist, so wird seitens des KBA eine dritte (und letzte) Mahnung an den Kommunikationspartner versendet.

Die betroffene Zulassung wird nach Ablauf der dritten Mahnfrist in den Zustand „ungültig“ überführt. Das KBA sperrt die während des Beantragungsprozesses dem Kommunikationspartner ausgehändigten Zugangsdaten, wodurch mit sofortiger Wirkung keine Möglichkeit des Zugriffs auf die i-Kfz-Webservices besteht.

8.8 Ansprechpartner beim KBA

Technische Informationen bezüglich der Netzanbindung und der Sicherheitsmaßnahmen erhalten Sie durch den technischen Support unter:

Technischer Support	
Telefon	(04 61) 3 16-14 00
Telefax	(04 61) 3 16-29 42
E-Mail	kba-benutzerservice@kba.de

Tabelle 10: Kontaktdaten des technischen Supports

Die weiterführenden Informationen zum Beantragungsprozess, sowie die Beantragungsunterlagen erhalten Sie über unserer Anwenderbetreuung:

Anwenderbetreuung	
Herr Erik Chilcott	Telefon: (04 61) 3 16-17 17 Telefax: (04 61) 3 16-29 42 E-Mail: Anwenderbetreuung@kba.de
Frau Nadine Fengler	
Frau Bettina Hinrichsen	
Frau Anke Raida	
Anschrift	Kraftfahrt-Bundesamt Anwenderbetreuung 24932 Flensburg

Tabelle 11: Kontaktdaten der Kundenbetreuung

9 Quellen

[BDSG] Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist

[BFDI-OHM] Orientierungshilfe Mandantenfähigkeit. Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur, Version 1.0, 11. Oktober 2012, http://www.bfdi.bund.de/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/OrientierungshilfeMandantenfaehigkeit.pdf?__blob=publicationFile

[BSI-ISI] BSI-Standards zur Internet-Sicherheit (ISi-Reihe), https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/ISi-Reihe/ISi-Reihe_node.html

[BSI-ISI-CLT] Absicherung eines PC-Clients (ISi-Client), Version 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_client_studie.pdf?__blob=publicationFile

[BSI-ISI-LANA] Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA), Version 2.0, 27. Juli 2012, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_studie_pdf.pdf?__blob=publicationFile

[BSI-ISI-SVR] Absicherung eines Servers (ISi-S), Version 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi-server_pdf.pdf?__blob=publicationFile

[BSI-ISI-WEB-CLT] Sichere Nutzung von Web-Angeboten (ISi-Web), Version 2008, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_web_client_studie_pdf.pdf?__blob=publicationFile

[BSI-ISI-WEB-SVR] Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server), Version 2008, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_web_server_studie_pdf.pdf?__blob=publicationFile

[BSI-ISI-VPN] Virtuelles Privates Netz (ISi-VPN), Version 1.0, 2009, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_vpn_leitlinie_pdf.pdf?__blob=publicationFile

[BSI-ISI-VPN-SG] Aufbau von Virtual Private Networks (VPN) und Integration in Sicherheitsgateways, Version 1.0, 2006, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/vpn_pdf.pdf?__blob=publicationFile

[BSI-ITG-100-2] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Version 2.0, 2008, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile

[BSI-ITG-ZERT] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Zertifizierungsschema, Version 1.2, 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.pdf?__blob=publicationFile

[BSI-MS-TLS] Mindeststandard des BSI nach § 8 Absatz 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung, Version 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile

[BSI-TR02102-1] BSI TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2014.01, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf.pdf?__blob=publicationFile

[BSI-TR02102-2] BSI TR-02102-2: Verwendung von Transport Layer Security (TLS), Version 2014.01, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.pdf?__blob=publicationFile

[BSI-TR02102-3] BSI TR-02102-3: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version 2014.01, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3_pdf.pdf?__blob=publicationFile

[BSI-TR03107-1] TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government, Teil 1: Vertrauensniveaus und Mechanismen, Version 1.0, 9. April 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile

[BSI-TR03107-2] TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government, Teil 2: Schriftformersatz mit elektronischem Identitätsnachweis, Version 1.0, 3. April 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-2.pdf?__blob=publicationFile

[BSI-TR03124-1] TR03124-1: eID-Client, Part 1: Specifications, Version 1.1, 2. Mai 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03124/TR-03124-1.pdf?__blob=publicationFile

[FZV] Fahrzeug-Zulassungsverordnung – FZV – vom 3. Februar 2011 (BGBl. I S. 139), die zuletzt durch Artikel 1 der Verordnung vom 30. Oktober 2014 (BGBl. I S. 1666) geändert worden ist

[FZVuGebOStÄndV] Erste Verordnung zur Änderung der Fahrzeug-Zulassungsverordnung und der Gebührenordnung für Maßnahmen im Straßenverkehr (1. FZVuGebOStÄndV), vom 8. Oktober 2013 (BGBl. I S. 3772)

[Grobkonzept] Internetbasierte Fahrzeugzulassung (i-Kfz) – Grobkonzept, Version 1.0, Stand: 27. September 2013

[Grobkonzept2] Internetbasierte Fahrzeugzulassung (i-Kfz) – Grobkonzept, Version 2.01, Stand: 16. Juli 2014

[IznAaKBAfB] Informationen zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden, Stand Mai 2014

[KBAG] Gesetz über die Errichtung eines Kraftfahrt-Bundesamts (KBAG), Ausfertigungsdatum: 4. August 1951: zuletzt geändert durch Artikel 3 des Gesetzes vom 28. August 2013 (BGBl. I S. 3313)

[StVGuaÄndG] Viertes Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze (4. StVGuaÄndG) vom 28. August 2013 (BGBl. I S. 3310)

