Bundesanzeiger
Herausgegeben vom
Bundesministerium der Justiz
www.bundesanzeiger.de

Kraftfahrt-Bundesamt

Bekanntmachung „Internetbasierte Fahrzeugzulassung (i-Kfz) – Mindestsicherheitsanforderungen an die internetbasierte Fahrzeugzulassung“ Version 1.5

Vom 17. Juli 2023

Auf Grund des § 18 Absatz 3 der zum 1. September 2023 in Kraft tretenden neugefassten Fahrzeug-Zulassungsverordnung (FZV) gebe ich nachfolgend die neu gefassten Standards „Internetbasierte Fahrzeugzulassung (i-Kfz) – Mindestsicherheitsanforderungen an die internetbasierte Fahrzeugzulassung, Stand 11. April 2023, Version 1.5“ bekannt (Anlage).

Die Neufassung gilt ab dem 1. September 2023.

Die Neufassung ist die Version 1.5 und hat den Stand vom 11. April 2023.

Die mitgeltenden Dokumente der Übermittlungsstandards sind auf der Internetseite des Kraftfahrt-Bundesamtes unter www.kba.de im geschützten Bereich eingestellt.

Die „Standards für Internetbasierte Fahrzeugzulassung (i-Kfz) – Mindest-Sicherheitsanforderungen an dezentrale Portale und Zulassungsbehörden“ vom 17. Juni 2021 (BAnz AT 06.09.2021 B5), werden zum 1. September 2023 aufgehoben.

Flensburg, den 17. Juli 2023

Kraftfahrt-Bundesamt

Der Präsident
R. Damm

Anlage

Änderungsverzeichnis

Version	Datum	Geänderte Kapitel	Grund der Änderung	Name
1.0	13.11.2014	alle	Vorbereitung der Veröffentlichung (Layout)	KBA
1.0.1	15.12.2014	8.5	Anpassung Fristen zum Nachweis Pen-Test/Audits	KBA
1.1	15.01.2016	alle	Redaktionelle Überarbeitung gemäß UAG Sitzung vom 13. Januar 2016	KBA
1.1.1	24.02.2016	7, 8.2	Streichung der Berichtsvorlage, Spezifizierung der Protokollaufbewahrung, Hinweis zur Gleichwertigkeit der ISO Zertifizierungen	KBA
1.2	01.04.2019	alle	Umsetzung der Ergebnisse der Sitzung am 7. März 2019: Zusammenfassung mit den Dokumenten Annex B und Anlage Pentest, Einarbeitung der FAQs, Erstellung des Kapitels „Fallszenarien“, Änderungen bezüglich i-Kfz Stufe 2 und 3	BPT
1.3	12.07.2019	alle	Fachliche Überarbeitung des Kapitels Pentests auf Basis der aktuellen BSI-Leitfäden, Überarbeitung des Kapitels „Fallszenarien“, Einarbeitung der direkten Kommunikationsmöglichkeit zwischen Fachverfahren und dezentralen Portalen über das NdB-VN, Anpassung der rechtlichen Regelungen bzgl. Grundschutz, DSGVO und eIDAS-VO, Aufnahme der BSI Mindeststandards und Berücksichtigung neuer Grundschutz, Überarbeitung der Quellen	KBA, BPT
1.4	13.07.2019	alle	Zusammenfassung letzter redaktioneller Änderungen und abschließende QS	KBA
1.4.1	22.07.2019	6, 8	Inkonsistente Nummerierung der Anforderungen in Nummer 6 sowie in den Fallszenarien in Nummer 8 angepasst. Anforderung A-6.1.12 bei den Fallszenarien ergänzt	KBA
1.4.2	12.10.2019	alle	Korrektur Rechtschreibfehler und Referenzen, Einarbeitung von Rückmeldungen des BSI, Ergänzung Rechtsgrundlagen, Änderung Anforderungen NdB-VN-DMZ (PAP/TLS 1.3), Änderung der Anforderungen für die außerordentliche Durchführung von Pentests	KBA
1.4.3	16.10.2019	5, 7, 8	Referenz zu nichtexistierendem Kapitel korrigiert	KBA
1.4.4	21.03.2021	alle	Klarstellungen und Auflösungen von Redundanzen, Einarbeitung von Rückmeldungen des BSI und des Fachkreises	KBA
1.4.9	30.11.22	alle	Anpassungen im Zuge der vierten i-Kfz-Stufe	KBA
1.5	11.04.23	alle	Klarstellungen und Auflösungen von Redundanzen, Einarbeitung von Rückmeldungen unter anderem des BSI	KBA

Inhaltsverzeichnis

1 Verzeichnisse

1.1 Mitgeltende Dokumente

– Internetbasierte Fahrzeugzulassung (i-Kfz) – Fachkonzept Stufe 4 – Zugang über i-Kfz-Portale

– Digitale Fahrzeugzulassung für Großkunden im Kraftfahrt-Bundesamt – Zentrale GKS

– Informationen zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt

– Standards für die Datenübermittlung zur Nutzung der Großkundenschnittstelle für Großkunden

– Standards für die Datenübermittlung an das Kraftfahrt-Bundesamt – Datenaustausch mit den Zulassungsbehörden

– Standards für die Datenübermittlung an das Kraftfahrt-Bundesamt – Datenaustausch mit i-Kfz-Portalen

Die Dokumente sind beziehungsweise werden in der jeweils aktuellen Fassung unter www.kba.de gegebenenfalls im „geschützten Bereich“ bereitgestellt.

Heute wird in öffentlichen Bereichen – wie auch beim KBA – auf gendergerechte Sprache geachtet. Es kann jedoch vorkommen, dass vor allem ältere Dokumente nicht diesem Anspruch genügen. Wir bitten dies im Hinblick auf den damit verbundenen redaktionellen Aufwand zu entschuldigen. Bei zukünftiger inhaltlicher Überarbeitung werden diese Dokumente ebenfalls auf gendergerechte Sprache überprüft und gegebenenfalls angepasst.

1.2 Abkürzungsverzeichnis

aAB	Automatisierte Antragsbearbeitung
AnVN	Anschlussbedingungen für das Verbindungsnetz
BDSG	Bundesdatenschutzgesetz
BMDV	Bundesministerium für Digitales und Verkehr
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-ISI	BSI Standards zur Internet-Sicherheit
BSI-ITG	BSI IT-Grundschutz
BSI-TR	BSI Technische Richtlinie
Cnn	Connector
DMZ	Demilitarisierte Zone
DSGVO	Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG)
eID	Elektronische Identifizierung
eIDAS-VO	elektronische Identifizierungs-, Authentifizierungs- und Vertrauensdienste – Verordnung (Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG [Signaturrichtlinie])
ESP	Encapsulated Security Payload
FZV	Fahrzeug-Zulassungsverordnung
GK	Großkunde
GKS	Großkundenschnittstelle
GUI	Graphische Benutzeroberfläche
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifikator/Kennung
IDS	Intrusion Detection System
IKE	Internet Key Exchange Protocol
i-Kfz	Internetbasierte Fahrzeugzulassung
IP	Internet Protocol
IPSec	Internet Protocol Security
IS	Informationssicherheit
ISi	Internet Sicherheit
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnologie
KBA	Kraftfahrt-Bundesamt
KBAG	Gesetz über die Errichtung eines Kraftfahrt-Bundesamtes
Kom-Modul	Kommunikation-Modul
MSA-i-Kfz	Mindestsicherheitsanforderungen an die internetbasierte Fahrzeugzulassung
NdB-VN	Netz des Bundes – Verbindungsnetz
OpenFT	Open File Transfer
RFC	Request for Comments
SABRINA	System zum asynchronen, behördenübergreifenden Informations- und Nachrichtenaustausch
tAB	teilautomatisierte Antragsbearbeitung
TLS	Transport Layer Security
TR	Technische Richtlinie
UAG	Unterarbeitsgruppe
VG	Verpflichtungsgrad
VPN	Virtual Private Network
WS	Web Service
XML	Extensible Markup Language
ZFZR	Zentrales Fahrzeugregister
ZulB	Zulassungsbehörde

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 KBA. Mit diesem Dokument werden Mindestanforderungen an die Informationssicherheit bei der Anbindung von i-Kfz-Portalen und Zulassungsbehörden definiert, die zwingend zu erfüllen sind.

Im Zuge der Umsetzung der ersten Stufe i-Kfz zum 1. Januar 2015, der zweiten Stufe i-Kfz zum 1. Oktober 2017 und der dritten Stufe i-Kfz zum 1. Oktober 2019 kann der komplette Lebenszyklus eines Fahrzeugs aus zulassungsrechtlicher Sicht, von der Neuzulassung bis zur Außerbetriebsetzung, internetbasiert abgewickelt werden. Die vierte Stufe i-Kfz stellt zum 1. September 2023 in seiner Gesamtheit eine umfangreiche Erweiterung der mit Stufe drei realisierten i-Kfz-Komponenten und -Funktionalitäten dar. Diese Ausbaustufe hat zum Ziel, die zulassungsrelevanten Anwendungsfälle zu automatisieren und diese auch für juristische Personen zu ermöglichen. Die Antragsstellung erfolgt über die i-Kfz-Portale der Zulassungsbehörden (ZulB) oder über die zentrale Großkundenschnittstelle (GKS) beim KBA.

In Diskussionen zwischen BMDV, KBA, BSI, Vertretern von kommunalen Spitzenverbänden, kommunalen IT-Dienstleistern und Zulassungsbehörden wurde eine grundlegende Architektur für die Kommunikationswege der Portale festgelegt („Hamburger Kompromiss“). Die i-Kfz-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. Das Gleiche gilt für die GKS und die Kommunikation der i-Kfz-Portale mit den Fachverfahren der ZulB.

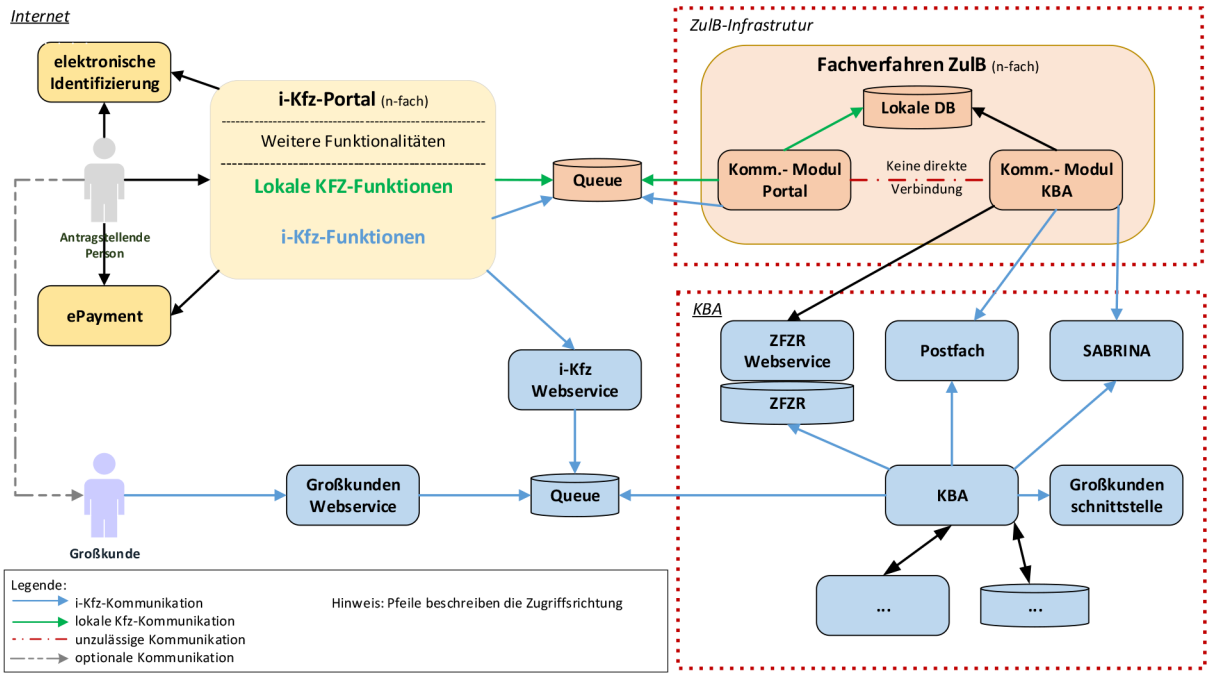

Abbildung 1: Kommunikationswege der Portale

Vor diesem Hintergrund ist die Datensicherheit der zentralen Register beim KBA sicherzustellen.

Der Schutzbedarf für das ZFZR wurde durch das KBA ermittelt. Er beträgt jeweils „hoch“ bezüglich aller drei Grundwerte (Vertraulichkeit, Integrität und Verfügbarkeit). Um dem hohen Schutzbedarf im Verfahren i-Kfz Rechnung zu tragen, hat das KBA entsprechende Mindestsicherheitsanforderungen an die Informationssicherheit der i-Kfz-Portale und der Zulassungsbehörden in diesem Dokument festgelegt.

Ein Sicherheitskonzept mit gegebenenfalls integrierter Risikoanalyse existiert für das Gesamtverfahren i-Kfz nicht. Somit ist eine ganzheitliche Betrachtung der Verfahrenssicherheit nicht möglich.

Unter Mitwirkung des BSI wurden deshalb die vorliegenden Mindestsicherheitsanforderungen entwickelt. Sie berücksichtigen die wichtigsten Aspekte der Informationssicherheit des i-Kfz-Verfahrens. Die Mindestsicherheitsanforderungen werden im weiteren Projektverlauf regelmäßig überprüft, ergänzt und gegebenenfalls 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 relevante rechtliche Grundlagen identifiziert:

- Gesetz über die Errichtung eines Kraftfahrt-Bundesamts (KBAG)
- Verordnung über die Zulassung von Fahrzeugen zum Straßenverkehr (Fahrzeug-Zulassungsverordnung – FZV)
- Viertes Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze (4. StVGuaÄndG)
- Bundesdatenschutzgesetz (BDSG)
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG DSGVO
- Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG EIDAS-VO

Weiterführende geltende Regelungen:

- Information zur netztechnischen Anbindung an das KBA für Behörden (vergleiche IznAaKBAfB).
- Standards für die Datenübermittlung zur Nutzung der Großkundenschnittstelle für Großkunden (vergleiche SDÜGK)
- Standard für die Datenübermittlung an das KBA – Datenaustausch mit den Zulassungsbehörden (vergleiche SDÜZulB)
- Standard für die Datenübermittlung an das KBA – Datenaustausch mit i-Kfz-Portalen (vergleiche SDÜiKP)

Das KBA nimmt gemäß KBAG, FZV und 4. 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 gelten insbesondere die §§ 18, 19 und 20 FZV.

4 Abgrenzung

Das vorliegende Dokument definiert die Mindestsicherheitsanforderungen, die zwingend ab der vierten Stufe des i-Kfz-Projekts erfüllt werden müssen. Es richtet sich primär an Zulassungsbehörden und deren Portal- und Fachverfahrensbetreiber.

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 Nummer 5.1) wird eine technische Sicht auf das Gesamtsystem dargestellt (vergleiche Nummer 5.2), in der die relevanten Netzwerkbereiche (vergleiche Nummer 5.3), die darin enthaltenen Komponenten (vergleiche Nummer 5.4) sowie die Schnittstellen (vergleiche Nummer 5.5) benannt und beschrieben werden.

5.1 Kommunikationsarchitektur innerhalb des i-Kfz-Systems

Die Abbildung 2 stellt die Anwendungen, die primären Akteure und die Kommunikationsflüsse aus funktionaler Sicht dar.

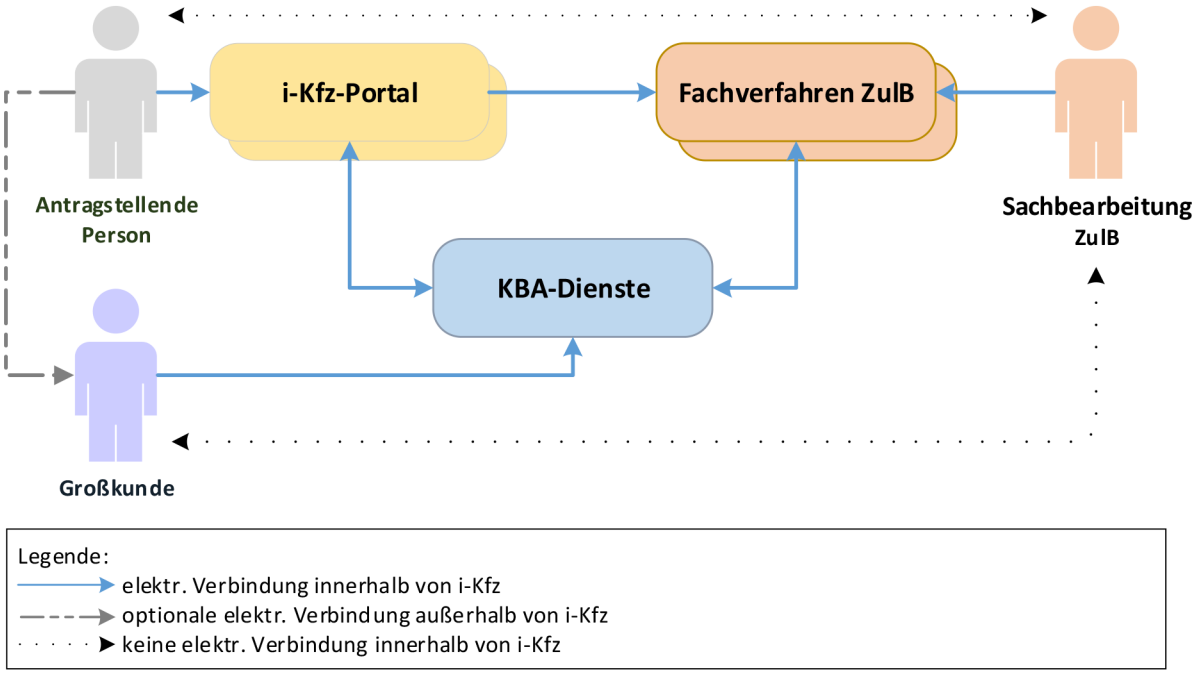

Abbildung 2: Primäre Akteure und Anwendungen sowie Kommunikationsflüsse im i-Kfz-System

Es sind drei primäre Akteure beteiligt:

- Antragstellende Person gemäß § 20 FZV
  - natürliche Personen (Bürger)
  - juristische Personen
  - Behörden
  - Vereinigungen, sofern ihnen ein Recht zustehen kann
  - beruflich Selbstständige als Halter
- Sachbearbeitung in der Zulassungsbehörde
- Großkunde (juristische Personen, die jährlich regelmäßig mehr als 500 Anträge im Sinne des § 33 Absatz 1 FZV stellen)
  - Flottenbetreiber (nur Anträge auf sich selbst [das eigene Unternehmen])
  - Dienstleister (Anträge für Dritte als Halter)

Weiterhin werden folgende Anwendungen genutzt:

- i-Kfz-Portal,
- Fachverfahren der Zulassungsbehörde,
- KBA-Dienste
  - Registerführung (insbesondere das ZFZR)
  - Großkundenschnittstelle (ermöglicht Großkunden die Maschine zu Maschine Kommunikation)
  - Kommunikationsplattform (System für asynchronen, behördenübergreifenden Informations- und Nachrichtenaustausch – kurz „SABRINA“)

5.1.1 Antragstellende Person

Die Rolle „Antragstellende Person“ bildet alle natürlichen und juristischen Personen (auch Behörden, Vereinigungen und beruflich Selbstständige) gemäß § 20 Absatz 3 FZV ab, welche entweder die Dienste eines i-Kfz-Portals über dessen graphische Benutzeroberfläche (GUI) oder die Dienste eines Großkunden (Dienstleister), der den KBA-Dienst Großkundenschnittstelle nutzt, in Anspruch nehmen. Die Verbindung der antragstellenden Person mit dem Großkunden (Dienstleister) stellt keine primäre i-Kfz-Funktionalität dar und wird daher in diesem Dokument nicht weiter betrachtet.