Anlage 2

Internetbasierte Fahrzeugzulassung (i-Kfz) – Anlage Penetrationstest –

Version: 1.0
Stand: 13. November 2014

Dokumenttitel: Mindestsicherheitsanforderungen an dezentrale Portale Anlage – Penetrationstests (Anlage-Pentests)

Projektname: Internetbasierte Fahrzeugzulassung

Freigegebene Version: 1.0

Änderungsverzeichnis

Version	Datum	Geänderte Kapitel	Grund der Änderung	Name
0.1	22. Oktober 2014	alle	Ersterstellung	BPT
0.5	24. Oktober 2014	alle	Fortschreibung	BPT
0.8	28. Oktober 2014	alle	Abschluss vom ersten Entwurf	BPT
0.9	04. November 2014	alle	Einarbeitung der Kommentare aus der QS-Runde	BPT
0.9.1	10. November 2014	alle	QS	KBA
1.0	13. November 2014	alle	Vorbereitung der Veröffentlichung (Layout)	KBA

Tabelle 1: Änderungsverzeichnis

Inhaltsübersicht

1 Allgemeines

1.1 Mitgeltende Dokumente

– Internetbasierte Fahrzeugzulassung (i-Kfz) – Mindest-Sicherheitsanforderungen an dezentrale Portale, Version 1.0

1.2 Abkürzungsverzeichnis

API	Application Programming Interface
ALG	Application-Level Gateway
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BPT	Bearing Point
DDOS	Distributed DOS
DMZ	Demilitarisierte Zone
DOS	Denial of Service
E-Modul	Eindringungsversuch-Modul
HR	Human Resources
IDS	Intrusion Detection System
i-Kfz	Internetbasierte Fahrzeugzulassung
I-Modul	Informationsbeschaffung-Modul
KBA	Kraftfahrt-Bundesamt
LDAP	Lightweight Directory Access Protocol
SQL	Structured Query Language
XSS	Cross-Site-Scripting

Tabelle 2: Abkürzungsverzeichnis

1.3 Abbildungsverzeichnis

1.4 Tabellenverzeichnis

2 Ziel und Zweck des Dokuments

Dieses Dokument gilt als eine Anlage zu dem Dokument mit dem Titel „Mindest-Sicherheitsanforderungen an dezentrale Portale“ (vergleiche [KBA-MSADP]). Die in diesem Dokument zitierten Anforderungen kommen aus [KBA-MSADP].

Gemäß der Anforderung A-6.1-2 müssen die Komponenten „dezentrales Portal“ (vergleiche [KBA-MSADP], Kapitel 5.4.7) und „Systeme der Fachverfahren“[1] (vergleiche [KBA-MSADP], Kapitel 5.4.6) besonderen Härtungsmaßnahmen unterzogen werden, um die geforderte Resistenz gegenüber potentiellen Angriffen aufweisen zu können. Zu den Maßnahmen gehört insbesondere eine erfolgreiche Durchführung der in diesem Dokument definierten Penetrationstests.

[1] Optional für die 1. Stufe, verpflichtend ab der 2. Stufe des i-Kfz-Projektes.

Ein Penetrationstest besteht dabei stets aus folgenden vier Bestandteilen:

- Durchführung einer IS-Kurzrevision[2],
- Durchführung eines IS-Webchecks[3],
- Durchführung von Blackbox-Penetrationstests,
- Durchführung von Whitebox-Penetrationstests.

[2] Vergleiche https://www.bsi.bund.de/DE/Themen/weitereThemen/ISRevision/ISKurzrevision/iskurzrevision_node.html

[3] Vergleiche https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Beschreibung_Webcheck.pdf?_blob=publicationFile

Es wird empfohlen die Kurzrevision grundsätzlich vorzuziehen, die Reihenfolge der anderen Bestandteile kann variieren.

Die genaue Beschreibung der Modalitäten der Durchführung ist dem Kapitel 8.4 in [KBA-MSADP] zu entnehmen. Im Rahmen dieses Dokumentes wird lediglich die Art sowie Umfang der durchzuführenden Prüfungen dargestellt.

Im Kapitel 3 wird zunächst auf die der Definition zugrunde liegenden Methodik verwiesen sowie diese kurz skizziert. Das darauf folgende Kapitel 4 definiert die mit Hilfe der vorgestellten Methodik beschriebenen Penetrationstests, die zwingend durchgeführt werden müssen.

Hinweis:

Das vorliegende, nicht vollständige Dokument beschreibt die verbindlich zu erfüllenden Anforderungen an die Penetrationstests gem. [KBA-MSADP].

Es handelt sich um eine erste Version, welche nach Vorliegen der Erkenntnisse aus einem noch durchzuführenden Pilot-Penetrationstest unter Leitung des BSI bei Dataport AöR, Hamburg fortgeschrieben wird.

3 Übersicht über die der Definition zugrunde liegende Methodik

Der Inhalt dieses Kapitels basiert auf den Ausführungen zu Penetrationstests in [BSI-PENTESTS].

Von Grundsatz her kann die Vorgehensweise bei der Durchführung der Penetrationstests in folgende Teilschritte unterteilt werden (vergleiche [BSI-PENTESTS], Kapitel 2.4):

- Recherche nach Informationen über das Zielsystem,
- Scan der Zielsysteme auf angebotene Dienste,
- System und Anwendungserkennung,
- Recherche nach Schwachstellen,
- Ausnutzen der Schwachstellen.

3.1 Einordnung und Zielsetzung

Ein wichtiger Aspekt, der für eine erfolgreiche Durchführung aus der Sicht des Auftraggebers unabdingbar ist, ist eine klare Zielvereinbarung für die Tests. In [BSI-PENTESTS], Kapitel 3.2, werden vier gängige Gruppen der Ziele vorgestellt.