Es ist zu beachten, dass darüber hinaus die Möglichkeit besteht, dass die antragstellende Person über bereits schon existierende Schnittstellen beziehungsweise Anwendungen mit dem Fachverfahren der Zulassungsbehörde kommuniziert, zum Beispiel um einen Termin mit der Zulassungsbehörde zu vereinbaren, ein Wunschkennzeichnen zu

reservieren oder auch die benötigten Eingaben im Vorwege zu erfassen. Diese Anwendungen gehören nicht zum Funktionsumfang des i-Kfz-Projekts und werden daher als indirekt am Zulassungsprozess beteiligte Verfahren bezeichnet. Da diese jedoch seit Umsetzung der Gebührenrückstandsprüfung mit Stufe zwei des i-Kfz-Verfahrens mit dem i-Kfz-Projekt in Verbindung stehen, werden diese daher auch in diesem Dokument betrachtet.

5.1.2 Sachbearbeitung in der Zulassungsbehörde

Innerhalb der Zulassungsbehörden bearbeiten die Sachbearbeitenden die seitens der antragstellenden Personen oder des Großkunden beantragten Leistungen.

5.1.3 Großkunde

Eine juristische Person, die jährlich regelmäßig mehr als 500 Anträge im Sinne des § 33 Absatz 1 FZV stellt und die Standards für die Datenübermittlung zur Nutzung der Großkundenschnittstelle für Großkunden erfüllt, kann sich beim KBA als GK registrieren lassen, um Anträge über den KBA-Dienst Großkundenschnittstelle (Maschine zu Maschine Kommunikation) für sich selbst (Flottenbetreiber) oder für Dritte als Halter (Dienstleister) einreichen zu können. Beide Rollen können gleichzeitig wahrgenommen werden. Von einem Großkunden beziehungsweise dessen Systemen können weitere lokale Funktionalitäten, die aber keine primäre i-Kfz-Funktionalität darstellen (zum Beispiel e-Payment, elektronischer Identitätsnachweis) genutzt werden. Die im Fall eines Dienstleisters notwendige Verbindung/Kommunikation mit der antragstellenden Person stellt keine primäre i-Kfz-Funktionalität dar (vergleiche Nummer 5.1.1).

5.1.4 i-Kfz-Portal

Im Auftrag der Zulassungsbehörden werden i-Kfz-Portale betrieben, welche den antragstellenden Personen über ein GUI die internetbasierte Neu-/Erstzulassung, Wiederzulassung, Umschreibung, Tageszulassung oder Außerbetriebsetzung anbieten. Die i-Kfz-Portale ermöglichen außerdem die vollautomatisierte Prüfung (aAB) der über die GUI oder über den KBA-Dienst Großkundenschnittstelle eingehenden Anträge inklusive der elektronischen Bereitstellung der jeweiligen Bescheide (bei Großkunden über die KBA-Dienste).

Ein i-Kfz-Portal kommuniziert im Rahmen des i-Kfz-Projekts ausschließlich mit den vom KBA hierzu bereitgestellten Diensten, sofern die KBA-Infrastruktur berührt wird. Von einem i-Kfz-Portal können weitere lokale Funktionalitäten genutzt werden, die aber keine primäre i-Kfz-Funktionalität darstellen (zum Beispiel e-Payment, elektronischer Identitätsnachweis oder indirekt am Zulassungsprozess beteiligte Verfahren) und mit Hilfe von Schnittstellen in Anspruch genommen werden.

Zusätzlich wird bei allen i-Kfz Zulassungsvorgängen immer eine Gebührenrückstandsprüfung vom i-Kfz-Portal initiiert. Dazu übermittelt das i-Kfz-Portal je nach Landesrecht eine Anfrage an die Zulassungsbehörde beziehungsweise an dessen Verfahren, ob das Gebührenkonto eines bestimmten Fahrzeughalters ausgeglichen ist. Nur wenn keine Gebührenrückstände vorhanden sind oder diese zum Beispiel mittels eines E-Payment-Systems des i-Kfz-Portals ausgeglichen werden, kann der Vorgang fortgesetzt werden, andernfalls ist er abzubrechen. Für die aAB werden gegebenenfalls noch weitere fachspezifische Prüfungen vom i-Kfz-Portal initiiert und von Sachbearbeitenden in der Zulassungsbehörde beziehungsweise den Fachverfahren der Zulassungsbehörde durchgeführt.

Hinweis: Nicht alle Zulassungsbehörden werden ein eigenes i-Kfz-Portal betreiben. Es können sich Cluster bilden, in denen mehrere Zulassungsbehörden ein i-Kfz-Portal, angeboten durch einen Diensteanbieter (zum Beispiel ein Landesrechenzentrum), gemeinsam nutzen. In solchen Fällen ist eine Mandantentrennung in Verbindung mit einer sicheren Virtualisierung bezogen auf die einzelnen Zulassungsbehörden innerhalb des Clusters erforderlich. Insbesondere sind eindeutige Zuständigkeiten im Bereich des Service Managements und der Administration sicherzustellen und zu dokumentieren.

5.1.5 Fachverfahren der Zulassungsbehörde

Ein Fachverfahren in einer Zulassungsbehörde stellt eine Anwendung dar, in der die Anträge auf Neu-/Erstzulassung, Wiederzulassung, Umschreibung, Tageszulassung oder Außerbetriebsetzung eines Fahrzeugs durch einen Mitarbeitenden der Zulassungsbehörde oder automatisiert bearbeitet werden.

Das Fachverfahren kommuniziert auf zweierlei Weise mit den KBA-Diensten:

- die im Rahmen des i-Kfz-Projekts gestellten Anträge (tAB) oder bei positiver Prüfung der i-Kfz-Portale die Entscheidung (aAB) 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 (bei GK auch den Gebührensammelbescheid und gegebenenfalls weitere Informationen für den GK) an das KBA (Kommunikationsverbindung: Fachverfahren → KBA-Dienste).

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

Ebenfalls kommuniziert das Fachverfahren auf zweierlei Weise mit dem i-Kfz-Portal:

- Die im Rahmen des i-Kfz-Projekts erforderliche Gebührenrückstandsprüfung und gegebenenfalls weitere fachspezifische Prüfungen werden vom i-Kfz-Portal initiiert (Kommunikationsverbindung: i-Kfz-Portal → Fachverfahren)
- Das Fachverfahren liefert die Ergebnisse der Prüfung an das i-Kfz-Portal zurück (Kommunikationsverbindung: Fachverfahren → i-Kfz-Portal)

Hinweis: Innerhalb der Zulassungsbehörden werden Fachverfahren unterschiedlicher Hersteller eingesetzt.

Es können auch Schnittstellen zwischen der antragstellenden Person und dem Fachverfahren der Zulassungsbehörde über das Internet existieren, zum Beispiel um einen Termin mit der Zulassungsbehörde zu vereinbaren, ein Wunschkennzeichnen zu reservieren oder auch die benötigten Eingaben im Vorwege zu erfassen (indirekt am Zulassungsprozess beteiligte Verfahren, siehe auch Antragstellende Person).

5.1.6 KBA-Dienste

Hierunter sind die folgenden vom KBA angebotenen Dienste zu verstehen:

- die Großkundenschnittstelle (ermöglicht beim KBA registrierten Großkunden die Antragsstellung per Maschine zu Maschine Kommunikation),
- die Kommunikationsplattform beziehungsweise das System für asynchronen, behördenübergreifenden Informations- und Nachrichtenaustausch – kurz „SABRINA“ (ermöglicht die elektronische Bereitstellung der Entscheidung der Zulassungsbehörde beziehungsweise des i-Kfz-Portals an den antragstellenden Großkunden)
- und unter anderem die Registerführung des ZFZR.

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

Hinweis: Es ist zu beachten, dass jegliche Kommunikation zwischen der antragstellenden Person oder des Großkunden und den Zulassungsbehörden im Rahmen des i-Kfz-Projekts über die i-Kfz-Portale oder den KBA-Dienst Großkundenschnittelle und über das KBA (hier die KBA-Dienste) erfolgen muss. Es ist nicht zulässig, dass antragstellende Personen, Großkunden oder die i-Kfz-Portale direkt über die Fachverfahren der Zulassungsbehörden mit dem KBA kommunizieren. Die Kommunikation der antragstellenden Personen, des Großkunden oder der i-Kfz-Portale mit den Fachverfahren ist nur für die Gebührenrückstandsprüfung, gegebenenfalls noch weitere Fachspezifische Prüfungen und indirekt am Zulassungsprozess beteiligte Verfahren erlaubt (siehe auch Antragstellende Person).

5.2 Technische Architektur des i-Kfz-Systems

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

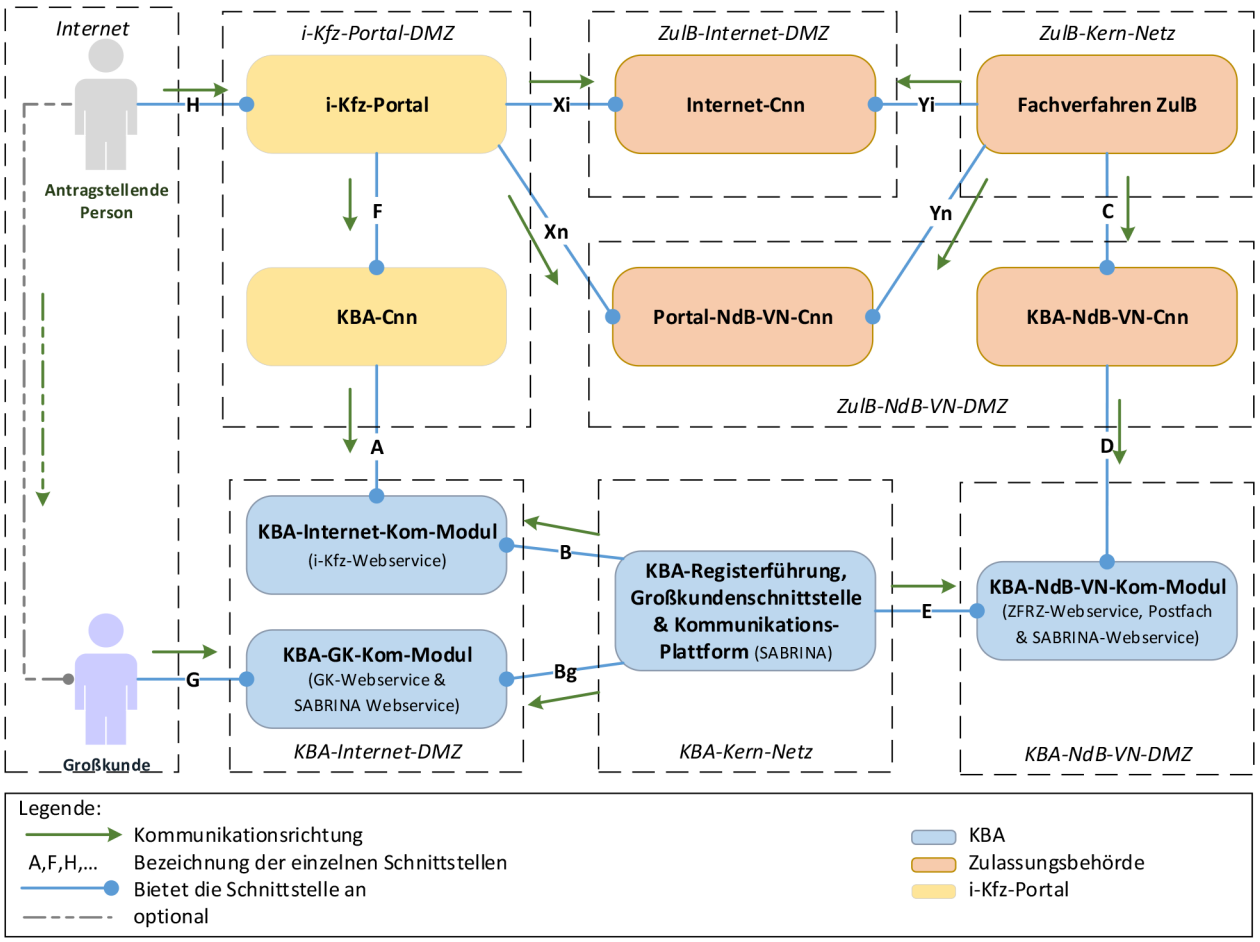

Abbildung 3: Technische Architektur des i-Kfz-Systems – das Gesamtbild

In den folgenden Kapiteln 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 in Nummer 6 beschrieben.

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

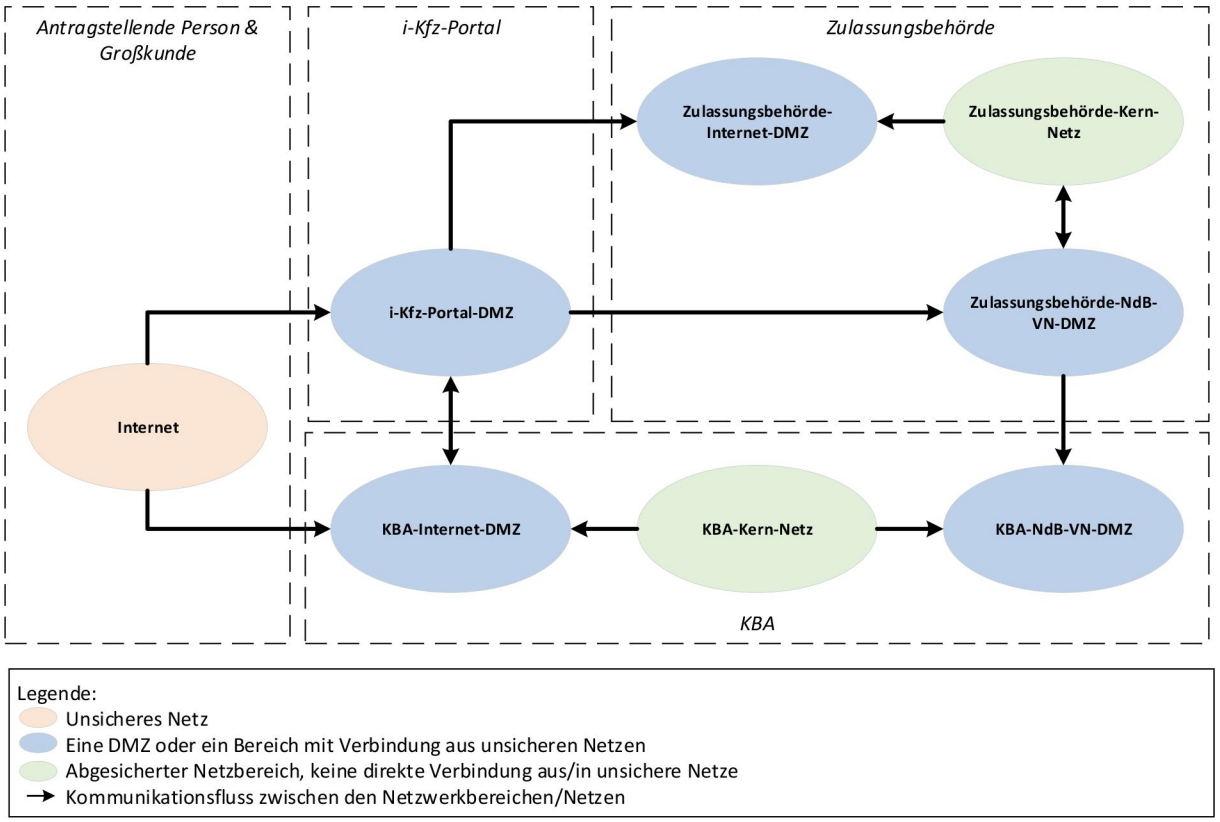

Abbildung 4: Netzwerkbereiche der definierten Architektur innerhalb i-Kfz

Hinweis: Gemäß BSI-ISI-LANA wird eine DMZ wie folgt definiert:

„Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird und sowohl von innen als auch von außen erreichbar ist. Die DMZ ist weniger stark gesichert als das interne Netz, dafür aber besser vom äußeren Netz aus erreichbar. Die DMZ dient der Schaffung eines zusätzlichen Sicherheitsbereichs für Dienste (zum Beispiel E-Mail, Web) oder Proxys, die von externen Netzen aus nutzbar sein sollen, aber aus Sicherheitsgründen nicht im internen Netz platziert werden dürfen."

Mindestanforderung an eine DMZ mit normalem Schutzbedarf ist 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 (vergleiche Nummer 5.4.1, „KBA-Internet-Kom-Modu" und Nummer 5.4.11 „KBA-GK-Kom-Modu").

5.3.2 KBA-Kern-Netz

Die Kerndienste des KBA (hier „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform", vergleiche Nummer 5.4.2) werden innerhalb des Netzwerkbereichs „KBA-Kern-Netz" angeboten. Bei der KBA-Registerführung handelt es sich insbesondere um das ZFZR. Das „KBA-Kern-Netz" stellt einen geschützten Bereich dar, der von externen Netzwerken durch die Verwendung der 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 (zum Beispiel Internet oder auch NdB-VN) zu eröffnen, ohne dass diese Verbindung über die korrespondierende DMZ (entsprechend „KBA-Internet-DMZ“ oder „KBA-NdB-VN-DMZ“) verläuft.

Die innerhalb dieses Segments untergebrachten Dienste können mit Hilfe eines Puffer-Mechanismus (zum Beispiel einer Nachrichtenschlange) mit den DMZ-Netzwerksegmenten kommunizieren.

5.3.3 KBA-NdB-VN-DMZ

Die Zulassungsbehörden kommunizieren bereits heute aus der Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ (vergleiche Nummer 5.4.6) heraus mit dem KBA über das Behördennetzwerk NdB-VN. Neben der Einhaltung der NdB-VN-Nutzerpflichten ist diese Kommunikation entsprechend den Anforderungen des KBAs abzusichern (siehe „Information zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden“ und „Standard für die Datenübermittlung an das Kraftfahrt-Bundesamt – Datenaustausch mit den Zulassungsbehörden“).

Für die Kommunikation zwischen KBA und Zulassungsbehörden mit Hilfe eines Postfachs wird auf die bereits implementierten Transport-Mechanismen zurückgegriffen.

5.3.4 i-Kfz-Portal-DMZ

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

Es sind eingehende Kommunikationsverbindungen der antragstellenden Person erlaubt. Eine direkte ausgehende Kommunikation ist nur in den Bereich „KBA-Internet-DMZ“ zulässig.

Zusätzlich ist eine indirekte Kommunikation in den Bereich „Zulassungsbehörde-Kern-Netz“ zulässig, welche ausschließlich über einen Nachrichtenpuffer (zum Beispiel einer Queue) erfolgen darf. Je nach Anbindung des i-Kfz-Portals kann diese Kommunikation entweder über die Komponente „Internet-Cnn“ und die „Zulassungsbehörde-Internet-DMZ“ oder über die Komponente „Portal-NdB-VN-Cnn“ und die „Zulassungsbehörde-NdB-VN-DMZ“ (die AnVN sind zu beachten) erfolgen.

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-NdB-VN-DMZ“ und „Zulassungsbehörde-Internet-DMZ“ hergestellt werden. Die Kommunikation in den Bereich „i-Kfz-Portal-DMZ“ über die „Zulassungsbehörde-NdB-VN-DMZ“ oder die „Zulassungsbehörde-Internet-DMZ“ erfolgt ausschließlich indirekt über einen Nachrichtenpuffer (zum Beispiel einer Queue).

5.3.6 Zulassungsbehörde-NdB-VN-DMZ

Die Komponenten, die die Kommunikation der Zulassungsbehörde mit dem KBA realisieren, werden im Bereich „Zulassungsbehörde-NdB-VN-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-NdB-VN-DMZ“ über das NdB-VN kommunizieren.

Des Weiteren darf die „Zulassungsbehörde-NdB-VN-DMZ“ auch für die Kommunikation mit „i-Kfz-Portal“ über das „NdB-VN“ genutzt werden. Die eingehende Kommunikation ist auch hier aus dem Bereich „Zulassungsbehörde-Kern-Netz“ und der ausgehende Datenverkehr in die „i-Kfz-Portal-DMZ“. Es handelt sich hier um die von den i-Kfz-Portalen ausgehende Kommunikation zur Zulassungsbehörde, die für die i-Kfz Abwicklung benötigt wird (zum Beispiel Gebührenrückstandsprüfung) oder für weitere Funktionen/Verfahren, die nicht zum Funktionsumfang von i-Kfz gehören (indirekt am Zulassungsprozess beteiligte Verfahren).