Um eine Möglichkeit einer allgemeinverständlichen Beschreibung der Penetrationstests zu schaffen, definiert [BSI-PENTESTS] im Kapitel 3.4 eine Klassifikation, die unter Verwendung von sechs Kriterien (Informationsbasis, Aggressivität, Umfang, Vorgehensweise, Technik und Ausgangspunkt) die Penetrationstests geeignet charakterisieren kann (vergleiche Abbildung 1).

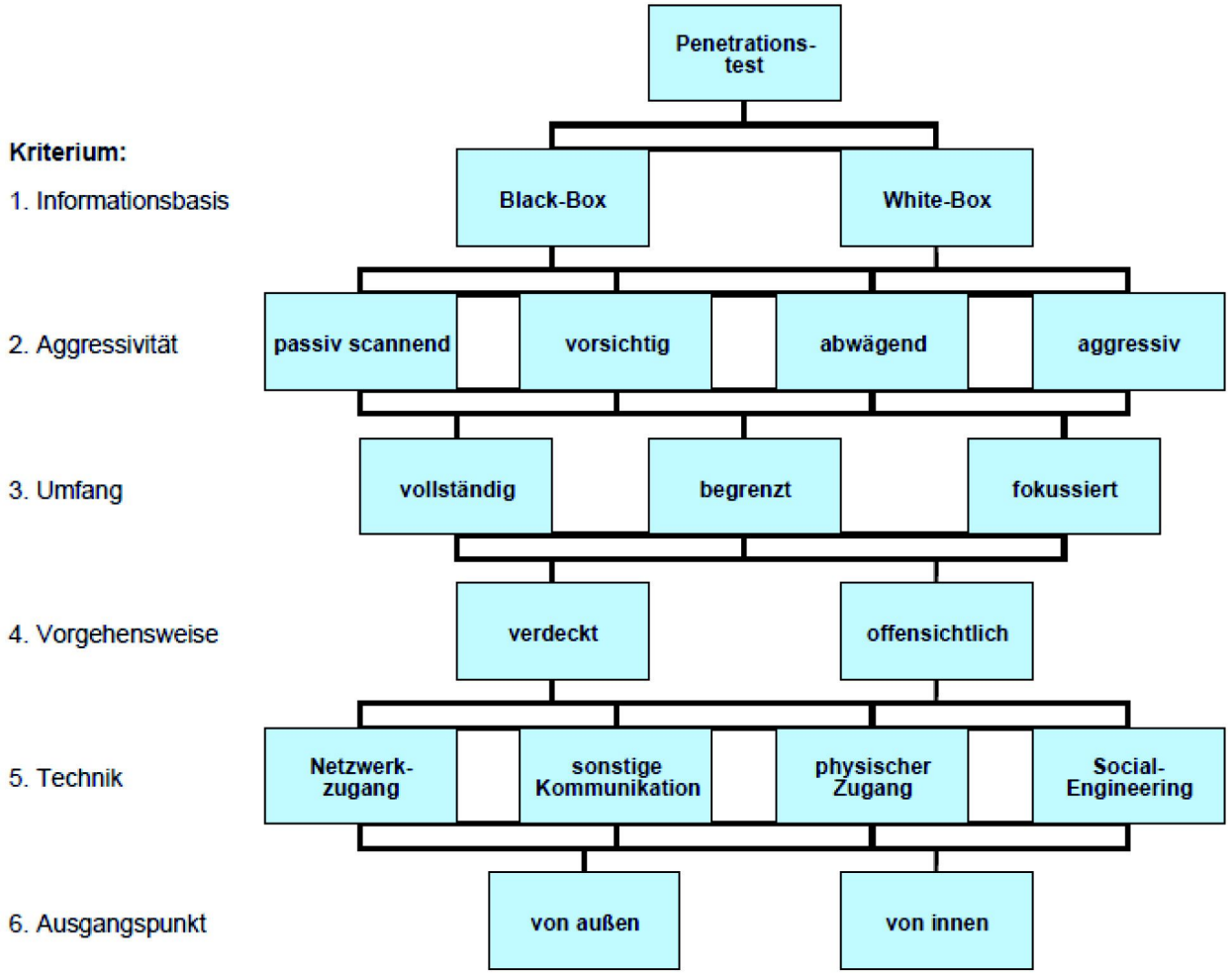

Abbildung 1: Klassifikation von Penetrationstests (Quelle: [BSI-PENTESTS])

In Tabelle 3 werden die Werte der einzelnen Kriterien kurz beschrieben.

Kriterium	Wert	Beschreibung
Informationsbasis	Black-Box	Simulation eines Angriffs ohne jegliches Insiderwissen
	White-Box	Simulation eines Angriffs unter Benutzung von vorhandenem Insiderwissen (z. B. ehemalige Mitarbeiter)
Aggressivität	Passiv scannend	Nur passive Untersuchung der Testobjekte (z. B. ein automatisches Portscan)
	Vorsichtig	Untersuchung der Schwachstellen, die mit Sicherheit keine Beeinträchtigung des untersuchten Systems nach sich ziehen (z. B. Test der Default-Passwörter oder Ausprobieren von Verzeichniszugriffen auf einem Web-Server)
	Abwägend	Untersuchung der Schwachstellen, die unter Umständen eine Beeinträchtigung des untersuchten Systems nach sich ziehen, nachdem die Konsequenzen abgewogen worden sind (z. B. Ausnutzen von bekannten Buffer-Overflows, oder automatisches Durchprobieren von Passwörtern)
	Aggressiv	Untersuchung aller potentiellen Schwachstellen (z. B. Schwachstellen, auch bei nicht eindeutig identifizierten Systemen oder DOS-Attacken)
Umfang	Vollständig	Betrachtung aller Systeme
	Begrenzt	Betrachtung von begrenzter Anzahl der Systeme (z. B. alle Systeme in einer DMZ oder alle Systeme, die einen funktionalen Verbund darstellen etc.)
	Fokussiert	Betrachtung mit Fokus auf ein bestimmtes Teilnetz, System oder bestimmten Dienst

Kriterium	Wert	Beschreibung
Vorgehensweise	Verdeckt	Benutzung von Methoden, die nicht direkt als Angriffsversuche erkannt werden können
	Offensichtlich	Einbeziehung der Systemverantwortlichen, Verwendung auch offensichtlicher Methoden (z. B. umfangreiche Port-Scans)
Technik	Netzwerkzugang	Penetration durch das Netzwerk (klassisches Vorgehen)
	Sonstige Kommunikationen	Untersuchung anderer vorhandener Kommunikationsnetze (z. B. Telefon, Telefax, Bluetooth etc.)
	Physischer Zugang	Überprüfung der physischen Zugänge
	Social Engineering	Interaktion mit den zuständigen Personen
Ausgangspunkt	Von außen	Untersuchung außerhalb des Netzes (typischerweise aus dem Internet)
	Von innen	Untersuchungen innerhalb des Netzes

Tabelle 3: Erklärung der Werte der einzelnen Kriterien

3.2 Rechtliche Aspekte

Die Durchführung der Penetrationstests simuliert einen Angriff auf die Ressourcen des Auftraggebers. Dieses Vorgehen zieht normalerweise juristische Konsequenzen, bezogen auf den Angreifer, nach sich. Aus diesem Grund ist es wichtig das geplante Vorhaben sehr genau in Form eines Vertrags zwischen dem Tester und Auftraggeber festzulegen (vergleiche [BSI-PENTESTS], Kapitel 4.3).

Weiterhin sind sehr oft im Zuge der Durchführung von Penetrationstests Daten, die unter besonderen Schutz (z. B. personenbezogene Daten) offengelegt wurden. Der Umgang mit solchen Daten ist sehr präzise geregelt und muss unbedingt befolgt werden (z. B. durch Einbeziehung des Datenschutzbeauftragten, eines Vertreters der HR-Abteilung etc.).

Eine tiefergreifende Betrachtung der rechtlichen Aspekte ist dem Kapitel 4 in [BSI-PENTESTS] zu entnehmen.

3.3 Weitere Rahmenbedingungen

Abgesehen vom rechtlichen Rahmen (vergleiche Kapitel 3.2) müssen bei der Durchführung von Penetrationstests auch die organisatorischen (vergleiche [BSI-PENTESTS], Kapitel 5.1), personellen (vergleiche [BSI-PENTESTS], Kapitel 5.2) und technischen (vergleiche [BSI-PENTESTS], Kapitel 5.3) Bedingungen erörtert werden.

3.4 Durchführung

Die Durchführung der Penetrationstests wird gemäß [BSI-PENTESTS] in fünf Phasen unterteilt:

– Vorbereitung,
– Informationsbeschaffung,
– Bewertung der Information/Risikoanalyse,
– Eindringversuche und
– Abschlussanalyse.

Diese Phasen werden dabei stets parallel von einer zusätzlichen Phase – Dokumentation – begleitet (vergleiche Abbildung 2).