Die AnVN sind zu beachten.

Hinweis: Auch das jeweilige Landesnetz darf für die Kommunikation zwischen dem i-Kfz-Portal und den Fachverfahren beziehungsweise der Zulassungsbehörde genutzt werden, es gelten seitens des KBA die gleichen Anforderungen wie bei der Nutzung des NdB-VN und der Zulassungsbehörde-NdB-VN-DMZ.

5.3.7 Internet

Dieser Bereich umfasst die Komponenten der antragstellenden Person und des Großkunden.

5.3.8 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 i-Kfz-Portalen ausgehende Kommunikation zur Zulassungsbehörde, die für die i-Kfz Abwicklung benötigt wird (zum Beispiel Gebührenrückstandsprüfung) oder für weitere Funktionen/Verfahren, die nicht zum Funktionsumfang von i-Kfz gehören (indirekt am Zulassungsprozess beteiligte Verfahren).

Eine weitere Kommunikationsmöglichkeit in das Netzwerksegment „Zulassungsbehörde-Internet-DMZ“ hinein besteht aus dem abgesicherten Netzwerkbereich der Zulassungsbehörde „Zulassungsbehörde-Kern-Netz“. Der Datenaustausch zwischen den beiden Netzsegmenten erfolgt ausschließlich indirekt über eine Queue (Nachrichtenschlage).

Hinweis: Es ist zulässig, dass die beiden Bereiche „i-Kfz-Portal-DMZ“ und „Zulassungsbehörde-Internet-DMZ“ zusammengelegt werden, wenn dies organisatorisch möglich ist (zum Beispiel bei gleichem Betreiber). Die Anforderungen an beide Bereiche sind weiterhin zu erfüllen.

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-NdB-VN-DMZ“ existieren (Im Fall der Zusammenlegung der Bereiche „i-Kfz-Portal-DMZ“ und „Zulassungsbehörde-Internet-DMZ“ ist eine Verbindung entsprechend der der „i-Kfz-Portal-DMZ“ zur „Zulassungsbehörde-NdB-VN-DMZ“ unter Beachtung der AnVN zulässig).

5.4 Komponenten der Architektur innerhalb des i-Kfz-Systems

Die vorgestellten Netzwerkbereiche beinhalten System-Komponenten (vergleiche auch Abbildung 3), die über definierte Schnittstellen miteinander kommunizieren.

5.4.1 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 i-Kfz-Portale (vergleiche Nummer 5.5.1),

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

Die Kommunikation vom KBA an das „i-Kfz-Portal“ wird analog umgesetzt. Die ans „i-Kfz-Portal“ adressierten Nachrichten werden mithilfe der Schnittstelle B von der „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ über Schnittstelle k dem „i-Kfz-Portal“ an der Schnittstelle A zur Abholung gestellt.

Eine logische synchrone Kommunikation über die Kommunikationsverbindung „i-Kfz-Portal“ → „KBA-Internet-Kom-Modul“ → „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ wird physikalisch durch den asynchronen Ansatz (die Verwendung der Nachrichtenschlange) auf der Kommunikationsverbindung „KBA-Internet-Kom-Modul“ → „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ transparent für die aufrufende Instanz umgesetzt. Gleiches gilt für die logische synchrone Kommunikation über die Kommunikationsverbindung „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ → „KBA-Internet-Kom-Modul“ → „i-Kfz-Portal“.

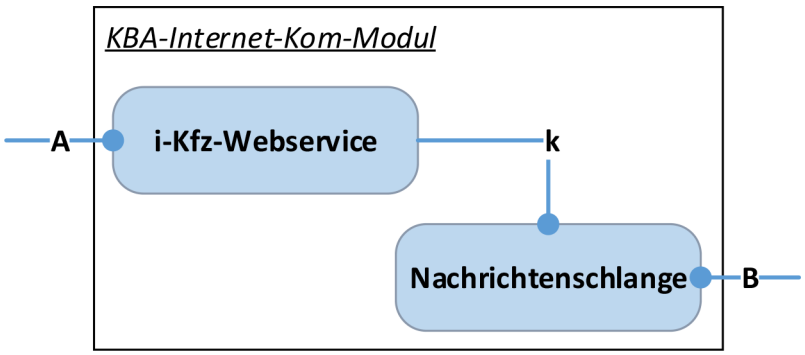

Abbildung 5: Interner Aufbau der Komponente „KBA-Internet-Kom-Modul“ (schematische Darstellung)

5.4.2 KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform

Unter der „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ werden Software-Komponenten (zum Beispiel Verarbeitungsmodule, Datenbanken, ZFZR et cetera) zusammengefasst, die innerhalb des Netzwerkbereichs „KBA-Kern-Netz“ in einer abgesicherten Umgebung ablaufen.

5.4.3 KBA-NdB-VN-Kom-Modul

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

Die eingehende Kommunikation von den Zulassungsbehörden wird mit Hilfe der Schnittstelle D (vergleiche Nummer 5.5.4) und von der „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ mit Hilfe der Schnittstelle E (vergleiche Nummer 5.5.5) entgegengenommen.

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

Das „KBA-NdB-VN-Kom-Modul“ wickelt die Kommunikation dabei für drei Anwendungsfälle ab, die teilweise bereits heute technisch implementiert sind und auch außerhalb der Funktionalität des i-Kfz-Projekts genutzt werden: (vergleiche Abbildung 6)[1]:

- Die Zugriffe der Zulassungsbehörden 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 diesem Fall werden die Nachrichten asynchron (durch die Zulassungsbehörden) abgeholt und die Antwortnachrichten abgelegt (Nachrichten von KBA an die ZulB) oder neue Nachrichten abgelegt und die Antwortnachrichten abgeholt (Nachrichten von der ZulB ans KBA).
- Die Zugriffe seitens der Zulassungsbehörde auf die Kommunikationsplattform (SABRINA-Webservice)

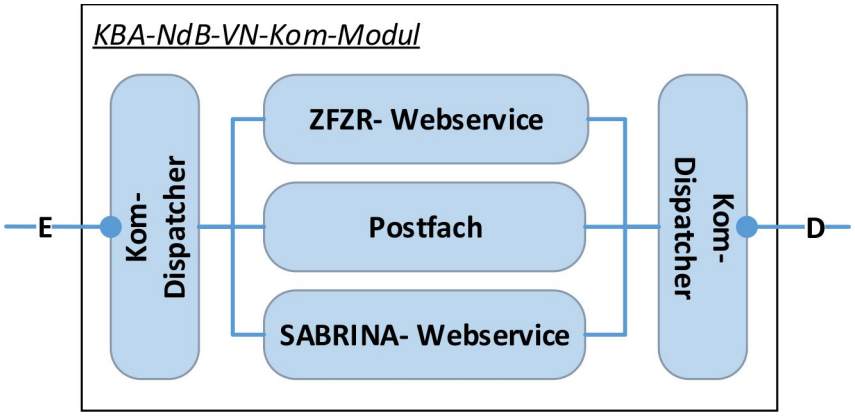

Abbildung 6: Interner Aufbau der Komponente „KBA-NdB-VN-Kom-Modul“

5.4.4 KBA-NdB-VN-Cnn

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

Das Modul bietet die Schnittstelle C (vergleiche Nummer 5.5.3) an, die durch die „Systeme der Fachverfahren der Zulassungsbehörde“ bedient wird. Weiterhin spricht die Komponente die vom KBA betriebene Kommunikationsgegenstelle („KBA-NdB-VN-Kom-Modul“) mit Hilfe der Schnittstelle D (vergleiche Nummer 5.5.4) an.

Das Modul „KBA-NdB-VN-Cnn“ bedient dabei drei Anwendungsfälle:

- Bereits heute implementierter Zugriff seitens der Zulassungsbehörden auf den ZFZR-Webservice,
- Der im Rahmen von i-Kfz verwendete Zugriff auf das Postfach (vergleiche Nummer 5.4.3),
- Den Zugriff seitens der Zulassungsbehörde auf die Kommunikationsplattform (SABRINA-Webservice).

5.4.5 Portal-NdB-VN-Cnn

Dieses Modul stellt eine sichere Kommunikationsschnittstelle zwischen den „Systemen der Fachverfahren der Zulassungsbehörde“ und dem „i-Kfz-Portal“ über sichere Netze (insbesondere NdB-VN) her.

Das Modul wird für die indirekte Kommunikation über das NdB-VN zwischen den Komponenten „Systeme der Fachverfahren der Zulassungsbehörde“ und „i-Kfz-Portal“ über einen Nachrichtenpuffer (zum Beispiel einer Queue) genutzt, als Alternative zur Kommunikation über die Komponente „Internet-Cnn“ mit den Schnittstellen Xi und Yi. Die Komponente bietet zwei Schnittstellen an:

- Schnittstelle Xn – über diese Schnittstelle wird die aus dem Internet kommende Kommunikation entgegengenommen (vergleiche Nummer 5.5.10),
- Schnittstelle Yn – 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 Nummer 5.5.11).

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

5.4.6 Systeme der Fachverfahren der Zulassungsbehörde

Die Komponente „Systeme der Fachverfahren der Zulassungsbehörde“[2] in der Zulassungsbehörde wird in dem sicheren Bereich „Zulassungsbehörde-Kern-Netz“ betrieben. Die Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ bietet keine Schnittstellen an, sondern bedient die von der Komponente „KBA-NdB-VN-Cnn“ angebotene Schnittstelle C (vergleiche Nummer 5.5.3), die von der Komponente „Internet-Cnn“ angebotene Schnittstelle Yi (vergleiche Nummer 5.5.9) und/oder die von der Komponente „Portal-NdB-VN-Cnn“ angebotene Schnittstelle Yn (vergleiche Nummer 5.5.11).

Die Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ ist immer eine Kommunikation initiierende Instanz und darf keine Kommunikationsanfragen entgegennehmen, auch nicht von den indirekt am Zulassungsprozess beteiligten Verfahren (gemäß § 19 Absatz 2 FZV).

5.4.7 i-Kfz-Portal

Die Komponente „i-Kfz-Portal“ bietet der „antragstellenden Person“ die Schnittstelle H (vergleiche Nummer 5.5.7) an und bedient die von der Komponente „KBA-Cnn“ (vergleiche Nummer 5.4.8) angebotene Schnittstelle F (vergleiche Nummer 5.5.6), über die die an das KBA oder vom KBA an das „i-Kfz-Portal“ adressierten Nachrichten weitergeleitet werden.

Außerdem bedient es die von der Komponente „Internet-Cnn“ angebotene Schnittstelle Xi (vergleiche Nummer 5.5.8) und/oder die von der Komponente „Portal-NdB-VN-Cnn“ angebotene Schnittstelle Xn (vergleiche Nummer 5.5.10), über welche die logische (indirekte) Kommunikation über eine Nachrichtenschlange zu den „Systemen der Fachverfahren der Zulassungsbehörde“ abgebildet ist.

Unter der Komponente „i-Kfz-Portal“ werden auch die Portale eingeschlossen, welche die indirekt am Zulassungsprozess beteiligten Verfahren (gemäß § 19 Absatz 2 FZV) wie zum Beispiel Wunschkennzeichen implementieren und die auch über das Internet erreichbar sind.

5.4.8 KBA-Cnn

Die Komponente „KBA-Cnn“ realisiert die Kommunikation zwischen einem „i-Kfz-Portal“ und dem KBA über die Komponente „KBA-Internet-Kom-Modul“ durch Aufbau einer gesicherten Virtual Private Network(VPN)-Verbindung. Die Kommunikation wird stets vom „i-Kfz-Portal“ über die „KBA-Cnn“ initiiert.

Der „KBA-Cnn“ bietet die Schnittstelle F (vergleiche Nummer 5.5.6) gegenüber dem „i-Kfz-Portal“ an, nimmt darüber die Nachrichten des „i-Kfz-Portal“ entgegen und leitet diese im nächsten Schritt an das „KBA-Internet-Kom-Modul“ über die Schnittstelle A (vergleiche Nummer 5.5.1) weiter. Der „KBA-Cnn“ holt ebenfalls über die vom „KBA-Internet-Kom-Modul“ über die Schnittstelle A bereitgestellten Nachrichten ab und leitet diese über die Schnittstelle F an das „i-Kfz-Portal“ weiter beziehungsweise stellt diese bereit.

5.4.9 Schnittstelle Antragstellende Person

Die Antragstellende Person möchte mit Hilfe der i-Kfz-Portale eine Kfz-Angelegenheit abwickeln. Dazu nutzt sie eine GUI, die über einen Browser bedient werden kann. Die Kommunikation wird durch die Schnittstelle H (vergleiche Nummer 5.5.7) charakterisiert.

5.4.10 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 Xi – über diese Schnittstelle wird die aus dem Internet kommende Kommunikation entgegengenommen (vergleiche Nummer 5.5.8),
- Schnittstelle Yi – 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 Nummer 5.5.9).

Die beispielhafte schematische Darstellung der Komponente „Internet-Cnn“ ist in der Abbildung 7 abgebildet. Die logisch synchrone Kommunikation zwischen den Komponenten „i-Kfz-Portal“ und „Systeme der Fachverfahren der Zulassungsbehörde“ wird über folgende asynchrone Teilschritte abgebildet:

- Die interne Komponente „Internet-Server“ nimmt die Nachrichten (Anfragen) über die äußere Schnittstelle Xi entgegen (zum Beispiel von der Komponente „i-Kfz-Portal“) und speichert diese über die interne Schnittstelle j in einem Nachrichtenpuffer (zum Beispiel einer Queue),
- Die Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ greift über die Schnittstelle Yi auf den Nachrichtenpuffer zu, liest die strukturierten Inhalte aus und prüft ihre Semantik. Anschließend holt sie die wartenden Nachrichten ab.

[2] Der Name „Systeme der Fachverfahren der Zulassungsbehörde“ wurde stellvertretend gewählt und steht für alle für die Zulassungszwecke von den Zulassungsbehörden verwendeten Fachverfahren unterschiedlicher Hersteller. Damit ist keine besondere Fachanwendung gemeint.

- Die abgeholten Nachrichten werden durch die Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ verarbeitet und die generierten Antwortnachrichten werden über die Schnittstelle Yi 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 Xi ankamen.

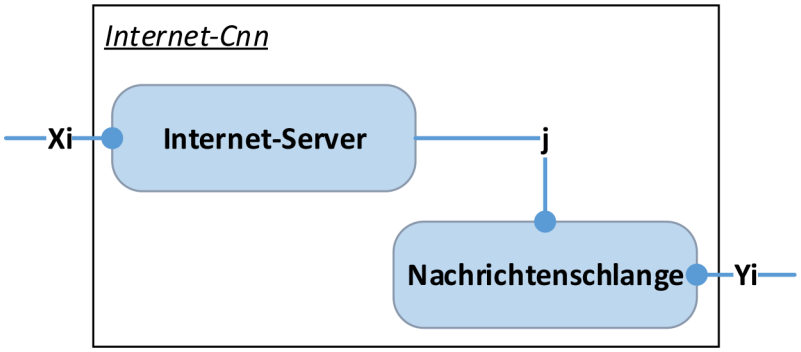

Abbildung 7: Schematische Darstellung des internen Aufbaus der Komponente „Internet-Cnn“

Hinweis: Die indirekt am Zulassungsprozess beteiligten Verfahren (gemäß § 19 Absatz 2 FZV), die über das Internet erreichbar sind, sind auch über die Schnittstelle Xi anzubinden.

5.4.11 KBA-GK-Kom-Modul

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

- Schnittstelle G – erreichbar aus dem Internet durch die Großkunden beziehungsweise dessen Systeme (vergleiche Nummer 5.5.12),
- Schnittstelle Bg – erreichbar nur aus dem Intranet des KBA („KBA-Kern-Netz“), (vergleiche Nummer 5.5.2).

Der interne Aufbau entspricht der Komponente „KBA-Internet-Kom-Modul“ und ist der Abbildung 8 zu entnehmen. Das Modul nimmt die über die Schnittstelle G eingehenden Nachrichten entgegen und speichert diese über eine interne Schnittstelle kg in einer Nachrichtenschlange, bis die Nachrichten über die Schnittstelle Bg abgeholt werden. Die über die Schnittstelle Bg zurückgeschriebenen Antworten werden über die interne Schnittstelle kg abgeholt und dann über die Schnittstelle G an die aufrufende Instanz als Antwort auf die Anfrage zurückgeschickt.

Die Kommunikation vom KBA zum Großkunden beziehungsweise dessen Systeme wird analog umgesetzt. Die an den Großkunden beziehungsweise dessen Systeme adressierten Nachrichten werden mithilfe der Schnittstelle Bg von der „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ über Schnittstelle kg den Großkunden beziehungsweise dessen Systeme an der Schnittstelle G zur Abholung bereitgestellt.

Eine logisch synchrone Kommunikation über die Kommunikationsverbindung Großkunden beziehungsweise dessen Systeme → „KBA-GK-Kom-Modul“ → „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ wird physikalisch durch den asynchronen Ansatz (die Verwendung der Nachrichtenschlange) auf der Kommunikationsverbindung „KBA-GK-Kom-Modul“ → „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ transparent für die aufrufende Instanz umgesetzt. Gleiches gilt für die logisch synchrone Kommunikation über die Kommunikationsverbindung „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ → „KBA-GK-Kom-Modul“ → Großkunden beziehungsweise dessen Systeme.

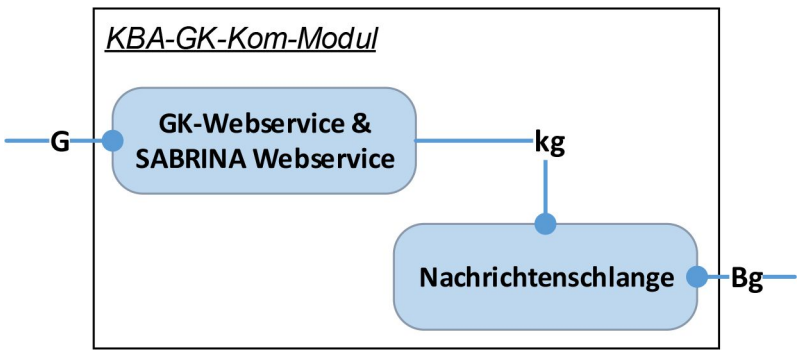

Abbildung 8: Interner Aufbau der Komponente „KBA-GK-Kom-Modul“ (schematische Darstellung)

5.5 Schnittstellen der Architektur innerhalb des i-Kfz-Systems

Die in Nummer 5.4 vorgestellten Komponenten der Architektur werden über definierte Schnittstellen angesprochen, 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 der Komponente „i-Kfz-Portal“ (über das Modul „KBA-Cnn“, vergleiche Abbildung 9) genutzt.

Hinweis: Die detaillierte technische Spezifikation der Schnittstelle ist in der seitens des KBAs zur Verfügung gestellten Information für Softwareanbieter zu finden.