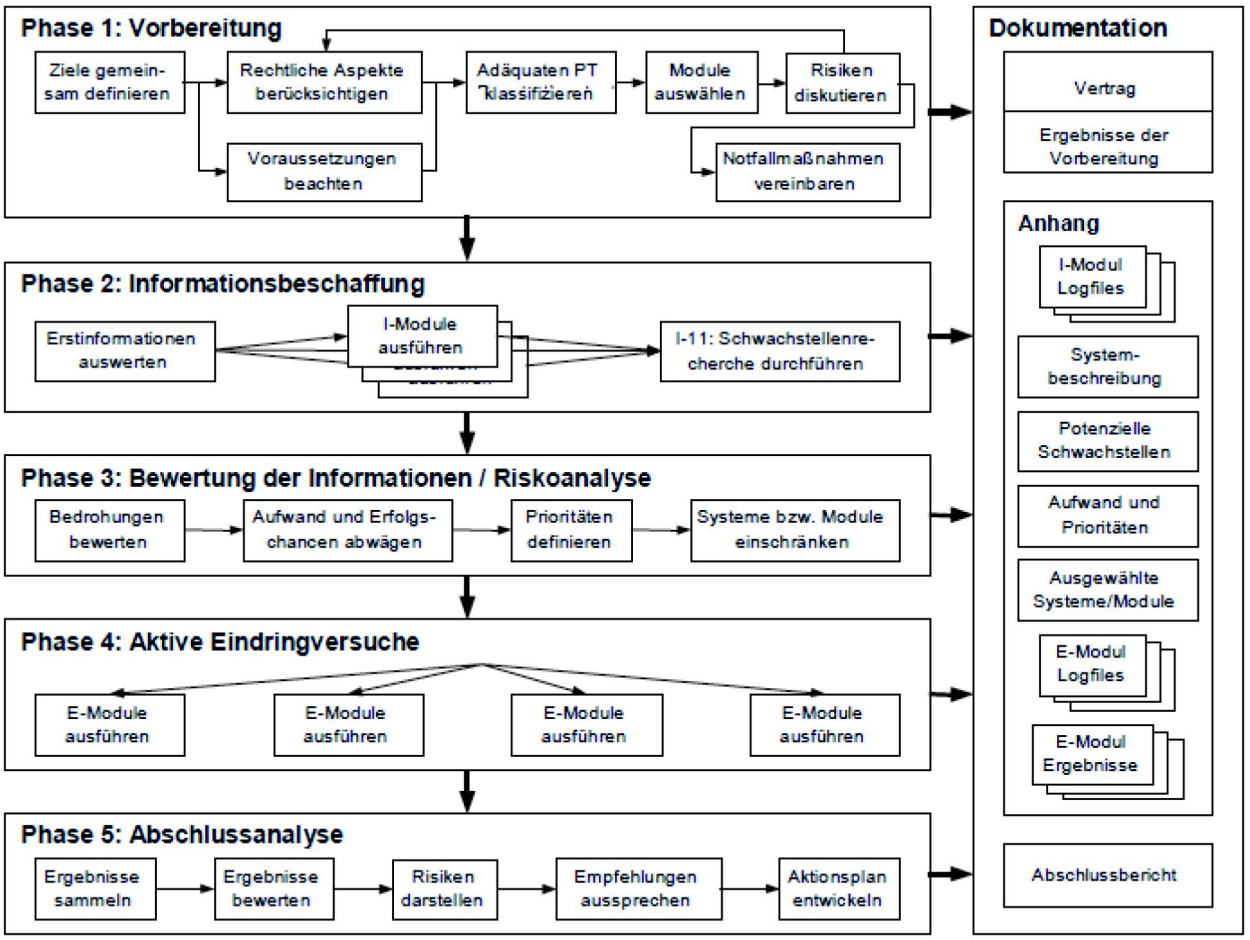

Abbildung 2: Fünfphasige Vorgehensweise für Penetrationstests (Quelle: [BSI-PENTESTS])

Detailliertere Beschreibung des Vorgehens ist dem Kapitel 6.3 in [BSI-PENTESTS] zu entnehmen.

Insbesondere werden in den Phasen 2 und 4 mit Hilfe der sogenannten I- und E-Module (vergleiche Kapitel 6) die tatsächlichen Tests durchgeführt. Die Auswahl der Module erfolgt nach einem negativen Ausschlussprinzip anhand der gewählten Klassifikation (vergleiche [BSI-PENTESTS], Kapitel 6.4.4 und Abbildung 3). Wird ein Modul nicht ausgeschlossen, so muss es durchgeführt werden. Falls ein Modul aus anderen Gründen ausgeschlossen werden soll, so müssen die dafür vorliegenden Gründe erläutert und dokumentiert werden.

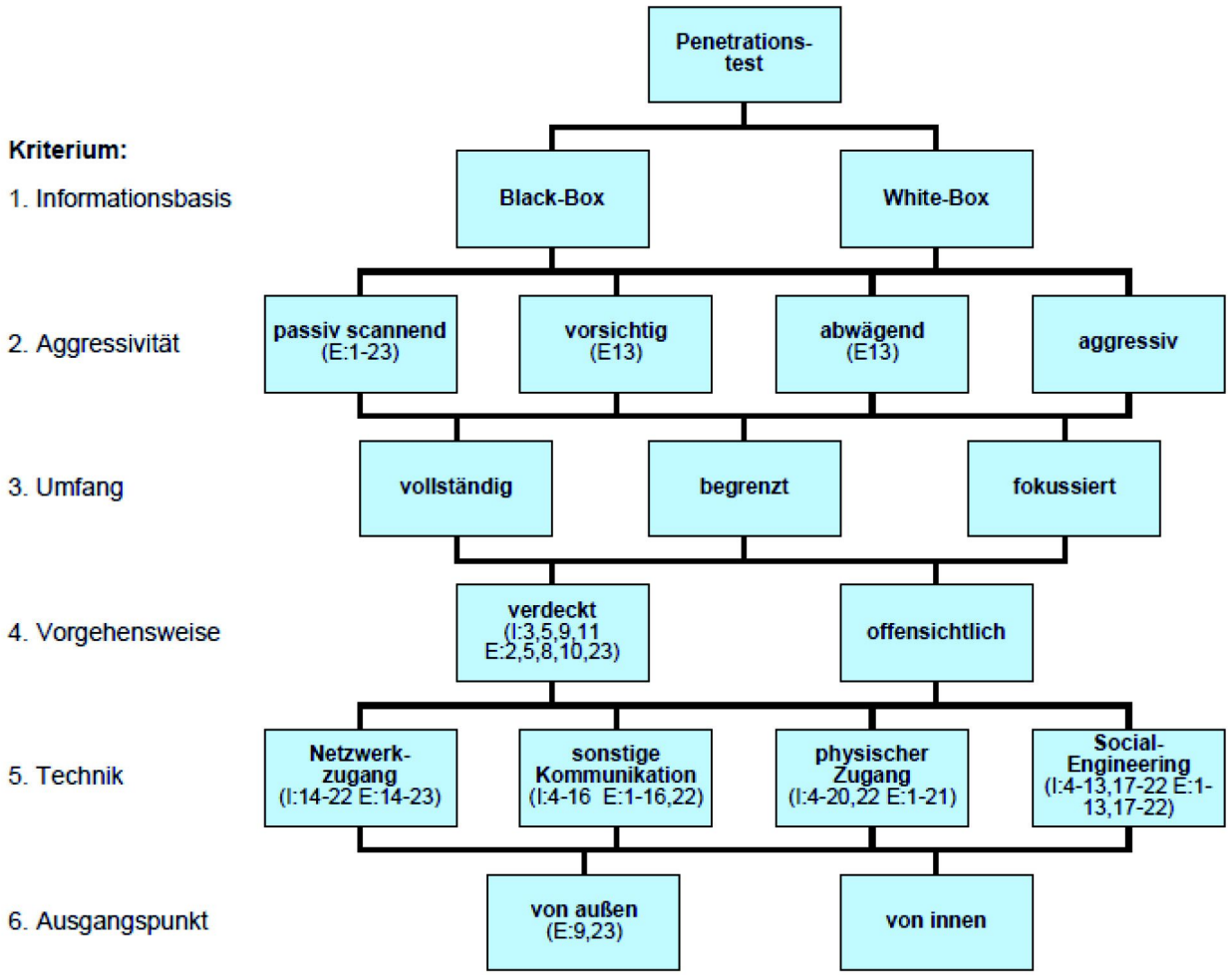

Abbildung 3: Ausschluss der Module durch die Klassifikationskriterien (Quelle: [BSI-PENTESTS])

Abbildung 3 zeigt die Zuordnung der auszuschließenden I- und E-Module pro Klassifikationskriterium.