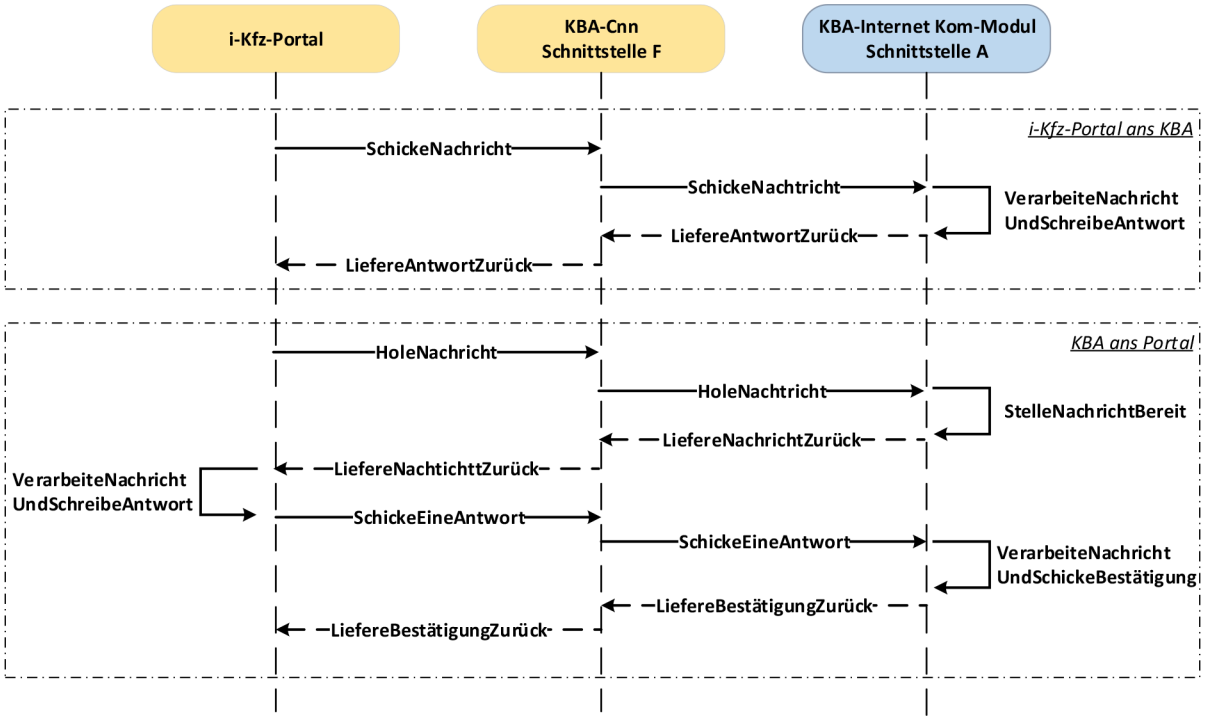

Abbildung 9: Verwendung der Schnittstelle A durch ein i-Kfz-Portal

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

Ebenfalls stellt die Schnittstelle A die für die Verarbeitung durch ein „i-Kfz-Portal“ gedachten Nachrichten dem „i-Kfz-Portal“ über die „KBA-Cnn“ zur Abholung bereit und nimmt dessen Antworten entgegen.

Die Kommunikation wird immer vom „i-Kfz-Portal“ über die „KBA-Cnn“ initiiert. Die Schnittstelle ist mit Hilfe der Webservice-Technologie (WS-Technologie) realisiert und bietet die, im Rahmen des i-Kfz-Projekts entwickelten, i-Kfz-Webservices an.

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

Die Nachrichten werden in einem vom KBA definierten Extensible Markup Language (XML)-Format realisiert. Entsprechende Schemadateien und WS-Beschreibungen sind im geschützten Bereich der KBA-Homepage veröffentlicht. Der „Standard für die Datenübermittlung an das Kraftfahrt-Bundesamt – Datenaustausch mit i-Kfz-Portalen“ ist einzuhalten.

5.5.2 Schnittstelle B & Bg

Bei der Schnittstelle B handelt es sich um eine Schnittstelle, die vom „KBA-Internet-Kom-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, Großkundenschnittstelle & Kommunikationsplattform“ aus dem „KBA-Kern-Netz“ greift auf diese Schnittstellen zu, um die für diese Komponenten bestimmten Nachrichten abzuholen. Die Schnittstelle Bg wird vom „KBA-GK-Kom-Modul“ angeboten und entspricht im funktionalen Verhalten der Schnittstelle B.

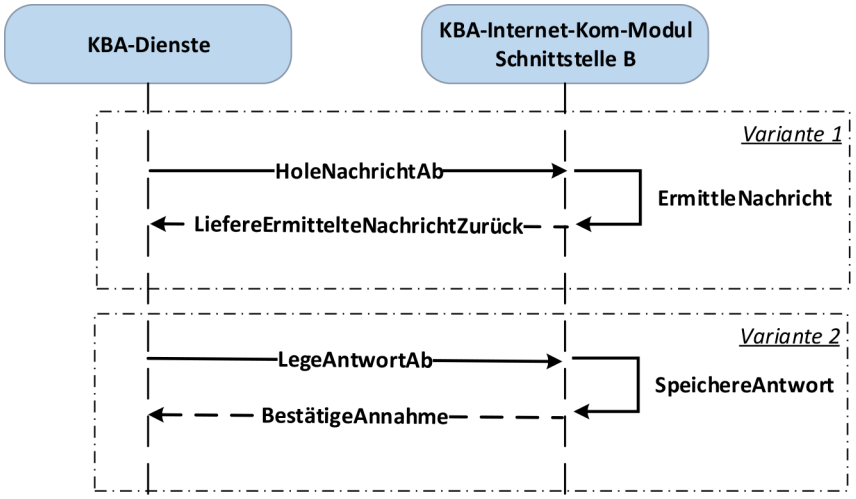

Abbildung 10: Verwendung der Schnittstelle B

Die Schnittstellen an sich werden im synchronen Modus betrieben, realisieren aber einen asynchronen Zugriff zwischen den Komponenten „KBA-Internet-Kom-Modul“ beziehungsweise „KBA-GK-Kom-Modul“ und der „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“.

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 der Zulassungsbehörde“ und „KBA-NdB-VN-Cnn“ und wird von der Komponente „KBA-NdB-VN-Cnn“ angeboten. Die aus der Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ 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 gleichbehandelt werden:

- Abschicken einer Nachricht aus der Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ an das KBA und Empfang einer Antwort – die Nachricht ist innerhalb der Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ erstellt worden und wird dann synchron an das KBA verschickt. Die zeitnah generierte Antwort seitens des KBAs wird an die Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ als Rückgabewert zurückgeliefert (vergleiche Abbildung 11 – Variante 1),
- Abholen einer Nachricht des KBAs an die Zulassungsbehörde und Ablegen einer Antwort durch die Zulassungsbehörde. In diesem Fall wird die Kommunikation seitens der Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ initiiert. Die Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ holt im ersten Schritt (erster Aufruf, vergleiche Abbildung 11 – Variante 2) die für sie bestimmte Nachricht ab, verarbeitet diese und legt gegebenenfalls die erzeugte Antwort an das KBA (zweiter Aufruf, vergleiche Abbildung 11 – Variante 3) ab.

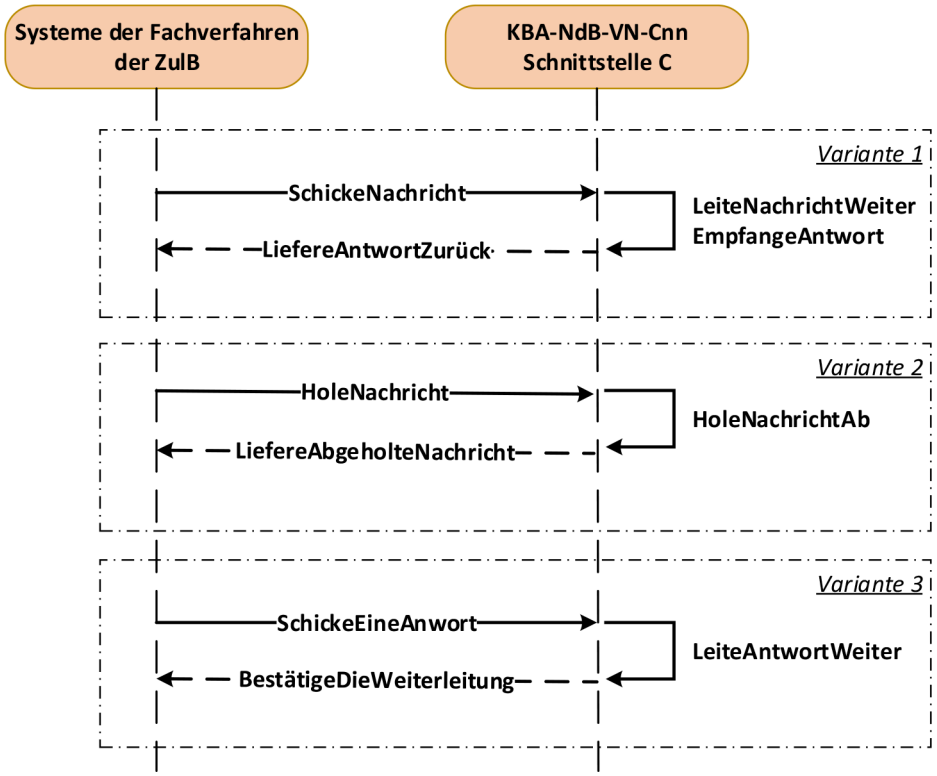

Abbildung 11: Verwendung der Schnittstelle C

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

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

Die im Rahmen des i-Kfz-Projekts ausgetauschten Nachrichten sind in einem vom KBA festgelegten XML-Format implementiert. Der „Standard für die Datenübermittlung an das Kraftfahrt-Bundesamt – Datenaustausch mit den Zulassungsbehörden“ ist einzuhalten.

5.5.4 Schnittstelle D

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

Es werden beide zur Schnittstelle C beschriebenen Kommunikationsmodi unterstützt.

5.5.5 Schnittstelle E

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

Analog der Schnittstelle B und Bg ist diese Schnittstelle synchron implementiert, realisiert aber eine asynchrone Kommunikation zwischen den Komponenten „KBA-Registerführung, Großkundenschnittstelle & Kommunikationsplattform“ und „KBA-NdB-VN-Kom-Modul“.

5.5.6 Schnittstelle F

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

Es handelt sich um 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 „i-Kfz-Portal“ darstellt. In dem Fall ist die Komponente „KBA-Cnn“ in die Komponente „i-Kfz-Portal“ integriert.

5.5.7 Schnittstelle H

Der Zugriff durch die Antragstellende Person auf ein i-Kfz-Portal wird durch die Schnittstelle H beschrieben. Die Schnittstelle H ist mit Hilfe der Web-Technologie realisiert und wird über einen Browser durch die Antragstellende Person bedient.

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

5.5.8 Schnittstelle Xi

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

Die Schnittstelle Xi, zwischen den Komponenten „i-Kfz-Portal“ und „Internet-Cnn“ aus den Bereichen „i-Kfz-Portal-DMZ“ und respektive „Zulassungsbehörde-Internet-DMZ“, realisiert einen Kommunikationskanal, der für die Prüfung der Gebührenrückstände, gegebenenfalls noch weitere fachspezifische Prüfungen und die indirekt am Zulassungsprozess beteiligten Verfahren verwendet werden kann. Die Anfragen werden dabei vom „i-Kfz-Portal“ abgesetzt und durch das involvierte Fachverfahren der Zulassungsbehörde beantwortet. Auf die Schnittstelle Xi wird über das unsichere Netz (hier Internet) zugegriffen. Die indirekt am Zulassungsprozess beteiligten Verfahren, die über das Internet erreichbar sind, sind ebenfalls über die Schnittstelle Xi anzubinden.

Hinweis: Die Anbindung des i-Kfz-Portals an die Fachverfahren der ZulB kann über die Schnittstellen Xn/Yn ODER Xi/Yi erfolgen. Eine redundante Anbindung ist nicht vorgesehen beziehungsweise erforderlich.

5.5.9 Schnittstelle Yi

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

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

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 Yi in den Bereich „Zulassungsbehörde-Kern-Netz“ direkt initiiert werden kann.

Die Schnittstelle Yi, zwischen den Komponenten „Systeme der Fachverfahren der Zulassungsbehörde“ und „Internet-Cnn“ aus den Bereichen „Zulassungsbehörde-Kern-Netz“ und respektive „Zulassungsbehörde-Internet-DMZ“, realisiert einen Kommunikationskanal, der im Rahmen des i-Kfz-Verfahrens für die Prüfung der Gebührenrückstände, gegebenenfalls noch weitere fachspezifische Prüfungen und die Kommunikation zwischen den i-Kfz-Portalen und den Fachverfahren verwendet werden kann. Die Anfragen werden dabei vom i-Kfz-Portal abgesetzt und durch das involvierte Verfahren der Zulassungsbehörde beantwortet. Die Schnittstelle ist auch von den indirekt am Zulassungsprozess beteiligten Verfahren, die über das Internet erreichbar sind, zu nutzen (siehe Nummer 5.1).

5.5.10 Schnittstelle Xn

Die Kommunikation zwischen den Komponenten „i-Kfz-Portal“ und „Portal-NdB-VN-Cnn“ wird über die Schnittstelle Xn realisiert. Der Initiator der Kommunikation ist dabei stets die Komponente „i-Kfz-Portal“. Die eingehenden Nachrichten werden von der Komponente „Portal-NdB-VN-Cnn“ entgegengenommen und die Antworten an die aufrufende Instanz in einem synchronen Modus zurückgeliefert.

Die Schnittstelle Xn, zwischen den Komponenten „i-Kfz-Portal“ und „Portal-NdB-VN-Cnn“ aus den Bereichen „i-Kfz-Portal-DMZ“ und respektive „Zulassungsbehörde-NdB-VN-DMZ“, realisiert einen Kommunikationskanal, der im Rahmen des i-Kfz-Verfahrens für die Prüfung der Gebührenrückstände, gegebenenfalls noch weitere fachspezifische Prüfungen und die Kommunikation zwischen den i-Kfz-Portalen und Fachverfahren verwendet werden kann. Die Anfragen werden dabei vom i-Kfz-Portal abgesetzt und durch das involvierte Fachverfahren der Zulassungsbehörde beantwortet.

Hinweis: Die Anbindung des i-Kfz-Portals an die Fachverfahren der ZulB kann über die Schnittstellen Xn/Yn ODER Xi/Yi erfolgen. Eine redundante Anbindung ist nicht vorgesehen beziehungsweise erforderlich.

5.5.11 Schnittstelle Yn

Die Komponente „Portal-NdB-VN-Cnn“ speichert die eingehenden Nachrichten von der Komponente „i-Kfz-Portal“ zwischen. Diese Nachrichten können dann von der Komponente „Systeme der Fachverfahren der Zulassungsbehörde“ über die Schnittstelle Yn abgerufen werden.

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-NdB-VN-DMZ“ über die Schnittstelle Yn in den Bereich „Zulassungsbehörde-Kern-Netz“ direkt initiiert werden kann.

Die Schnittstelle Yn, zwischen den Komponenten „Systeme der Fachverfahren der Zulassungsbehörde“ und „Portal-NdB-VN-Cnn“ aus den Bereichen „Zulassungsbehörde-Kern-Netz“ und respektive „Zulassungsbehörde-NdB-VN-DMZ“, realisiert einen Kommunikationskanal, der im Rahmen des i-Kfz-Verfahrens für die Prüfung der Gebührenrückstände, gegebenenfalls noch weitere fachspezifische Prüfungen und die Kommunikation zwischen den i-Kfz-Portalen und Fachverfahren verwendet werden kann. Die Anfragen werden dabei vom i-Kfz-Portal abgesetzt und durch das involvierte Verfahren der Zulassungsbehörde beantwortet.

5.5.12 Schnittstelle G

Die Großkunden greifen aus dem „Internet“ auf die Schnittstelle G zu, um Anträge an die KBA-Infrastruktur zu übermitteln oder für sie bestimmte Nachrichten abzuholen. Die Schnittstelle G wird vom „KBA-GK-Kom-Modul“ angeboten und ermöglicht eine Maschine zu Maschinen Kommunikation unter Einhaltung der „Standards für die Datenübermittlung zur Nutzung der Großkundenschnittstelle für Großkunden“.

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

6 Abgeleitete Sicherheitsanforderungen

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

Jede Anforderung besteht aus vier Teilen:

- ID – die im Rahmen dieses Dokuments 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 (zum Beispiel erhält die zweite Anforderung, die in Nummer 6.2.6 beschrieben ist, die folgende ID: A-6.2.6-2),
- Anforderungstitel,
- Verpflichtungsgrad (VG),
- Anforderungsbeschreibung.

ID	Anforderungstitel	VG

Anforderungsbeschreibung

Der Verpflichtungsgrad einer Anforderung kann einen der folgenden Werte annehmen:

- „muss“ – eine „muss“-Anforderung ist unbedingt zu erfüllen,
- „soll“ – eine „soll“-Anforderung muss normalerweise erfüllt werden, es kann aber Gründe geben, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und im Falle einer Nichterfüllung stichhaltig begründet und dokumentiert werden.
- „kann“ – ist eine optionale Anforderung.

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

6.1 Allgemeine Sicherheitsanforderungen

In diesem Kapitel werden die allgemeinen Sicherheitsanforderungen beschrieben. Diese müssen von allen Beteiligten eingehalten werden, die das i-Kfz-Portal, das Fachverfahren und/oder die indirekt am Zulassungsprozess beteiligten Verfahren (zum Beispiel zur Wunschkennzeichenreservierung oder Terminvereinbarung in der Zulassungsstelle) betreiben. Ausgenommen davon ist A-6.1-1, diese Anforderung muss nur vom Betreiber des i-Kfz-Portals erfüllt werden.

Hinweis: Die indirekt am Zulassungsprozess beteiligten Verfahren zum Beispiel zur Wunschkennzeichenreservierung oder Terminvereinbarung in der Zulassungsstelle sind oft funktional im jeweiligen Bürgerportal integriert.

A-6.1-1	Kommunikationswege zwischen i-Kfz-Portalen und dem KBA	muss

Die Kommunikation zwischen den i-Kfz-Portalen und dem KBA muss über die vom KBA angebotene Schnittstelle A erfolgen. Gleiches gilt für die Kommunikation zwischen den i-Kfz-Portalen und dem Großkunden, auch diese muss über das KBA und die 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 potenziellen Angriffen aufweisen zu können. Es handelt sich dabei um die folgenden Komponenten aus der Architektur:

- „i-Kfz-Portal“ (vergleiche Nummer 5.4.7) inklusive „KBA-Cnn“, insbesondere im Hinblick auf die Implementierung der Schnittstellen H und F sowie die Verwendung der Schnittstelle F, Xi und Xn
- „Systeme der Fachverfahren“ (vergleiche Nummer 5.4.6) inklusive „KBA-NdB-VN-Cnn“, „Portal-NdB-VN-Cnn“ und „Internet-Cnn“, insbesondere in Bezug auf die Implementierung und Verwendung der Schnittstellen C, Xi, Xn, Yi und Yn und die Verwendung der Schnittstellen D
- „indirekt am Zulassungsprozess beteiligte Verfahren“ (sofern vorhanden), zum Beispiel Wunschkennzeichenreservierung oder Terminvereinbarung (siehe auch § 19 FZV).

Zur Bestätigung der erfolgreichen Härtung müssen Penetrationstests entsprechend der Nummer 7.4 durchgeführt werden. Die Tests müssen immer von fachlich qualifizierten Personen durchgeführt werden, die unabhängig von den untersuchten Bereichen sind und die nicht bei Konzeption, Aufbau oder Betrieb des untersuchten Informationsverbundes mitgewirkt haben. Eine Durchführung zum Beispiel durch die Anwendungsentwicklung, Betreiber oder betriebsverantwortlichen Personen ist nicht zulässig. Das beauftragte Unternehmen muss in dem Umfeld etabliert sein (zum Beispiel durch Fachpublikation, vergleichbare Referenzen von Kunden). Empfehlung: Einsatz von BSI-zertifizierten IT-Sicherheitsdienstleistern für IS-Penetrationstests.

Die gefundenen Mängel müssen schnellstmöglich behoben werden:

- Die Beseitigung der im Schadenspotential als „mittel“ oder „höher“ eingestuften Mängel müssen dem KBA durch eine erfolgreiche Nachprüfung durch einen qualifizierten unabhängigen Dritten (dieser kann auch die vorangegangenen Tests durchgeführt haben) unaufgefordert nachgewiesen werden.
- Die Beseitigung der weiteren Mängel (Schadenspotential unter „mittel“) sind dem KBA ebenfalls unaufgefordert schriftlich zu bestätigen.

Die Einzelheiten des Vorgehens, insbesondere die Form und der Umfang der Mitteilung an das KBA, werden durch das Zulassungsverfahren geregelt (vergleiche Nummer 7 „Zulassungsverfahren für die Anbindung an die KBA-Infrastruktur“).

A-6.1-3	Organisatorische Sicherheit	muss

Es müssen mindestens folgende organisatorische Maßnahmen konzipiert und umgesetzt werden:

Von der Leitungsebene muss ein Informationssicherheitsbeauftragter (ISB) für mindestens die im Punkt A-6.1-8 aufgeführten Komponenten benannt werden.[3] Die Gesamtverantwortung muss von der Institutionsleitung übernommen werden.