4 Die durchzuführenden Penetrationstests

In diesem Kapitel werden die Prüfungen beschrieben, deren erfolgreiche Durchführung im Rahmen des Zulassungsverfahrens für die Anbindung an die KBA-Infrastruktur (vergleiche [KBA-MSADP], Abschnitt 8) gegenüber dem KBA nachgewiesen werden müssen.

Die Durchführung der im Rahmen dieses Dokumentes vorgeschriebenen Prüfungen soll die Bestätigung der Infomationssicherheit durch einen externen Dritten als Ziel verfolgen.

4.1 IS-Kurzrevision

Die IS-Kurzrevision dient der Unterstützung bei der Umsetzung und Optimierung der Informationssicherheit. Gegenstand ist die Basisabsicherung nach IT-Grundschutz. Dabei werden auch Aspekte, wie die Einbettung in die Infrastruktur oder organisatorische Fragen untersucht.

Die Durchführung einer IS-Kurzrevision erfolgt nach der vom BSI herausgegebenen Methodik[4].

[4] Siehe [BSI-KURZREV]

4.2 IS-Webcheck

Der IS-Webcheck dient der Prüfung des Sicherheitsstandards einer Internetpräsenz durch den Einsatz automatisierter Methoden.

Die Durchführung eines IS-Webchecks erfolgt nach der vom BSI herausgegebenen Methodik[5].

[5] Siehe [BSI-WEBCHK]

4.3 IS-Penetrationstest

Der IS-Pentest untersucht vorrangig die Schnittstellen einer Institution nach außen über die potentielle Angreifer die IT-Systeme kompromittieren könnten.

4.3.1 Klassifikation

Es werden IS-Penetrationstests mit folgenden Klassifikationen (vergleiche Tabelle 4) gefordert:

Kriterium	Klassifikation 1	Klassifikation 2
Informationsbasis	Black-Box, White-Box	Black-Box, White-Box
Aggressivität	Abwägend	Abwägend
Umfang	Fokussiert	Fokussiert
Vorgehensweise	Offensichtlich	Offensichtlich
Technik	Netzwerkzugang	Physischer Zugang
Ausgangspunkt	Von außen	Von außen

Tabelle 4: Klassifikation der durchzuführenden Penetrationstests

Für die Auswahl der beiden Klassifikationen war das Kriterium Technik von entscheidender Bedeutung. Einerseits werden die Netzwerkinfrastruktur und andererseits die physikalische Absicherung der Umgebung betrachtet.

4.3.2 Ausgeschlossene I-/E-Module

Basierend auf der in Tabelle 4 dargelegten Klassifikation ergibt sich folgende Tabelle der ausgeschlossenen I- und E-Module.

Kriterium	Werte	Ausgeschlossene I-Module	Ausgeschlossene E-Module
Informationsbasis	Black-Box		
	White-Box		
Aggressivität	Abwägend		E13
Umfang	Fokussiert		
Vorgehensweise	Offensichtlich		
Technik	Netzwerkzugang	I14 bis I22	E14 bis E23
	Physischer Zugang	I4 bis I20; I22	E1 bis E21
Ausgangspunkt	Von außen		E9; E23

Tabelle 5: Ausgeschlossene I- und E-Module für spezifizierte Klassifikation

Somit ergibt sich, dass die folgenden Module ausgeschlossen sind:

	Klassifikation 1	Klassifikation 2
I-Module	I14 bis I22	I4 bis I20; I22
E-Module	E9; E13 bis E23	E1 bis E21; E23

Tabelle 6: Ausgeschlossene I- und E-Module

Die durchzuführenden Module sind der Tabelle 7 und der Tabelle 8 zu entnehmen.

Test	Durchzuführende I-Module
Klassifikation 1	– I1 – Auswertung öffentlich zugänglicher Daten – I2 – Verdeckte Abfragen von Netzwerkbasisinformationen – I3 – Offensichtliche Abfragen von Netzwerkbasisinformationen – I4 – Verdeckte Durchführung von Portscans – I5 – Offensichtliche Durchführung von Portscans – I6 – Identifikation von Anwendungen – I7 – Identifikation von Systemen – I8 – Verdeckte Identifikation der Router – I9 – Offensichtliche Identifikation der Router – I10 – Verdeckte Identifikation der Firewalls – I11 – Offensichtliche Identifikation der Firewalls – I12 – Recherche nach Schwachstellen – I13 – Identifikation von Anwendungsschnittstellen

Test	Durchzuführende I-Module
Klassifikation 2	– I1 – Auswertung öffentlich zugänglicher Daten – I2 – Verdeckte Abfragen von Netzwerkbasisinformationen – I3 – Offensichtliche Abfragen von Netzwerkbasisinformationen – I21 – Analyse der physischen Umgebung

Tabelle 7: Durchzuführende I-Module

Test	Durchzuführende E-Module
Klassifikation 1	– E1 – Verdeckte Verifikation tatsächlicher Schwachstellen – E2 – Offensichtliche Verifikation tatsächlicher Schwachstellen – E3 – Verifikation tatsächlicher Schwachstellen in Anwendungsschnittstellen – E4 – Verdeckter Test der Router – E5 – Offensichtlicher Test der Router – E6 – Test von Vertrauensbeziehungen zwischen Systemen – E7 – Verdeckter Test der Firewall von außen – E8 – Offensichtlicher Test der Firewall von außen – E10 – Test des IDS – E11 – Abhören von Passwörtern – E12 – Test von Passwörtern
Klassifikation 2	– E22 – Aktiver Test der Zutrittskontrollen

Tabelle 8: Durchzuführende E-Module

Die konkreten, durchzuführenden Prüfungsschritte sind in der Beschreibung der jeweiligen Module enthalten (vergleiche [BSI-PENTESTS], Kapitel 6.5).