Ein Informationssicherheitsmanagementsystem (ISMS) muss für mindestens die im Punkt A-6.1-8 aufgeführten Komponenten etabliert und implementiert werden.

A-6.1-4	Fachkunde und Zuverlässigkeit des Personals	muss

Die Fachkunde und Zuverlässigkeit des eingesetzten Personals müssen gewährleistet werden.

Der Betreiber der Komponenten „i-Kfz-Portal“ inklusive „KBA-Cnn“, „Systeme der Fachverfahren“ inklusive „KBA-NdB-VN-Cnn“, Portal-NdB-VN-Cnn“ und „Internet-Cnn“ und der „indirekt am Zulassungsprozess beteiligten Verfahren“ muss die erforderliche Fachkunde und Zuverlässigkeit nachweisen. In diesem Zusammenhang ist von besonderer Wichtigkeit, dass die Mitarbeitenden im ausreichenden Maße geschult sind.

Eine Schulung muss insbesondere eine Einarbeitung/Einweisung in die implementierten Funktionalitäten als auch eine Sensibilisierung hinsichtlich der sicherheitsrelevanten sowie datenschutzrechtlichen Aspekte der Anwendung sowie die Erkennung und das Verhalten bei Sicherheitsvorfällen 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 geltenden 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,

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

„KBA-NdB-VN-Cnn“ – Implementierung des NdB-VN-Zugangs mit PrivateWire/Open File Transfer (OpenFT)/Log-FT in die KBA-Infrastruktur,

„Internet-Cnn“ – Implementierung des Zugangs über das Internet zum Zulassungsbehörde-Kern-Netz

„Portal-NdB-VN-Cnn“ – Implementierung des NdB-VN-Zugangs zum Zulassungsbehörde-Kern-Netz

darf nur autorisierten Personen gewährt werden.

Es sind räumliche und organisatorische Maßnahmen mindestens für die kritischen Komponenten zu treffen und im Zutrittskonzept zu dokumentieren, wie die diese umsetzen werden.

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 i-Kfz-Portals muss netztechnisch (zum Beispiel durch Einsatz geeigneter Paketfilter) von anderen angebotenen Anwendungen des Betreibers separiert werden.

Das Einspielen aktueller, stabiler Sicherheitspatches und -updates und die netztechnische Absicherung der Komponenten (zum Beispiel durch Verwendung von Paketfiltern, Application Layer Gateways et cetera) 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 (zum Beispiel Internet et cetera) ausgesetzt sind:

„i-Kfz-Portal“ inklusive „KBA-Cnn“,

„KBA-Internet-Kom-Modul“,

„Systeme der Fachverfahren der Zulassungsbehörde“,

„Internet-Cnn“,

„Portal-NdB-VN-Cnn“,

und „indirekt am Zulassungsprozess beteiligte Verfahren“ (sofern vorhanden).

Die Vorgaben und Empfehlungen des BSI, insbesondere zum Thema „sicheres Bereitstellen von Web-Angeboten“ gemäß BSI-ISI-WEB-SVR müssen beachtet und umgesetzt werden. Die Regelungen zur Umsetzung der Maßnahmen sowie die Verantwortlichen für die Umsetzung und der dazugehörige Managementprozess müssen innerhalb des Informationssicherheitskonzepts (vergleiche auch Anforderung A-6.1-8) dargestellt werden.

Hinweis: Im Rahmen dieses Dokuments gilt folgende Definition des Begriffs „Sicherheitsvorfall“.

Als Sicherheitsvorfall wird im Rahmen dieses Dokuments ein Ereignis verstanden, das die Vertraulichkeit, Verfügbarkeit und/oder Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme beziehungsweise IT-Anwendungen, die innerhalb des i-Kfz-Projekts zum Einsatz kommen, derart beeinträchtigt, dass ein größerer Schaden für mindestens einen der beteiligten Akteure entstehen kann.

A-6.1-7	Incident Management	muss

Ein tragfähiges Incident Management zum Erkennen, Bearbeiten und Lösen von Sicherheitsvorfällen muss konzipiert (ein Incident-Management-Konzept erstellt) und eingeführt/implementiert werden, insbesondere im Hinblick auf den Umgang mit:

Informationssicherheitsvorfällen,

Patching-Policy.

Das Konzept muss insbesondere die Reaktion auf gemeldete Schwachstellen und 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 (vergleiche Nummer 5) müssen einer Informationssicherheitskonzeption unterzogen werden, die sich am BSI-ITG-200-2 IT-Grundschutz[4] orientiert. Dafür kann die Vorgehensweise Kern-Absicherung oder Standard-Absicherung gewählt werden.

Insbesondere folgende Komponenten müssen betrachtet werden:

„i-Kfz-Portal“,

„KBA-Cnn“,

„Internet-Cnn“,

„Systeme der Fachverfahren der Zulassungsbehörde“,

[4] Die Nummer 3.2 des Umsetzungsplans der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ UP-LIöV fordert: „Bei der Planung, Aufbau und Anpassung Ebenen übergreifender IT-Verfahren ist der IT-Grundschutz des BSI in seiner jeweils gültigen Fassung anzuwenden. ... Für die tatsächliche Umsetzung des IT-Grundschutzes wird durch den Verantwortlichen für das IT-Verfahren ein geeigneter Nachweis (gegebenenfalls qualifizierte Eigenauskunft/Grundschutz Testat/Zertifikat) geführt“.

„KBA-NdB-VN-Cnn“,

„Portal-NdB-VN-Cnn“,

und „indirekt am Zulassungsprozess beteiligte Verfahren“ (sofern vorhanden).

A-6.1-9	Kommunikation zwischen den Komponenten	muss

Jede Komponente muss über die ihr im Rahmen der Architektur (vergleiche Nummer 5) zugeordneten Komponenten kommunizieren.

Es muss verhindert werden, dass eine direkte Weiterleitung von Nachrichten aus dem Netzwerkbereich „Zulassungsbehörde-Internet-DMZ“ über die Komponente „Systeme der Fachverfahren“ (im Netzwerkbereich „Zulassungsbehörde-Kern-Netz“) in den Netzwerkbereich „Zulassungsbehörde-NdB-VN-DMZ“ (eine Art von 1-zu-1-Weiterleitung) erfolgt.

A-6.1-10	Demilitarisierte Zonen	muss

Die in der vorgestellten Architektur (vergleiche Nummer 5) abgebildeten demilitarisierten Zonen (DMZ) müssen gemäß den Vorgaben des BSI erstellt werden (vergleiche BSI-ISI-LANA).

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 vom BSI definierten PAP-Struktur (Paketfilter – Application Layer Gateway – Paketfilter) entsprechen.

Für die Zulassungsbehörde-NdB-VN-DMZ (Schnittstelle C) kann abweichend auch eine reine Paketfilter-Lösung implementiert werden. Dies liegt darin begründet, dass über diese in der Regel bereits bestehende Schnittstelle die ZFZR-Webservice-Kommunikation mit dem KBA erfolgt. Hier handelt es sich um eine mittels Client-Zertifikate authentifizierte Transport Layer Security(TLS)-Kommunikation (TLS 1.2 und 1.3 möglich). Ein Aufbrechen der TLS-Verbindung am Application Layer Gateway kann hier insbesondere bei TLS 1.3 auf Grund der Verschlüsselung von Werten im TLS-Handshake zu Problemen bei der Authentizitätsprüfung der Gegenstelle führen.

A-6.1-11	Mandantentrennung	muss

Im Falle des Betriebs für mehrere Mandanten (zum Beispiel i-Kfz-Portale für mehrere Zulassungsbehörden oder Fachverfahren für mehrere Zulassungsstellen) muss eine Mandantentrennung konzipiert und implementiert werden.

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

Wird die Mandantenfähigkeit mit Hilfe von Virtualisierung implementiert, muss die sogenannte IT-System-Virtualisierung (Virtualisierung von vollständigen Server-Systemen) verwendet werden. Die Aspekte der sicheren Virtualisierung müssen gemäß dem Baustein „SYS.1.5 Virtualisierung“ des IT-Grundschutz-Kompendiums unter der Berücksichtigung der darin enthaltenen Anforderungen implementiert werden. Insbesondere die Isolation und Kapselung der einzelnen Mandanten (sowohl auf der 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 Administration 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	Nutzung von externen Cloud-Diensten	muss

Im Falle der Nutzung eines externen Cloud-Dienstes[5], zum Beispiel bei der Nutzung von virtuellen Servern oder Speicher aus der Cloud für Fachverfahren, i-Kfz-Portale, indirekt am Zulassungsprozess beteiligte Verfahren oder E-Payment-Dienste, müssen die Vorgaben des BSI zur Nutzung von externen Cloud-Diensten berücksichtigt und eingehalten werden (vergleiche BSI-MS-CLOUD).

A-6.1-13	Zugangs- und Zugriffskonzept	muss

Ein Zugangs- und Zugriffskonzept muss erstellt und implementiert werden.

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

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

Die Anzahl der Administrierenden, 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.

[5] Externe Cloud-Dienste im Sinne des BSI-Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netzwerke und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden (vergleiche BSI-MS-CLOUD).

A-6.1-14	Nachweispflicht gegenüber KBA	muss

Die Erfüllung der im Rahmen dieses Dokuments verfassten Mindestsicherheitsanforderungen muss in Form eines schriftlichen Berichts erstellt und dem KBA im Zuge des in Nummer 7 beschriebenen Zulassungsverfahrens nachgewiesen werden.

Ein formloser Bericht ist dabei ausreichend. Dieser muss als Anlage die vollständigen Penetrationstest-Berichte (vergleiche A-6.1-2 sowie Nummer 7.4) und den vollständigen Audit-Bericht (Nachweis der Einhaltung der Anforderung aus den Nummer 6, vergleiche auch 7.2) sowie, falls vorhanden, die ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund des i-Kfz-Portals, des Fachverfahrens und/oder des indirekt zulassungsrelevanten Verfahrens, beinhalten. Die in den Nummern 7.2 bis 7.4 beschriebenen Punkte sind einzuhalten.

6.2 Sicherheitsanforderungen an die Schnittstellen der Architektur

Basierend auf der Beschreibung des Verhaltens an den Schnittstellen werden in diesem Kapitel Sicherheitsanforderungen an die in Nummer 5.5 aufgeführten Schnittstellen der Architektur des i-Kfz-Systems definiert.

6.2.1 Anforderungen an die Schnittstelle A

Die Ausgestaltung der Schnittstelle A ist der Nummer 5.5.1 zu entnehmen. Es werden 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 Internet Protocol Security (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 Internet Key Exchange Protocol (IKE) aufgebaut werden.

Die vom BSI publizierten Vorgaben zur Verwendung von IPSec gemäß den Nummern 2.2 und 3.3 in BSI-TR02102-3 sollten eingehalten werden.

Die genaue Konfiguration der IPSec-Verbindung wird vom KBA im Zuge des Zulassungsverfahrens zur Verfügung gestellt. Besteht vorab Informationsbedarf, so kann der technische Support beziehungsweise die Anwenderbetreuung des KBA unterstützen und gegebenenfalls entsprechende Dokumente zur Verfügung stellen (vergleiche Nummer 9).

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. Besteht vorab Informationsbedarf, so kann der technische Support beziehungsweise die Anwenderbetreuung des KBA unterstützen und gegebenenfalls entsprechende Dokumente zur Verfügung stellen (vergleiche Nummer 9).

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 Protokolls ESP sichert die Vertraulichkeit zu.

Es sollten die Vorgaben des BSI zur Verwendung von IPSec (Nummern 2.2 und 3.3 gemäß BSI-TR02102-3) erfüllt werden.

Die genaue Auflistung der benutzten Parameter wird vom KBA im Zuge des Zulassungsverfahrens bereitgestellt. Besteht vorab Informationsbedarf, so kann der technische Support beziehungsweise die Anwenderbetreuung des KBA unterstützen und gegebenenfalls entsprechende Dokumente zur Verfügung stellen (vergleiche Nummer 9).

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

Die während der Übertragung gegebenenfalls 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 i-Kfz-Portal kommende Aufruf des i-Kfz-Webservices muss authentifiziert werden.

Die im Dokument „Standard für die Datenübermittlung an das Kraftfahrt-Bundesamt – Datenaustausch mit i-Kfz-Portalen“ enthaltenen Vorgaben müssen eingehalten werden.

Die genauen Eingaben zum benutzten Mechanismus werden vom KBA im Zuge des Zulassungsverfahrens bereitgestellt. Besteht vorab Informationsbedarf, so kann der technische Support beziehungsweise die Anwenderbetreuung des KBA unterstützen und gegebenenfalls entsprechende Dokumente zur Verfügung stellen (vergleiche Nummer 9).

6.2.2 Anforderungen an die Schnittstelle B & Bg

Interne Schnittstelle des KBA.

6.2.3 Anforderungen an die Schnittstelle C

Die Ausgestaltung der Schnittstelle C ist der Nummer 5.5.3 zu entnehmen. 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-NdB-VN-DMZ“ angeboten werden und darf nur von Komponenten aus dem Bereich „Zulassungsbehörde-Kern-Netz“ verwendet werden.

Insbesondere ist es explizit untersagt, dass eine Komponente aus dem Bereich „Zulassungsbehörde-Internet-DMZ“ über einen Zugriff auf die Schnittstelle C verfügt. Auch die Komponente „Portal-NdB-VN-Cnn“ darf nicht über einen Zugriff auf die Schnittstelle C verfügen.

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

Ergänzend ist in diesem Zusammenhang die Anforderung A-6.2.9-1 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 IznAaKBAfB“ und „Standard für die Datenübermittlung an das Kraftfahrt-Bundesamt – Datenaustausch mit den Zulassungsbehörden“ enthaltenen Vorgaben müssen eingehalten werden.

Die Vorgaben aus BSI-TR02102 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 protokolliert werden. Die Protokolldaten unterliegen einer engen Zweckbindung und dürfen ausschließlich dem Zweck der Entdeckung und Erörterung der Gründe von potenziell aufkommenden Unregelmäßigkeiten in der Kommunikation dienen (Sicherstellung des ordnungsgemäßen Betriebs).

Die Protokolldaten müssen die Identität der zugreifenden Instanz sowie systemtechnische Daten (zum Beispiel Internet Protocol (IP)-Adresse und Port et cetera) beinhalten.

Die Protokolldaten müssen für sechs Monate aufbewahrt und danach unverzüglich automatisiert gelöscht werden. Ergibt sich in dieser Frist der Bedarf für eine längere Speicherung zum Zwecke der Datenschutzkontrolle oder Datensicherheit, hat die Löschung unverzüglich nach Fortfall dieses Bedarfs zu erfolgen (§ 18 FZV).

Die geltenden Datenschutzbestimmungen müssen eingehalten werden.

Die Vorgaben aus BSI-ITG (Baustein OPS.1.1.5 und DER.1) und BSI-MS-PROT zur Protokollierung und Detektion von Cyber-Angriffen müssen beachtet werden.

6.2.4 Anforderungen an die Schnittstelle D

Die Anforderungen an die Schnittstelle D sind in Informationen zur netztechnischen Anbindung an das KBA für Behörden IznAaKBAfB beschrieben. Die Eigenschaften der Schnittstelle D sind in Nummer 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 muss über die Schnittstelle D erfolgen.

Es müssen die für die Schnittstelle D in diesem Dokument und in IznAaKBAfB und „Standard für die Datenübermittlung an das Kraftfahrt-Bundesamt – Datenaustausch mit den Zulassungsbehörden“ definierten Anforderungen 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 mittels OpenFT oder Log-FT möglich sein.

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

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

6.2.5 Anforderungen an die Schnittstelle E

Interne Schnittstelle des KBA.

6.2.6 Anforderungen an die Schnittstelle F

Die Ausgestaltung der Schnittstelle F ist der Nummer 5.5.6 zu entnehmen. Es werden folgende Anforderungen an die Schnittstelle F abgeleitet:

A-6.2.6-1	Die Benutzung der Schnittstelle F	muss

Die Schnittstelle F muss von einer Komponente aus dem Bereich „i-Kfz-Portal-DMZ“ zur Verfügung gestellt werden und es muss sichergestellt sein, dass sie nur von Komponenten aus dem gleichen Bereich angesprochen wird.

A-6.2.6-2	Die Integration der Schnittstelle F	kann

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

In diesem Fall muss (zum Beispiel 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 (zum Beispiel IP-Adresse und Port et cetera) beinhalten.

Die Protokolldaten müssen für sechs Monate aufbewahrt und danach unverzüglich automatisiert gelöscht werden. Ergibt sich in dieser Frist der Bedarf für eine längere Speicherung zum Zwecke der Datenschutzkontrolle oder Datensicherheit, hat die Löschung unverzüglich nach Fortfall dieses Bedarfs zu erfolgen (§ 18 FZV). Die geltenden Datenschutzbestimmungen müssen eingehalten werden.

Die Vorgaben aus BSI-ITG (Baustein OPS.1.1.5 und DER.1) und aus BSI-MS-PROT zur Protokollierung und Detektion von Cyber-Angriffen müssen beachtet werden.

6.2.7 Anforderungen an die Schnittstelle H

Die Ausgestaltung der Schnittstelle H ist der Nummer 5.5.7 zu entnehmen. Es werden folgende Anforderungen an die Schnittstelle H abgeleitet:

A-6.2.7-1	Implementierung des elektronischen Identitätsnachweises	muss

Die Identität der Antragstellenden Person muss auf dem Vertrauensniveau „substantiell“ oder „hoch“ im Sinne des Artikels 8 der EIDAS-VO sicher nachzuweisen sein. Dazu können die Online-Ausweisfunktion (eID-Funktion) oder andere elektronische Identifizierungsmittel gemäß § 20 FZV verwendet werden, sofern der Nachweis der Identität auf dem Vertrauensniveau „substantiell“ oder „hoch“ erfolgt.

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

Ausschließlich bei der Außerbetriebsetzung kann auf die Identifizierung der antragstellenden Person entsprechend § 24 Absatz 4 FZV verzichtet werden.

Die für den Antrag erforderlichen Angaben sind, soweit elektronisch auslesbar, aus dem zur Identifizierung verwendeten Verfahren zu übernehmen.

Bezüglich der vom Halter eingegebenen Daten ist § 20 Absatz 4 FZV einzuhalten.

A-6.2.7-2	Die Authentizität der Daten	muss

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

Die Benutzung von einem sicheren Transportkanal (TLS gemäß BSI-MS-TLS) zusammen mit der Durchführung des elektronischen Identitätsnachweises sichert die Bestätigung der Identität der beiden Instanzen Antragstellende Person und i-Kfz-Portal (Vorlage des Berechtigungszertifikates) (vergleiche BSI-TR03107-1 & BSI-TR02102 zu sicheren Kryptoverfahren).

A-6.2.7-3	Die Vertraulichkeit der Daten	muss

Die Daten müssen zwischen dem Browser der antragstellenden Person und dem Web-Server des i-Kfz-Portals stets verschlüsselt übertragen werden.

Im Rahmen des durchgeführten elektronischen Identitätsnachweises mit Hilfe eines elektronischen Identifizierungsmittels gemäß A-6.2.7-1 wird eine TLS-geschützte Verbindung unter Berücksichtigung des BSI-MS-TLS zwischen dem Web-Browser und dem Web-Server aufgebaut (vergleiche BSI-TR03107-1 und BSI-TR03124-1). Diese Verbindung muss für die Übertragung der Antragsdaten benutzt werden.

A-6.2.7-4	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 sechs Monate aufbewahrt und danach unverzüglich automatisiert gelöscht werden. Ergibt sich in dieser Frist der Bedarf für eine längere Speicherung zum Zwecke der Datenschutzkontrolle oder Datensicherheit, hat die Löschung unverzüglich nach Fortfall dieses Bedarfs zu erfolgen (§ 18 FZV). 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.

Die geltenden Datenschutzbestimmungen müssen eingehalten werden.

Die Vorgaben aus BSI-ITG (Baustein OPS.1.1.5 und DER.1) und BSI-MS-PROT zur Protokollierung und Detektion von Cyber-Angriffen müssen ebenfalls beachtet werden.

6.2.8 Anforderungen an die Schnittstelle Xi

Die Ausgestaltung der Schnittstelle Xi ist der Nummer 5.5.8 zu entnehmen. Es werden folgende Anforderungen an die Schnittstelle Xi abgeleitet:

Hinweis: Die indirekt am Zulassungsprozess beteiligten Verfahren, die über das Internet erreichbar sind, sind ebenfalls über die Schnittstelle Xi anzubinden.

A-6.2.8-1	Die Integrität der Daten muss geschützt werden.	muss

Im Rahmen des Integritätsschutzes muss insbesondere die Herkunft der Daten sichergestellt werden. Nur Daten mit sicherer Herkunft dürfen verarbeitet werden.

Die beiden Kommunikationspartner müssen vor Beginn der Kommunikation authentifiziert werden.

Eine potenzielle Manipulation der Daten auf der Übertragungsstrecke muss durch den Empfänger der Nachricht erkannt werden.

Eine in der Transport-Schicht aufgesetzte Sicherung der Integrität ist für die Zwecke der Absicherung der Schnittstelle Xi ausreichend.

Die Verwendung einer authentifizierten Hypertext Transfer Protocol Secure (HTTPS)-Verbindung unter Berücksichtigung des BSI-MS-TLS (vergleiche auch RFC2818) stellt ein Beispiel für die Ausgestaltung dar. Es können auch vergleichbare Technologien gemäß dem Stand der Technik verwendet werden (zum Beispiel VPN-Tunnel).

Die Vorgaben zu den Schlüssellängen und verwendeten Algorithmen des BSI müssen befolgt werden (vergleiche BSI-MS-TLS oder BSI-TR02102-3).

A-6.2.8-2	Die Vertraulichkeit der zu übertragenden Daten muss zu jeder Zeit gewährleistet werden.	muss

Die Vertraulichkeit der zu übertragenden Daten muss in beiden Kommunikationsrichtungen, entsprechend den Vorgaben aus dem festgestellten Schutzbedarf (vergleiche Nummer 2), zugesichert werden.

Eine in der Transport-Schicht umgesetzte Verschlüsselung der zu übertragenden Daten ist ausreichend.

Die Verwendung von einer authentifizierten HTTPS-Verbindung unter Berücksichtigung des BSI-MS-TLS (vergleiche auch RFC2818) stellt ein Beispiel für die Ausgestaltung dar. Es können auch vergleichbare Technologien gemäß dem Stand der Technik verwendet werden (zum Beispiel VPN-Tunnel).

Die Vorgaben zu den Schlüssellängen und verwendeten Algorithmen des BSI müssen befolgt werden (vergleiche BSI-MS-TLS oder BSI-TR02102-3).

A-6.2.8-3	Die Nachvollziehbarkeit muss gewährleistet werden.	muss

Die Übertragung der Daten (Versand und Empfang) muss auf der gesamten Strecke hinreichend protokolliert werden.

Die Protokolldaten müssen die Identität der sendenden und empfangenden Instanz sowie systemtechnische Daten (zum Beispiel IP-Adresse und Port et cetera) beinhalten.

Die Protokolldaten müssen für sechs Monate aufbewahrt und danach unverzüglich automatisiert gelöscht werden. Ergibt sich in dieser Frist der Bedarf für eine längere Speicherung zum Zwecke der Datenschutzkontrolle oder Datensicherheit, hat die Löschung unverzüglich nach Fortfall dieses Bedarfs zu erfolgen (§ 18 FZV).

Insbesondere sind die Vorgaben und Empfehlungen des BSI zur Erstellung und Verwaltung der sicheren Protokolldaten in den Dokumenten der Internet Sicherheit (ISi)-Reihe (vergleiche Anforderung A-6.2.3-3, Nummer 7.2.3) einzuhalten.

Die geltenden Datenschutzbestimmungen müssen eingehalten werden.

Die Vorgaben aus BSI-ITG (Baustein OPS.1.1.5 und DER.1) und BSI-MS-PROT zur Protokollierung und Detektion von Cyber-Angriffen müssen ebenfalls beachtet werden.

A-6.2.8-4	Sichere Anbindung der lokalen Netze an das Internet	muss

Die Vorgaben des BSI-Standards zur Internet-Sicherheit (ISi-Reihe), besonders die zur Sicheren Anbindung von lokalen Netzen an das Internet (ISi-LANA), müssen berücksichtigt und eingehalten werden (vergleiche unter anderem BSI-ISI-LANA, BSI-ISI-SVR, oder BSI-ISI-WEB-SVR).

6.2.9 Anforderungen an die Schnittstelle Yi

Die Ausgestaltung der Schnittstelle Yi ist der Nummer 5.5.9 zu entnehmen. Es werden folgende Anforderungen an die Schnittstelle Yi abgeleitet:

Hinweis: Die Schnittstelle ist auch von den indirekt am Zulassungsprozess beteiligten Verfahren, die über das Internet erreichbar sind, zu nutzen (siehe Nummer 5.1).

A-6.2.9-1	Verwendung der Schnittstelle Yi	muss

Die Schnittstelle Yi 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.

A-6.2.9-2	Integrität und Vertraulichkeit der Daten müssen geschützt werden.	muss

Die Integrität und Vertraulichkeit der übermittelten Daten müssen gemäß dem attestierten Schutzbedarf (vergleiche Nummer 2) und gemäß dem Stand der Technik geschützt werden.[6]

A-6.2.9-3	Die Nachvollziehbarkeit muss gewährleistet werden.	muss

Die Übertragung der Daten (Versand und Empfang) muss auf der gesamten Strecke hinreichend protokolliert werden.

Die Protokolldaten müssen die Identität der sendenden und empfangenden Instanz sowie systemtechnische Daten (zum Beispiel IP-Adresse und Port et cetera) beinhalten.

Die Protokolldaten müssen für sechs Monate aufbewahrt und danach unverzüglich automatisiert gelöscht werden. Ergibt sich in dieser Frist der Bedarf für eine längere Speicherung zum Zwecke der Datenschutzkontrolle oder Datensicherheit, hat die Löschung unverzüglich nach Fortfall dieses Bedarfs zu erfolgen (§ 18 FZV).

Die geltenden Datenschutzbestimmungen müssen eingehalten werden.

Die Vorgaben aus BSI-ITG (Baustein OPS.1.1.5 und DER.1) und BSI-MS-PROT zur Protokollierung und Detektion von Cyber-Angriffen müssen beachtet werden.

6.2.10 Anforderungen an die Schnittstelle Xn

Die Ausgestaltung der Schnittstelle Xn ist der Nummer 5.5.10 zu entnehmen. Es werden folgende Anforderungen an die Schnittstelle Xn abgeleitet:

A-6.2.10-1	Die Integrität der Daten muss geschützt werden.	muss

Im Rahmen des Integritätsschutzes muss insbesondere die Herkunft der Daten sichergestellt werden. Nur Daten mit sicherer Herkunft dürfen verarbeitet werden.

Die beiden Kommunikationspartner müssen vor Beginn der Kommunikation authentifiziert werden.

Eine potenzielle Manipulation der Daten auf der Übertragungsstrecke muss durch den Empfänger der Nachricht erkannt werden.

Eine in der Transport-Schicht aufgesetzte Sicherung der Integrität ist für die Zwecke der Absicherung der Schnittstelle Xn ausreichend.

Die Verwendung einer authentifizierten HTTPS-Verbindung unter Berücksichtigung des BSI-MS-TLS (vergleiche auch RFC2818) stellt ein Beispiel für die Ausgestaltung dar. Es können auch vergleichbare Technologien gemäß dem Stand der Technik verwendet werden (zum Beispiel VPN-Tunnel).

Die Vorgaben zu den Schlüssellängen und verwendeten Algorithmen des BSI müssen befolgt werden (vergleiche BSI-MS-TLS oder BSI-TR02102-3).

A-6.2.10-2	Die Vertraulichkeit der zu übertragenden Daten muss zu jeder Zeit gewährleistet werden.	muss

Die Vertraulichkeit der zu übertragenden Daten muss in beiden Kommunikationsrichtungen, entsprechend den Vorgaben aus dem festgestellten Schutzbedarf, zugesichert werden.

Eine in der Transport-Schicht umgesetzte Verschlüsselung der zu übertragenden Daten ist ausreichend.

Die Verwendung einer authentifizierten HTTPS-Verbindung unter Berücksichtigung des BSI-MS-TLS (vergleiche auch RFC2818) stellt ein Beispiel für die Ausgestaltung dar. Es können auch vergleichbare Technologien gemäß dem Stand der Technik verwendet werden (zum Beispiel VPN-Tunnel).

Die Vorgaben zu den Schlüssellängen und verwendeten Algorithmen des BSI müssen befolgt werden (vergleiche BSI-MS-TLS oder BSI-TR02102-3).

A-6.2.10-3	Die Nachvollziehbarkeit muss gewährleistet werden.	muss

Die Übertragung der Daten (Versand und Empfang) muss auf der gesamten Strecke hinreichend protokolliert werden.

Die Protokolldaten müssen die Identität der sendenden und empfangenden Instanz sowie systemtechnische Daten (zum Beispiel IP-Adresse und Port et cetera) beinhalten.

Die Protokolldaten müssen für sechs Monate aufbewahrt und danach unverzüglich automatisiert gelöscht werden. Ergibt sich in dieser Frist der Bedarf für eine längere Speicherung zum Zwecke der Datenschutzkontrolle oder Datensicherheit, hat die Löschung unverzüglich nach Fortfall dieses Bedarfs zu erfolgen (§ 18 FZV).

Die geltenden Datenschutzbestimmungen müssen eingehalten werden.

[6] Stand der Technik sind zum Beispiel die Vorgaben des IT-Grundschutzes und die Mindeststandards des BSI.

Die Vorgaben aus BSI-ITG (Baustein OPS.1.1.5 und DER.1) und BSI-MS-PROT zur Protokollierung und Detektion von Cyber-Angriffen müssen ebenfalls beachtet werden.

6.2.11 Anforderungen an die Schnittstelle Yn

Die Ausgestaltung der Schnittstelle Yn ist der Nummer 5.5.10 zu entnehmen. Es werden folgende Anforderungen an die Schnittstelle Yn abgeleitet:

A-6.2.11-1	Verwendung der Schnittstelle Yn	muss

Die Schnittstelle Yn muss von einer Komponente aus dem Bereich „Zulassungsbehörde-NdB-VN-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.

A-6.2.11-2	Integrität und Vertraulichkeit der Daten müssen geschützt werden.	muss

Die Integrität und Vertraulichkeit der übermittelten Nachrichten müssen gemäß dem attestierten Schutzbedarf (vergleiche Nummer 2) und gemäß dem Stand der Technik geschützt werden.[7]

A-6.2.11-3	Die Nachvollziehbarkeit muss gewährleistet werden.	muss

Die Übertragung der Daten (Versand und Empfang) muss auf der gesamten Strecke hinreichend protokolliert werden.

Die Protokolldaten müssen die Identität der sendenden und empfangenden Instanz sowie systemtechnische Daten (zum Beispiel IP-Adresse und Port et cetera) beinhalten.

Die Protokolldaten müssen für sechs Monate aufbewahrt und danach unverzüglich automatisiert gelöscht werden. Ergibt sich in dieser Frist der Bedarf für eine längere Speicherung zum Zwecke der Datenschutzkontrolle oder Datensicherheit, hat die Löschung unverzüglich nach Fortfall dieses Bedarfs zu erfolgen (§ 18 FZV).

Die geltenden Datenschutzbestimmungen müssen eingehalten werden.

Die Vorgaben aus BSI-ITG (Baustein OPS.1.1.5 und DER.1) und BSI-MS-PROT zur Protokollierung und Detektion von Cyber-Angriffen müssen beachtet werden.

7 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 für Kommunikationspartner werden in diesem Kapitel beschrieben.

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.

7.1 Lebenszyklus einer Zulassung

Der Lebenszyklus einer Zulassung zur Kommunikation mit der KBA-Infrastruktur im Rahmen des i-Kfz-Projekts (im weiteren Verlauf auch nur Zulassung genannt) wird in der Abbildung 12 dargestellt.

[7] Stand der Technik sind zum Beispiel die Vorgaben des IT-Grundschutzes und die Mindeststandards des BSI.

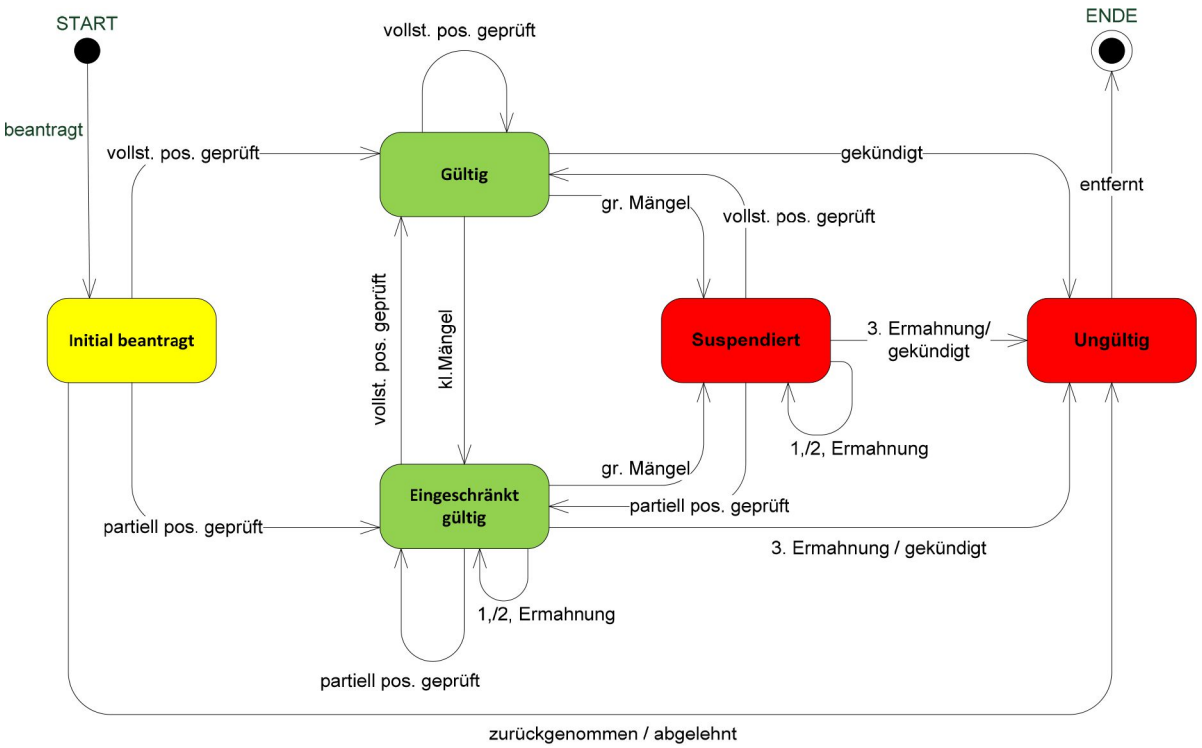

Abbildung 12: Der Lebenszyklus einer Zulassung

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 folgende 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 (zum Beispiel „gültig“ – kleine Mängel → „gültig“),
- „out“ – ein ausgehender Übergang, bedeutet mit Hilfe dieses Übergangs kann der betrachtende Zustand verlassen werden (zum Beispiel „eingeschränkt gültig“ – vollständig positiv geprüft → „gültig“),
- „in/out“ – ein- und ausgehender Übergang, bedeutet mit Hilfe dieses Übergangs kann der betrachtende Zustand verlassen, aber gleichzeitig auch wieder betreten werden (zum Beispiel „eingeschränkt gültig“ – erste Ermahnung → „eingeschränkt gültig“),
- „Name“ – der Name eines Übergangs (zum Beispiel „erste Ermahnung“),
- „Start“ – Anfangszustand eines Übergangs,
- „Ziel“ – Zielzustand eines Übergangs,
- „Beschreibung“ – eine textuelle Beschreibung des Übergangs.

7.1.1 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 Nummer 7.1.2).

Eine Zulassung befindet sich in dem Zustand „initial beantragt“, wenn der Beantragungsprozess erfolgreich abgeschlossen wurde (vergleiche Nummer 7.5).

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 1 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 Antragungsunterlagen seitens des KBAs statt.
out	„vollständig 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 der antragstellenden Person zurückgenommen oder durch das KBA abgelehnt. Es wurde keine Zulassung erteilt.

Tabelle 1: Zulassungsverfahren – Übergänge des Zustands „initial beantragt“

7.1.2 Eine „gültige“ Zulassung

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

1. Der Beantragungsprozess wurde erfolgreich abgeschlossen (vergleiche Nummer 7.5).
2. Die in diesem Dokument definierten Mindestsicherheitsanforderungen (vergleiche Nummer 6) sind vollständig erfüllt (die Einhaltung/Erfüllung konnte vollständig positiv geprüft werden).
3. Die Erfüllung der Mindestsicherheitsanforderungen wurde im Rahmen eines Audits (vergleiche Nummer 7.2) durch einen unabhängigen Dritten (im weiteren Verlauf auditierende Person genannt) überprüft und bestätigt.
4. Die Dauer bis zur Fälligkeit eines nächsten Audits ist länger als zwei Monate.

Hinweis: Sobald die Zeit bis zur Vorlage der Ergebnisse des Re-Audits kürzer als zwei Monate ist, ist die Zulassung automatisch „eingeschränkt gültig“.

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

In der Tabelle 2 werden die möglichen Aktivitäten (Übergänge) und die 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 (zum Beispiel 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, zum Beispiel erneute rechtzeitige Vorlage aktualisierter Zulassungsdokumente.
out	„kleine Mängel“		„eingeschränkt gültig“	Kleine Mängel (zum Beispiel 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 2: Zulassungsverfahren – Übergänge des Zustands „gültig“

7.1.3 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 Nummer 7.7).

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

In der Tabelle 3 werden, bezogen auf eine „eingeschränkt gültige“ Zulassung, die Aktivitäten (Übergänge) und die 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 (zum Beispiel 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 beziehungsweise 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.
	„erste/zweite 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 (zum Beispiel schwerwiegender Informationssicherheitsvorfall). Die Zulassung wurde suspendiert. Die Mängel müssen in vorgegebener Zeit beseitigt werden. Es findet keine Kommunikation mit der KBA-Infrastruktur statt.
	„dritte Ermahnung/ gekündigt“		„ungültig“	Die Zulassung wurde vom Kommunikationspartner gekündigt, oder aufgrund nicht erfüllter Auflagen wurde 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 3: Zulassungsverfahren – Übergänge des Zustands „eingeschränkt gültig“

7.1.4 Eine „suspendierte“ Zulassung

Eine Zulassung kann aufgrund der festgestellten großen Mängel suspendiert werden. Zu der Gruppe der großen Mängel gehören unter anderem:

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

Eine suspendierte Zulassung wird normalerweise 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 Erfüllungs- und Nachweisfristen kann zur Ungültigkeit der Zulassung führen (vergleiche Nummer 7.7).

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

In der Tabelle 4 werden die Aktivitäten (Übergänge) und daraus resultierende neue Zustände der Zulassung, bezogen auf eine „suspendierte“ Zulassung, dargestellt:

Übergänge				
Art	Name	Start	Ziel	Beschreibung
in	„großer Mangel“	„gültig“	„suspendiert“	Es wurde zumindest ein großer Mangel festgestellt (zum Beispiel ein schwerwiegender Informationssicherheitsvorfall). Es werden bestimmte Auflagen auferlegt, die in einer Frist vom Kommunikationspartner erfüllt werden müssen.
		„eingeschränkt gültig“		
in/out	„erste/zweite 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 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.
	„dritte Ermahnung/ gekündigt“		„ungültig“	Die Zulassung wurde vom Kommunikationspartner gekündigt, oder aufgrund der Nichterfüllung von Auflagen wurde eine dritte und endgültige Ermahnung seitens des KBA ausgesprochen. Die Zulassung ist „ungültig“. Um die Kommunikation mit KBA wieder aufzunehmen, muss erneut eine Zulassung beantragt werden.