4.3.3 Dokumentation

Die erfolgreiche Absolvierung der Penetrationstests muss dokumentiert werden. Diese Dokumentation muss dem KBA entsprechend vorgelegt werden (vergleiche hierzu [KBA-MSADP], Kapitel 8.4).

Die Dokumentation soll zumindest folgende Bestandteile aufweisen:

1. Die Dokumentation der durchgeführten Prüfungsschritte zur Informationsbeschaffung einschließlich einer Liste der geprüften Schwachstellen,
2. die Dokumentation der durchgeführten Prüfungsschritte bei den Eindringversuchen einschließlich einer Liste der geprüften Schwachstellen,
3. Abschlussbericht.

4.3.4 Übersicht über relevante Angriffstechniken

In diesem Kapitel wird eine kurze Übersicht über die üblichen Angriffstechniken vermittelt, deren Verwendung empfohlen wird. Weiterhin wird zu jeder vorgestellten Angriffstechnik ein Mapping auf die relevante Module eingegeben.

Netzwerk- und Portscanning

Es können offensichtliche und/oder auch verdeckte Scan-Aktivitäten durchgeführt werden. Die Durchführung zielt auf die Auffindung der im untersuchten Netz aktiven IT-Systeme und somit Identifizierung der dahinter stehenden Dienste (hier gegeben durch bestimmte Ports) ab. Die gewonnenen Erkenntnisse dienen als Informationsbasis für die weiterführenden Aktivitäten.

Involvierte I- und E-Module: I3, I4, I5, I7, I8, I9, I10, I11, I12, I13.

Ausnutzung mangelhafter Eingabeüberprüfung

Die vom Benutzer getätigten Eingaben sollten auf deren Korrektheit und Plausibilität geprüft und ggf. zurückgewiesen werden. Findet diese Filterung nicht bzw. im unzureichenden Umfang statt, besteht unter Umständen eine Möglichkeit in das System einen fremden Code einzuschleusen und die Anwendung in der Funktionalität zu beeinträchtigen oder geschützte Information zu gewinnen (z. B. Cross-Site-Scripting[6] [XSS], LDAP-/SQL-Injection[7], etc.).

[6] Vgl. http://de.wikipedia.org/wiki/Cross-Site-Scripting

[7] Vgl. http://de.wikipedia.org/wiki/SQL-Injection

Involvierte I- und E-Module: E1, E2, E3, E6, E7, E8, E9, I10, E11.

Denial-of-Service-Angriffe (DOS) – optional

DOS und insbesondere die verteilte Variante hiervon – D-DOS gehören zu sehr aggressiven Angriffstechniken. Das Ziel des Angriffs ist die Blockierung des untersuchten Netzes oder IT-Systems, normalerweise mit Hilfe eines massiv er-

höhten Datenaufkommens oder der Ausnutzung möglicher Software-Schwachstellen (z. B. Ping of Death[8]). Aus diesem Grund ist es einzeln abzuwägen, im welchem Umfang diese Techniken während der Penetrationstests zum Einsatz kommen sollen.

[8] Vgl. http://de.wikipedia.org/wiki/Ping_of_Death

Involvierte I- und E-Module: E13 – kein ausgewähltes Modul.

Information Gathering

Durchführung von Aktivitäten, die die Vorbereitung einer Informationsbasis für die Durchführung der tatsächlichen Attacken ermöglichen sollen (z. B. ein Versuch, die benutzten Schemata für die Benennung der Systeme und Verzeichnisse zu identifizieren).

Involvierte I- und E-Module: I1, I2, I3, I6, I12.

Passwort-Attacken

Der Versuch die benutzten Kennwörter mit Hilfe unterschiedlicher Techniken zu kompromittieren. Die Angriffspalette reicht hier vom einfachen Ausprobieren der Standard-Passwörter, über die sogenannten Wörterbuchattacken[9] bis hin zu Brute-Force-Attacken[10].

[9] Vgl. http://de.wikipedia.org/wiki/W%C3%B6rterbuchangriff

[10] Vgl. http://de.wikipedia.org/wiki/Brute-Force-Methode

Involvierte I- und E-Module: E4, E5, E11, E12.

Ausnutzen von Software-Schwachstellen

Zum Umfang dieser Technik gehört das Ausprobieren bekannter Schwachstellen einer Software, indem Exploits[11] eingesetzt werden.

[11] Vgl. http://de.wikipedia.org/wiki/Exploit

Involvierte I- und E-Module: E1, E2, E3, I10.

Kryptographische Angriffe

Die Angriffe dieser Kategorie versuchen Schwachstellen eingesetzter Verschlüsselungsalgorithmen und Schlüsselverwaltungen in Implementierungen zu überprüfen.

Involvierte I- und E-Module: E5.

Infrastruktur-Untersuchungen

Unter diese Kategorie fällt die Untersuchung von baulichen Maßnahmen, wie z. B. die Zutritts- bzw. Schließungseinrichtungen. Darüber hinaus sind weiterreichende Aspekte, wie z. B. ordnungsgemäße Entsorgung von Materialien (z. B. Dumpster Diving) inbegriffen.

Involvierte I- und E-Module: I21, E22.