Tabelle 4: Zulassungsverfahren – Übergänge des Zustands „suspendiert“

7.1.5 Eine „ungültige“ Zulassung

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

Eine ungültige Zulassung ermächtigt nicht zur Kommunikation mit der KBA-Infrastruktur (die i-Kfz-Zugangsdaten werden seitens des KBAs gesperrt beziehungsweise gelöscht).

In Tabelle 5 werden die Aktivitäten (Übergänge) und daraus resultierende neue Zustände der Zulassung, bezogen auf eine „ungültige“ Zulassung, dargestellt:

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

Tabelle 5: Zulassungsverfahren – Übergänge des Zustands „ungültig“

7.2 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). Mindestens die Auditteamleitung muss eine entsprechende Zulassung/Zertifizierung nach ISO-27001 auf der Basis von BSI-IT-Grundschutz besitzen (mindestens dessen Zertifikats-Nummer ist im Audit-Bericht aufzuführen). Weitere spezifische Qualifikationen sind nicht notwendig.

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

Der Umfang des durchzuführenden Audits besteht aus einer Überprüfung der Anforderungen, die in Nummer 6 definiert sind. Alle getesteten Anforderungen sind mit der ID im Audit-Bericht aufzuführen, inklusive der eindeutigen Angabe, ob die jeweilige Anforderung erfüllt wurde oder nicht. Wenn für einzelne Anforderungen auf bereits durchgeführte Prüfungen zum Beispiel des Dienstleisters verwiesen wird, ist mindestens der vollständige Titel inklusive Version und Datum des Prüfberichts aufzuführen und der Prüfbericht dem KBA vorzulegen, falls dieser nicht bereits vorliegt. Die Übertragbarkeit der bereits durchgeführten Prüfungen ist durch die auditierende Person zu bestätigen.

Aus dem Audit-Bericht muss eindeutig erkennbar sein, gegen welche Version der MSA-i-Kfz geprüft wurde, welches Fallszenario (vergleiche Nummer 8), welche Anforderungen (vergleiche Nummer 6), Netzwerkbereiche (vergleiche Nummer 5.3), Komponenten (vergleiche Nummer 5.4) und Schnittstellen (vergleiche Nummer 5.5) getestet und wie diese getestet wurden (Art des Nachweises). Auch das genutzte i-Kfz-Portal, Fachverfahren und gegebenenfalls indirekt am Zulassungsprozess beteiligte Verfahren sowie dessen jeweiliger Betreiber sind aufzuführen.

Im Falle einer bestehenden ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund des i-Kfz-Portals, des Fachverfahrens und der indirekt am Zulassungsprozess beteiligten Verfahren sind im Audit nur die i-Kfz-spezifischen Anforderungen zu prüfen, welche über die IT-Grundschutzprüfung hinausgehen (vergleiche Nummer 7.3). Dies ist durch die auditierende Person zu bestätigen. Mindestens die entsprechende Zertifikats-Nummer, die Gültigkeit, der Geltungsbereich der Zertifizierung und die Bestätigung der Abdeckung des Informationsverbunds des i-Kfz-Portals, des Fachverfahrens und der indirekt am Zulassungsprozess beteiligten Verfahren ist im Audit-Bericht aufzuführen. Sollte zum Beispiel nur für den Informationsverbund des i-Kfz-Portals eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegen, müssen für die Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren alle Anforderungen, nicht nur die der Nummer 7.3, geprüft werden.

Die bei der Überprüfung (Audit) aufgezeigten Mängel müssen unverzüglich und unaufgefordert beseitigt werden. Deren Beseitigung muss durch eine erfolgreiche Nachprüfung, ebenfalls durch einen qualifizierten unabhängigen Dritten (dieser kann auch die vorangegangenen Tests durchgeführt haben), gegenüber dem KBA unaufgefordert nachgewiesen werden. Ist die Beseitigung der Mängel nicht innerhalb von drei Monaten nach Ausstellungsdatum des Berichts von der auditierenden Person möglich, ist in gut begründeten Ausnahmefällen eine Fristverlängerung beim KBA zu beantragen. Hierfür muss dem KBA ein entsprechender Umsetzungsplan mit festem Abschlusstermin unaufgefordert vorgelegt und mit dem KBA abgestimmt werden.

Hinweis: Ein „ISO 27001-Zertifikat auf der Basis von IT-Grundschutz“ erfüllt die Anforderungen der „ISO 27001 native“. Jedoch erfüllt ein „Zertifikat nach ISO 27001 native“ nicht automatisch das gleiche Niveau wie ein „ISO 27001-Zertifikat auf der Basis von IT-Grundschutz“. Somit ist die Anwendung des IT-Grundschutzes bei einer ISO 27001 native nicht in jedem Fall gegeben und die Erfüllung des Umsetzungsplans der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung UP-LIöV ebenfalls nicht in jedem Fall sichergestellt.

7.3 Prüfung der zusätzlichen Anforderungen

Dieses Dokument spezifiziert einige Anforderungen, die über den Rahmen der IT-Grundschutz-Stufe hinausreichen. Insbesondere diese Anforderungen müssen im Zuge des Audits (vergleiche Nummer 7.2) überprüft und entsprechend der Anforderung A-6.1-14 dokumentiert 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 in Nummer 7.4 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 (vergleiche Anforderung A-6.1-6) muss überprüft und das Ergebnis dokumentiert werden.
- Die Kommunikation der Komponenten (vergleiche Anforderung A-6.1-9) und die 1-zu-1-Kommunikation (direkte Weiterleitung der Nachrichten) (vergleiche Anforderung A-6.1-9) sowie Kommunikation zwischen den i-Kfz-Portalen und dem KBA (vergleiche Anforderung A-6.1-1) müssen überprüft und das Ergebnis dokumentiert werden.
- Die Architektur und Aufbau demilitarisierten Zonen (DMZ) (vergleiche Anforderung A-6.1-10) muss überprüft und das Ergebnis dokumentiert werden.
- Im Falle des Betriebs für mehrere Mandanten muss die Mandantentrennung (vergleiche A-6.1-11) überprüft und das Ergebnis dokumentiert werden.

- Im Falle der Nutzung eines externen Cloud-Dienstes müssen die Vorgaben des BSI zur Nutzung von externen Cloud-Diensten (vergleiche Anforderung A-6.1-12) berücksichtigt, überprüft und das Ergebnis dokumentiert werden.
- Die Erfüllung der Anforderungen an die Schnittstellen (vergleiche Nummer 6.2) müssen überprüft und dokumentiert werden.

7.4 Penetrationstests (IS-Kurzrevision, IS-Webcheck und IS-Penetrationstests)

Im Zuge der Maßnahmen zur Härtung der kritischen Anwendungen müssen an den Komponenten (vergleiche hierzu die Anforderung A-6.1-2 in Nummer 6.1) sogenannte Penetrationstests durchgeführt werden. Dabei sind die Vorgaben aus Nummer 7.4.1 einzuhalten. Das Ergebnis muss dem KBA in Form eines Penetrationstest-Berichts mitgeteilt werden. Die im Penetrationstest aufgezeigten Mängel müssen unverzüglich beseitigt werden. Außerdem muss die Beseitigung der im Schadenspotential als „mittel“ oder „höher“ eingestuften Mängel durch eine erfolgreiche Nachprüfung ebenfalls durch einen qualifizierten unabhängigen Dritten (dieser kann auch die vorangegangenen Tests durchgeführt haben) gegenüber dem KBA unaufgefordert nachgewiesen werden. Die Beseitigung der weiteren Mängel (unter „mittel“) ist dem KBA unaufgefordert schriftlich zu bestätigen, es wird jedoch empfohlen, auch deren Beseitigung durch einen unabhängigen Dritten bestätigen zu lassen. Ist die Beseitigung aller aufgezeigten Mängel nicht innerhalb von drei Monaten nach Ausstellungsdatum des Berichts von der Penetrationstestenden Person möglich, ist in gut begründeten Ausnahmefällen eine Fristverlängerung beim KBA zu beantragen. Hierfür muss dem KBA ein entsprechender Umsetzungsplan mit festem Abschlusstermin für alle aufgezeigten Mängel unaufgefordert vorgelegt und mit dem KBA abgestimmt werden.

Aus dem Penetrationstest-Bericht muss eindeutig erkennbar sein, welches Fallszenario (vergleiche Nummer 8), welche Netzwerkbereiche (vergleiche Nummer 5.3), Komponenten (vergleiche Nummer 5.4) und Schnittstellen (vergleiche Nummer 5.5) getestet wurden und wie diese getestet wurden (Art der Angriffstechnik) sowie die Zuordnungen der getesteten Systeme, Anwendungen, Schnittstellen und Bereiche zu diesen (siehe auch Nummer 7.4.1). Auch das genutzte i-Kfz-Portal, Fachverfahren und gegebenenfalls indirekt am Zulassungsprozess beteiligte Verfahren sowie dessen jeweiliger Betreiber sind aufzuführen.

Beim Penetrationstest sind alle i-Kfz-Zulassungsvorgänge, also alle möglichen Lebenszyklen von Fahrzeugen aus zulassungsrechtlicher Sicht, von der Neu-/Erstzulassung, Wiederzulassung, Umschreibung, Tageszulassung bis zur Außerbetriebsetzung zu betrachten, vorzugweise an einem Fahrzeug, wenn dies nicht möglich ist, dann anhand von unterschiedlichen Fahrzeugen.

Hinweis: Für manche Tests ist eine Zusammenarbeit der i-Kfz-Portale und der Fachverfahren erforderlich.

Wenn die auditierende Person die A-6.1-2 erfüllt, kann diese auch den Penetrationstest durchführen.

Die Penetrationstests sind alle zwei Jahre erfolgreich zu wiederholen (siehe Empfehlung des BSI in BSI-LF-PENTEST) und das Ergebnis ist im Rahmen des Zulassungsverfahrens dem KBA unaufgefordert vorzulegen.

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

- Feststellung eines scherwiegenden Informationssicherheitsvorfalls und Beseitigung dessen Ursachen.
- Einsatz einer neuen Hauptversion der i-Kfz-Portal-Fachverfahren oder indirekt am Zulassungsprozess beteiligten Anwendungen. Es handelt sich hier generell nicht um ein Minor-Update beziehungsweise Sicherheitspatch, sondern um ein Major-Release der Software (zum Beispiel von der Version 2.0 auf die Version 3.0).
- Durchführung der Änderungen an den kritischen Schnittstellen, insbesondere an den Außenschnittstellen. Begründet können die Penetrationstests partiell innerhalb des betroffenen Bereiches durchgeführt werden.
- Durchführung von wesentlichen Änderungen an anderen involvierten und sicherheitskritischen Infrastrukturkomponenten – zum Beispiel ein Paketfilter wird gegen ein gänzlich anderes Modell ausgetauscht oder einem Major-Update (neue Hauptversion der Firmware beziehungsweise des Betriebssystems) unterzogen.

In diesen Fällen muss das KBA informiert werden. Dort wird dann entschieden, ob und gegebenenfalls in welchem Umfang ein außerordentlicher Penetrationstest notwendig und das Ergebnis dem KBA mitzuteilen ist (abhängig von den Gegebenheiten vollständig oder punktuell abgestimmt auf die relevanten Bereiche).

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.

Für die Durchführung der Tests sind die vom KBA bereitgestellten Systeme der externen Testumgebung anzusprechen. Eine Beschreibung dieser Umgebung KBA-ExtTU und die vom KBA bereitgestellten Testdatensätze KBA-TDV sind im geschützten Bereich der KBA-Internetseite veröffentlicht.

Sofern diese Daten nicht ausreichen, können die i-Kfz-Portal- und/oder Fachverfahrensanbieter abhängig von der Netzanbindung für alle betroffenen nationalen Verfahren schreibende Zugriffe erhalten und so eigene Testdaten einstellen. Die Beantragung dieser Zugriffe erfolgt formlos – unter Benennung der benötigten Zugriffe – bei der Anwenderbetreuung des KBA (siehe Nummer 9).

Falls die Tests gegen eine Test- oder Staging-Umgebung des i-Kfz-Portals, die Systeme der Fachverfahren oder die indirekt am Zulassungsprozess beteiligten Verfahren durchgeführt werden sollen, benötigt das KBA eine schriftliche Bestätigung, dass die Test- oder Staging-Umgebung der Produktionsumgebung in allen Punkten (zum Beispiel eingesetzte Hard- und Software, Firmware-Stände et cetera) vollständig entspricht.

Wurden bereits Penetrationstests oder Sicherheitsüberprüfungen einer Software im Rahmen von i-Kfz bei einem anderen i-Kfz-Portalbetreiber oder Softwarehersteller durchgeführt, dann können die Ergebnisse verwendet werden, wenn diese dem KBA vorliegen beziehungsweise vorgelegt werden. Es müssen dann nur die umgebungsspezifischen beziehungsweise infrastrukturabhängigen Aspekte geprüft werden. Die Voraussetzung einer Anerkennung von Testergebnissen ist, dass der durchgeführte Test alle zu prüfenden Aspekte der eigenen Umgebung berücksichtigt und dass die Rahmenbedingungen (Umgebung, Infrastruktur, Versionen) denen der eigenen, zu testenden Umgebung entsprechen. Alle abweichenden beziehungsweise nicht abgedeckten (umgebungsspezifischen, infrastrukturabhängigen) Aspekte müssen in einem eigenen/separaten Test getestet werden. Wenn auf andere Tests oder Sicherheitsüberprüfungen verwiesen wird, ist sicherzustellen und schriftlich von einem unabhängigen Dritten beziehungsweise im Penetrationstest-Bericht zu bestätigen, dass die Software und die Umgebung in allen Punkten (zum Beispiel eingesetzte Hard- und Software, Firmware- und Patch-Stände et cetera) vollständig identisch sind. Des Weiteren ist nachvollziehbar im Penetrationstest-Bericht aufzuführen, welche Anforderungen durch die Tests bereits abgedeckt sind und welche nicht. Wenn für einzelne Punkte auf bereits durchgeführte Prüfungen zum Beispiel des Dienstleisters verwiesen wird, ist auch mindestens der vollständige Titel inklusive Version und Datum des Prüfberichts aufzuführen und der Prüfbericht dem KBA vorzulegen, falls dieser nicht bereits vorliegt.

7.4.1 Art und Umfang des Penetrationstests (IS-Kurzrevision, IS-Webcheck und IS-Penetrationstests)

Gemäß der Anforderung A-6.1-2 müssen Komponenten besonderen Härtungsmaßnahmen unterzogen werden, um die Wirksamkeit der vorhandenen Sicherheitsmaßnahmen zu überprüfen und potentielle Schwachstellen aufdecken und beheben zu können. Hierfür stehen zwei Testmethoden zur Verfügung, der IS-Penetrationstest sowie der IS-Webcheck, die beide für ihr jeweiliges Anwendungsfeld angewendet werden müssen. Darüber hinaus dient die IS-Kurzrevision des Informationsverbunds der Komponenten als Revisionskomponente dazu, die grundlegende Konformität des ISMS mit dem BSI-IT-Grundschutz nachzuweisen.

Zu den Härtungsmaßnahmen gehört die erfolgreiche Durchführung der in diesem Kapitel definierten Methoden:

- Durchführung einer IS-Kurzrevision (entsprechend dem Leitfaden für die IS-Revision BSI-LF-REVISION, entfällt bei Vorliegen einer ISO 27001 Zertifizierung auf Basis von IT-Grundschutz),
  - Festlegung des Prüfplans
  - Sichtung der zur Verfügung gestellten Dokumente zur Bestimmung der Stichproben und Schwerpunkte
  - Vor-Ort-Prüfung
  - Abschlussbericht
- Durchführung eines IS-Webchecks (entsprechend dem Praxis-Leitfaden für IS-Webchecks BSI-LF-WEBCHECK),
  - Einarbeitung des Prüfers
  - Test des Prüfobjekts
    - Anfangsgespräch
    - Einrichtung der Arbeitsumgebung
    - Praktische Prüfung
      - Schwachstellensuche
      - Schwachstellentest
      - Logische Fehler/Konfigurationsfehler
      - Exploits (Optional)
    - Abschlussgespräch
  - Abschlussbericht
- Durchführung von IS-Penetrationstests (entsprechend dem Praxis-Leitfaden für IS-Penetrationstests BSI-LF-PENTEST)
  - Einarbeitung der prüfenden Person
  - Test des Prüfobjekts
    - Anfangsgespräch
    - Einrichtung der Arbeitsumgebung
    - Praktische Prüfung
      - Konzeptionelle Schwächen
      - Umsetzung Härtungsmaßnahmen

  - Bekannte Schwachstellen
  - Exploits (Optional)
- Abschlussgespräch
- Abschlussbericht

Die genaue Beschreibung der Modalitäten der Durchführung ist der Nummer 7.4 zu entnehmen. Im Rahmen dieses Kapitels wird lediglich die Art sowie der Umfang der durchzuführenden Prüfungen dargestellt.

Es wird empfohlen, die IS-Kurzrevision grundsätzlich vorzuziehen, anschließend den IS-Webcheck und zum Schluss den IS-Penetrationstest durchzuführen. Beim IS-Webcheck ist die Webanwendung beziehungsweise Internetpräsenz ohne vorgeschaltetes Sicherheitsgateway zu untersuchen. Das Sicherheitsgateway sowie die weiteren Komponenten und Schnittstellen werden im IS-Penetrationstest überprüft.

Aus jedem Abschlussbericht müssen die nachfolgenden Informationen einfach ersichtlich sein:

- die Informationsbasis beziehungsweise das Testverfahren (hier in der Regel White-Box)
- der Prüfumfang
  - Prüftiefe (technisches Sicherheitsaudit, nicht invasiver Schwachstellenscan, invasiver Schwachstellenscan beziehungsweise Exploits)
  - Prüfort (vor Ort oder über das Internet)
  - Prüfbedingungen (Originalsystem oder Testsystem, mit oder ohne Sicherheitsgateway)
  - und Prüfzeitraum
- die geprüften Prüfobjekte (Systeme, Anwendungen, Schnittstellen, … inklusive Zuordnung zu den Komponenten gemäß Nummer 5.4)
- die geprüften Bereiche (inklusive Zuordnung zu den Netzwerkbereichen gemäß Nummer 5.3)
- die geprüften Schnittstellen (inklusive Zuordnung zu den Schnittstellen gemäß Nummer 5.5)
- das vorliegende Fallszenario gemäß Nummer 8
- die geprüften Module mit Nummern, Namen beziehungsweise Angriffstechniken (siehe unten)
- die gefundenen Schwachstellen inklusive deren Kritikalität

Die Tests müssen immer von fachlich qualifizierten Personen durchgeführt werden, die unabhängig von den untersuchten Bereichen sind und die nicht bei Konzeption, Aufbau oder Betrieb des untersuchten Informationsverbunds mitgewirkt haben. Eine Durchführung zum Beispiel durch die Anwendungsentwicklung, Betreiber oder betriebsverantwortlichen Person ist nicht zulässig. Das beauftragte Unternehmen muss in dem Umfeld etabliert sein (zum Beispiel durch Fachpublikation, vergleichbare Referenzen von Kunden). Die Beauftragung BSI-zertifizierter IT-Sicherheitsdienstleister wird empfohlen.

Die Tests sind als White-Box-Tests durchzuführen, den Prüfern sollten daher nach Möglichkeit alle für die Testdurchführung notwendigen Informationen zur Verfügung gestellt werden.

Wenn Tests nicht auf dem Originalsystem stattfinden können, ist sicherzustellen, dass Testsysteme identisch mit dem Originalsystem sind (eingesetzte Hard- und Software, Firmware-Stände et cetera). Dies ist – wie in Nummer 7.4 aufgeführt – im Abschlussbericht aufzuführen.

Hinweis: Das vorliegende Dokument beschreibt die verbindlich zu erfüllenden Anforderungen an die IS-Penetrationstests, IS-Kurzrevision und IS-Webcheck gemäß MSA-i-Kfz.

7.4.1.1 IS-Kurzrevision

Die IS-Kurzrevision dient der Unterstützung bei der Umsetzung und Optimierung der Informationssicherheit. Dabei werden auch Aspekte wie die Einbettung in die Infrastruktur oder organisatorische Fragen untersucht. Die Durchführung einer IS-Kurzrevision erfolgt nach dem Leitfaden für die IS-Revision BSI-LF-REVISION des BSI.