5 Quellen

[BSI-PENTESTS] Studie: Durchführungskonzept für die Penetrationstests, BSI, Stand: November 2003, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest_pdf.pdf?__blob=publicationFile

[BSI-KURZREV] Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz –: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf?__blob=publicationFile

[BSI-WEBCHK] IS-Webcheck – Sicherheits-Check für Webauftritte durch das BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Beschreibung_Webcheck.pdf?__blob=publicationFile

[BSI-M5.150] IT-Grundschutz, M 5.150 Durchführung von Penetrationstests, Stand: 13. EL Stand 2013, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05150.html

[KBA-MSADP] Mindest-Sicherheitsanforderungen an dezentrale Portale, KBA, Version 1.0

6 Anhang A

6.1 Vollständige Auflistung der I-/E-Module

Nr.	Modulbezeichnung
I1	Auswertung öffentlich zugänglicher Daten
I2	Verdeckte Abfragen von Netzwerkbasisinformationen

Nr.	Modulbezeichnung
I3	Offensichtliche Abfragen von Netzwerkbasisinformationen
I4	Verdeckte Durchführung von Portscans
I5	Offensichtliche Durchführung von Portscans
I6	Identifikation von Anwendungen
I7	Identifikation von Systemen
I8	Verdeckte Identifikation der Router
I9	Offensichtliche Identifikation der Router
I10	Verdeckte Identifikation der Firewalls
I11	Offensichtliche Identifikation der Firewalls
I12	Recherche nach Schwachstellen
I13	Identifikation von Anwendungsschnittstellen
I14	Sammlung von Informationen für Social-Engineering
I15	Sammlung von Informationen für computerbasiertes Social-Engineering
I16	Sammlung von Informationen für persönliches Social-Engineering
I17	Überprüfung der drahtlosen Kommunikation (nur scannend)
I18	Test der Telefonanlage (Identifikation)
I19	Test des Voicemail Systems (Identifikation)
I20	Test des Faxsystems (Identifikation)
I21	Analyse der physischen Umgebung
I22	Identifikation von Zutrittskontrollen

Tabelle 9: Liste der Module zur Informationsbeschaffung (I-Module)

Nr.	Modulbezeichnung
E1	Verdeckte Verifikation tatsächlicher Schwachstellen
E2	Offensichtliche Verifikation tatsächlicher Schwachstellen
E3	Verifikation tatsächlicher Schwachstellen in Anwendungsschnittstellen
E4	Verdeckter Test der Router
E5	Offensichtlicher Test der Router
E6	Test von Vertrauensbeziehungen zwischen Systemen
E7	Verdeckter Test der Firewall von außen
E8	Offensichtlicher Test der Firewall von außen
E9	Beidseitiger Test der Firewall
E10	Test des IDS
E11	Abhören von Passwörtern
E12	Test von Passwörtern
E13	Test von „Denial-of-Service“-Anfälligkeit
E14	Computerbasiertes Social-Engineering
E15	Direktes, persönliches Social-Engineering mit physischem Zutritt
E16	Indirektes, persönliches Social-Engineering ohne physischen Zutritt
E17	Überprüfung der drahtlosen Kommunikation
E18	Test der administrativen Zugänge zur Telefonanlage
E19	Test des Voicemail Systems
E20	Test der administrativen Zugänge zum Faxsystem

Nr.	Modulbezeichnung
E21	Test von Modems
E22	Aktiver Test der Zutrittskontrollen
E23	Überprüfung der Eskalationsprozeduren

Tabelle 10: Liste der Module für aktive Eindringungsversuche (E-Module)

6.2 Beispiele einer Beschreibung der I-/E-Module

I 4. Verdeckte Durchführung von Portscans	
Es werden alle identifizierten Geräte einem unauffälligen bzw. verdeckten Portscan unterzogen um festzustellen, welche Dienste das jeweilige Gerät mit welchem Betriebssystem anbietet.	
Erwartete Ergebnisse:	**erledigt**
• Informationen über angebotene Dienste des Geräts	☐
• Identifizierung des Betriebssystems	☐
Voraussetzungen:	
Kenntnis von Netzwerkbasisinformationen.	
Prüfungsschritte:	**Aufwand**
• Durchführung eines Portscans, der sich nicht bzw. nur schwierig entdecken lässt. Dies kann z. B. mit Hilfe geeigneter Parameter bei dem Einsatz von Portscanning–Tools oder durch lange Pausen zwischen den einzelnen Abfragen erreicht werden.	mittel
Risiken:	
Der Portscan könnte entdeckt werden.	

Abbildung 4: Beschreibung eines I-Moduls – Beispiel

E 9. Beidseitiger Test der Firewall	
Untersuchung der Firewall durch gleichzeitigen Test auf beiden Seiten der Firewall: Ein „außen" platziertes System sendet Pakete, ein „innen" platziertes System analysiert die durchkommenden Pakete und umgekehrt.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung der Firewallregeln	☐
• Verifikation von identifizierten Schwachstellen des eingesetzten Firewalltyps	☐
• Vervollständigte Auflistung der erreichbaren Systeme hinter der Firewall	☐
Voraussetzungen:	
Ergebnisse I 10: Informationen über die eingesetzten Firewallkomponenten, Netzzugang zu einem Punkt hinter der Firewall.	
Prüfungsschritte:	**Aufwand**
• Test, ob (u. U. auch mit Hilfe von getunnelten Protokollen) unzulässige Verbindungen aus dem internen Netz ins Internet aufgebaut werden können	hoch
• Einsatz eines Schwachstellenscanners auf die Hosts des Firewall-Systems (Firewall-Host, externer Router, interner Router) von innen	mittel
• Ermittlung der Firewallregeln mit Hilfe geeigneter Tools (beidseitiges Firewalking)	hoch
• Überprüfung der Reaktion der Firewall auf fragmentierte und gespoofte Pakete, die mittels eines Paketgenerators erzeugt wurden	sehr hoch
Risiken:	
Das Firewallsystem könnte in seiner Funktion beeinträchtigt werden.	

Abbildung 5: Beschreibung eines E-Moduls – Beispiel