Sollten die Komponenten (vergleiche A-6.1-2) in ISO 27001 auf Basis vom IT-Grundschutz-zertifizierten Informationsverbünden betrieben werden, ist eine IS-Kurzrevision nicht erforderlich. Sollte zum Beispiel nur für den Informationsverbund des i-Kfz-Portals eine IT-Grundschutz- oder ISO-27001-Zertifizierung vorliegen, muss für die Informationsverbünde der Systeme Fachverfahren und der indirekt am Zulassungsprozess beteiligten Verfahren eine IS-Kurzrevision durchgeführt werden.

7.4.1.2 IS-Webcheck

Ein IS-Webcheck ist ein Spezialfall eines IS-Penetrationstests. Der IS-Webcheck dient der Prüfung des Sicherheitsstandards einer Internetpräsenz (Webanwendungen, Webserver, Anwendungen und Datenbanken).

Die Webanwendungen sind ohne Filterung durch ein Sicherheitsgateway zu prüfen, der prüfenden Person ist ein direkter Weg freigeschaltet. Die Funktion des Sicherheitsgateways ist im IS-Penetrationstest zu testen.

Als Prüftiefe ist ein nicht invasiver Schwachstellenscan (Schwachstellenscan, die Schwachstellen werden aber nicht ausgenutzt) zu wählen. Die Schwachstellen bei den Interaktionsmöglichkeiten des Anwenders wie Eingabefelder, Formularfelder oder Click-Buttons beziehungsweise teilweise bei den Zugriffen auf die Anwendungen und Datenbanken hinter der Webanwendung sind ohne Ausnutzen der Schwachstelle nicht nachweisbar und müssen daher ausgenutzt werden.

Hier sollte darauf geachtet werden, dass die Schwachstellen nur auf harmlose, nicht invasive Weise ausgenutzt werden.

Der IS-Webcheck sollte über das Internet durchgeführt werden.

Beim IS-Webcheck sind die OWASP Top 10 und mindestens die nachfolgenden Module zu testen und im IS-Webcheck-Bericht aufzuführen. Der IS-Webcheck sollte aber auch immer an die jeweiligen Gegebenheiten angepasst werden. Die Reihenfolge der Module kann individuell festgelegt werden, auch können einzelne Module mehrfach durchgeführt oder gleichzeitig abgearbeitet werden.

- Modul 1 – Schwachstellensuche
  - Korrektes Verhalten der Webanwendung
  - Aktualität der Patchstände und der eingesetzten Softwareversionen
  - Verschlüsselung entsprechend den aktuellen Sicherheitsanforderungen
  - Unerwünschte Informationspreisgabe
  - Eingabe und Interaktionsmöglichkeiten
- Modul 2 – Schwachstellentest
  - Eingabevalidierung
  - Session Handling
  - Zugriffskontrolle
  - Verschlüsselung
  - Fehlerhandling
  - Absicherung der beteiligten Datenbanken und Anwendungen
  - Absicherung von Dateiuploadmöglichkeiten und weiteren Interaktionsmöglichkeiten
  - versteckte Parameter/Verzeichnisse
- Modul 3 – Logische Fehler/Konfigurationsfehler
  - Fehler beim Aufbau oder Konfiguration zum Beispiel des Hypertext Transfer-Protokolls (HTTP)
  - Mögliche Seiteneffekte
- Modul 4 – Exploits (optional)

7.4.1.3 IS-Penetrationstest

Ein IS-Penetrationstest ist ein erprobtes und geeignetes Vorgehen, um das Angriffspotenzial auf ein IT-Netz, ein einzelnes IT-System oder eine Anwendung festzustellen. Der IS-Penetrationstest untersucht vorrangig die Schnittstellen einer Institution nach außen, über die potenzielle Angreifer die IT-Systeme kompromittieren könnten.

Als Prüftiefe ist ein technisches Sicherheitsaudit (die prüfende Person lässt sich von der Administration zeigen, welche Versionen in welcher Konfiguration eingesetzt werden und welche Härtungsmaßnahmen getroffen wurden) und ein nicht invasiver Schwachstellenscan (Schwachstellenscan des Netzwerkes, die Schwachstellen werden jedoch nicht ausgenutzt) zu wählen.

Der IS-Penetrationstest kann vor Ort oder über das Internet durchgeführt werden. Die Prüfung vor Ort ist zu bevorzugen.

Es sind mindestens die nachfolgenden Objekte zu prüfen oder im IS-Penetrationstest-Bericht nachvollziehbar zu begründen, warum auf diese verzichtet werden kann (zum Beispiel Objekt nicht vorhanden oder Verweis auf durchgeführte vergleichbare/gleichwertige Prüfungen). So kann damit flexibel auf jeweilige Gegebenheiten eingegangen werden.

- Netzkoppelelemente (Router, Switches, Gateways)
- Sicherheitsgateways und andere direkt IT-sicherheitsrelevante Objekte (Firewalls, Paketfilter, Intrusion Detection System (IDS), Virenscanner et cetera)
- Server (Datenbankserver, Webserver, Fileserver, Speichersysteme et cetera)
- Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop) mit vorgeschaltetem Sicherheitsgateway
- Relevante Clients
- Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)

Die Objekte sind in jedem Fall im IS-Penetrationstest-Bericht aufzuführen.

Beim Penetrationstest sind mindestens die nachfolgenden Module zu testen und im IS-Penetrationstest-Bericht aufzuführen. Die Reihenfolge der Module kann individuell festgelegt werden, auch können einzelne Module mehrfach durchgeführt oder gleichzeitig abgearbeitet werden.

- Modul 1 – konzeptionelle Schwächen
  - Prüfung der Unterlagen über die Prüfobjekte beziehungsweise den Prüfbereich auf Schwachstellen, offene Punkte und Auffälligkeiten.
- Modul 2 – Umsetzung Härtungsmaßnahmen
  - offene Ports (Es sollten nur die für die IT-Anwendung oder für das IT-System benötigten Ports erreichbar sein)
  - Schnittstellen (Prüfung auf nicht benötigte oder unerwünschte Schnittstellen, Einsatzzweck jeder Schnittstelle sollte durch die Administrierenden und Fachverantwortlichen genau erläutert werden können)
  - Patchstände und eingesetzte Softwareversionen (Aktualität der Patchstände und der eingesetzten Softwareversionen)
  - Zugangsvoraussetzungen zu Programmen/Authentisierung
  - Absicherung der Dienste/Regelwerke (Prüfung, ob nur die Funktionen verfügbar sind, die wirklich benötigt werden)
- Modul 3 – Bekannte Schwachstellen
  - Prüfung des Prüfobjekts auf bekannte Schwachstellen mittels Schwachstellenscannern
- Modul 4 – Exploits (optional)

7.5 Beantragung einer Zulassung

Nur zugelassene Kommunikationspartner dürfen im Rahmen des i-Kfz-Projekts mit der KBA-Infrastruktur kommunizieren. Die für die Kommunikation notwendige Zulassung muss von jedem Kommunikationspartner beantragt werden.

Der Prozess der Beantragung wird gestartet, indem die antragstellende Person die Beantragungsdokumente bei der KBA-Anwenderbetreuung bestellt. Im Folgenden wird der Beantragungsprozess grob skizziert.

Nr.	Initiator	Involvierte Instanz	Beschreibung
1	Antragstellende Person	KBA-Anwender-betreuung	Die antragstellende Person fordert bei der KBA-Anwenderbetreuung Antragsunterlagen zur Beantragung einer Zulassung zur Kommunikation mit der KBA-Infrastruktur im Rahmen i-Kfz an. Die antragstellende Person erhält die Zusendung der Unterlagen per E-Mail oder erhält die Zugangsdaten zum geschützten Bereich der KBA-Internetseite, in dem die Unterlagen per Download heruntergeladen werden können.
2a	KBA-Anwender-betreuung	Antragstellende Person	Die Antragsunterlagen werden an die antragstellende Person versendet.
2b[8]	Antragstellende Person	KBA-Portal	Die antragstellende Person lädt sich die Antragsunterlagen vom KBA-Portal herunter.
3	Antragstellende Person	Gegebenenfalls Portal-Betreiber	Die Erfüllung der in diesem Dokument vorgelegten Mindestsicherheitsanforderungen wird seitens der antragstellenden Person und gegebenenfalls auch weiterer Akteure (zum Beispiel seitens des Portal-Betreibers) sichergestellt.
4	Antragstellende Person	Gegebenenfalls Portal-Betreiber, KBA-Technischer Support	Die antragstellende Person führt selbst die technischen Tests der Kommunikationsstrecke mit der KBA-Infrastruktur durch oder veranlasst diese.
5	Antragstellende Person	Penetrationstests ausführendes Unternehmen	Die antragstellende Person beauftragt ein Unternehmen mit entsprechender Expertise, um die vorgeschriebenen Penetrationstests durchzuführen. Mit dem erfolgreichen Abschluss der Penetrationstests und Erstellung des Berichts ist dieser Schritt abgeschlossen.
6	Antragstellende Person	Auditierende Person	Es wird durch die antragstellende Person ein Audit beauftragt, um die Überprüfung der Einhaltung der Mindestsicherheitsanforderungen zu bestätigen (vergleiche Nummer 7.2).

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

Nr.	Initiator	Involvierte Instanz	Beschreibung
7	Antragstellende Person	KBA-Verfahrens-betreuung	Die ausgefüllten Antragsunterlagen mit Anlagen: Bericht zum erfolgreichen Abschluss des Penetrationstests Bericht zum erfolgreichen Abschluss des Audits, werden elektronisch an die in Nummer 9 genannte E-Mail-Adresse der Verfahrensbetreuung gesendet. Die Zulassung befindet sich somit in dem Zustand „initial beantragt“ und es folgt eine Prüfung der Unterlagen durch das KBA.

Tabelle 6: Grobe Schritte des Beantragungsprozesses einer Zulassung

7.6 Kündigung einer laufenden Zulassung

Eine laufende Zulassung kann jederzeit seitens des Kommunikationspartners beim KBA schriftlich gekündigt werden. Zur Wiederaufnahme der Zulassung ist eine erneute initiale Beantragung notwendig.

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

7.7 Ermahnungsverfahren, Sperrung einer Zulassung

Um ein reibungsloses Zulassungsverfahren anbieten zu können, müssen auch die Aspekte des Umgangs mit den gegebenenfalls auftretenden Versäumnissen geregelt werden. Insbesondere im Falle einer „eingeschränkt gültigen“ beziehungsweise „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 Ermahnung 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) Ermahnung zu versenden inklusive einer zweiten (finalen) Ersatzfrist. Sollte auch die finale Frist nicht eingehalten werden und die Erfüllung der auferlegten Auflage nicht feststellbar sein, so wird seitens des KBA eine dritte (und letzte) Ermahnung 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 kein Zugriff auf die i-Kfz-Web-Services mehr besteht.

7.8 Vorlage der Nachweise für Zulassungsbehörden

Alle Zulassungsbehörden (beziehungsweise dessen Dienstleister), die an der internetbasierten Fahrzeugzulassung teilnehmen, müssen die in Nummer 7.2 beziehungsweise die in Nummern 7.3 und 7.4 genannten Nachweise (Audit und Penetrationstest) für die relevanten Systembestandteile liefern. Hier gelten die oben beschriebenen Fristen. Details können den Fallbeispielen aus Nummer 8 entnommen werden.

8 Fallszenarien

In diesem Kapitel werden die Mindestsicherheitsanforderungen für verschiedene Fallszenarien aufgearbeitet. Dabei wird davon ausgegangen, dass die ZulB einen externen Dienstleister nutzt, der entweder über das Internet oder NdB-VN angebunden ist. Der Fall, dass die ZulB mehrere Dienstleister (zum Beispiel einen für das i-Kfz-Portal und einen anderen für die indirekt am Zulassungsprozess beteiligten Verfahren) nutzt, ist hier nicht berücksichtigt.

Wenn die Zulassungsbehörde zur Umsetzung von Komponenten Dienstleister beziehungsweise Dritte einsetzt, ist es Aufgabe der Zulassungsbehörde, sicherzustellen, dass der beauftragte Dienstleiter die Anforderungen erfüllt beziehungsweise nur Dienstleiter nutzt, die die Anforderungen erfüllen. Wenn die beauftragten Dienstleiter wiederum einen Dienstleiter einsetzen, muss dieser sicherstellen, dass auch dessen Dienstleiter die von der Zulassungsbehörde gestellten Anforderung erfüllt und so weiter.

Die Zulassungsbehörde kann wie in den Nummern 7.2 und 7.4 aufgezeigt auf bereits durchgeführte Prüfungen verweisen.

Ziel der Fallszenarien ist es, dass auf einen Blick ersichtlich ist, welche Mindestsicherheitsanforderungen je spezifischem Fall von wem eingehalten werden müssen.

Dafür werden sechs Szenarien unterschieden:

1. Zulassungsbehörde oder Dienstleister betreibt alle Komponenten (i-Kfz-Portal, Systeme der Fachverfahren und indirekt am Zulassungsprozess beteiligte Verfahren)
2. Zulassungsbehörde betreibt die Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren (ein Dienstleister betreibt das i-Kfz-Portal) – Anbindung des i-Kfz-Portals über das Internet (Schnittstellen Xi und Yi)

3. Zulassungsbehörde betreibt die Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren (ein Dienstleister betreibt das i-Kfz-Portal) – Anbindung des i-Kfz-Portals über das NdB-VN (Schnittstellen Xn und Yn), Anbindung der indirekt am Zulassungsprozess beteiligten Verfahren über das Internet (Schnittstellen Xi und Yi)
4. Zulassungsbehörde betreibt die Systeme der Fachverfahren (ein Dienstleister betreibt das i-Kfz-Portal und die indirekt am Zulassungsprozess beteiligten Verfahren) – Anbindung beider an die Systeme der Fachverfahren über das Internet (Schnittstellen Xi und Yi)
5. Zulassungsbehörde betreibt die Systeme der Fachverfahren (ein Dienstleister betreibt das i-Kfz-Portal und die indirekt am Zulassungsprozess beteiligten Verfahren) – Anbindung beider an die Systeme der Fachverfahren über das NdB-VN (Schnittstellen Xn und Yn)
6. Zulassungsbehörde betreibt die indirekt am Zulassungsprozess beteiligten Verfahren (ein Dienstleister betreibt das i-Kfz-Portal und die Systeme der Fachverfahren) – Anbindung indirekt am Zulassungsprozess beteiligter Verfahren über das Internet (Schnittstellen Xi und Yi)

Hinweis: Des Weiteren wird davon ausgegangen, dass indirekt am Zulassungsprozess beteiligte Verfahren (vergleiche Antragstellende Person sowie § 19 Absatz 2 FZV) vorhanden sind. Wenn durch einen unabhängigen Dritten schriftlich bestätigt wird, dass indirekt am Zulassungsprozess beteiligte Verfahren vollständig von den i-Kfz-Verfahren getrennt werden und keine Verbindungen bestehen, müssen die Verfahren nicht getestet werden. Dies ist entsprechend im Test-Bericht aufzuführen. Gleiches gilt, wenn indirekt am Zulassungsprozess beteiligte Verfahren nicht vorhanden sind. In diesem Fall ist dies ebenfalls entsprechend im Test-Bericht aufzuführen. Dies gilt auch für den IS-Webcheck. Wenn im Test-Bericht bestätigt wird, dass es keine Schnittstellen zum beziehungsweise ins Internet gibt, kann auf einen IS-Webcheck verzichtet werden.

Hinweis: In diesem Kapitel werden nicht abschließend alle möglichen Fälle dargestellt. Generell kann immer vor Beauftragung eines Audits oder Penetrationstests eine Abstimmung mit dem KBA durchgeführt werden.

Hinweis: Auch das jeweilige Landesnetz darf für die Kommunikation zwischen dem i-Kfz-Portal und den Fachverfahren beziehungsweise der Zulassungsbehörde genutzt werden. Es gelten seitens des KBA die gleichen Anforderungen wie bei der Nutzung des NdB-VN und der Zulassungsbehörde-NdB-VN-DMZ (vergleiche auch Nummer 5.3.6).

8.1 Zulassungsbehörde oder Dienstleister betreibt alle Komponenten

Der externe Dienstleister oder die Zulassungsbehörde selbst betreibt alle Komponenten: das i-Kfz-Portal, die Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren (siehe § 19 FZV) beziehungsweise Portale.

8.1.1 Anforderungen an den Betreiber (Zulassungsbehörde oder Dienstleister):

In diesem Fall müssen vom Betreiber alle allgemeinen Sicherheitsanforderungen sowie die Sicherheitsanforderungen an alle Schnittstellen beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-1	A-6.2.1-1
A-6.1-2	A-6.2.1-2
A-6.1-3	A-6.2.1-3
A-6.1-4	A-6.2.1-4
A-6.1-5	A-6.2.1-5
A-6.1-6	A-6.2.3-1
A-6.1-7	A-6.2.3-2
A-6.1-8	A-6.2.3-3
A-6.1-9	A-6.2.4-1
A-6.1-10	A-6.2.4-2
A-6.1-11	A-6.2.6-1
A-6-1-12	A-6.2.6-2
A-6.1-13	A-6.2.6-3
A-6.1-14	A-6.2.7-1
	A-6.2.7-2
	A-6.2.7-3
	A-6.2.7-4
	A-6.2.8-1
	A-6.2.8-2
	A-6.2.8-3
	A-6.2.8-4
	A-6.2.9-1
	A-6.2.9-2

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
	A-6.2.9-3
	A-6.2.10-1
	A-6.2.10-2
	A-6.2.10-3
	A-6.2.11-1
	A-6.2.11-2
	A-6.2.11-3

Tabelle 7: Anforderungen Fallszenario 8.1.1

Hinweis: In den Sicherheitsanforderungen an die Schnittstellen sind sowohl die Schnittstellen Xi und Yi als auch die Schnittstellen Xn und Yn aufgenommen. Falls nur die Schnittstellen Xi und Yi genutzt werden, müssen die Anforderungen an die Schnittstellen Xn und Yn nicht erfüllt werden, ebenso im umgekehrten Fall.

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung bestätigt werden (siehe Nummer 7.2). Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund des i-Kfz-Portals, der Systeme der Fachverfahren und der indirekt am Zulassungsprozess beteiligten Verfahren vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[9]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Ja	Ja	Ja
Systeme des Fachverfahrens	Ja	Ja	Ja
Indirekt am Zulassungsprozess beteiligte Verfahren	Ja	Ja	Ja

Tabelle 8: Penetrationstests Fallszenario 8.1.1

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben in Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

8.2 Zulassungsbehörde betreibt die Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren (ein Dienstleister betreibt das i-Kfz-Portal) – Anbindung des i-Kfz-Portals über das Internet (Schnittstellen Xi und Yi)

Die Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren (vergleiche § 19 FZV) werden von der Zulassungsbehörde betrieben. Ein externer Dienstleister betreibt nur das i-Kfz-Portal.

	i-Kfz-Portal	*Systeme der Fachverfahren*	*Indirekt am Zulassungsprozess beteiligte Verfahren*
Externer Dienstleister	x		
Zulassungsbehörde		x	x

Tabelle 9: Fallszenario 8.2

8.2.1 Anforderungen an die Zulassungsbehörde:

In diesem Fall müssen von der Zulassungsbehörde alle allgemeinen Sicherheitsanforderungen bezogen auf die Systeme des Fachverfahrens und die indirekt am Zulassungsprozess beteiligten Verfahren, außer A-6.1-1, sowie die Sicherheitsanforderungen an die Schnittstellen C, D, Xi und Yi beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-2	A-6.2.3-1
A-6.1-3	A-6.2.3-2
A-6.1-4	A-6.2.3-3
A-6.1-5	A-6.2.4-1
A-6.1-6	A-6.2.4-2
A-6.1-7	A-6.2.8-1
A-6.1-8	A-6.2.8-2
A-6.1-9	A-6.2.8-3
A-6.1-10	A-6.2.8-4
A-6.1-11	A-6.2.9-1
A-6.1-12	A-6.2.9-2
A-6-1-13	A-6.2.9-3
A-6.1-14	

Tabelle 10: Anforderungen Fallszenario 8.2.1

[9] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung entsprechend Nummer 7.2 bestätigt werden. Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund der Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[10]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Nein	Nein	Nein
Systeme des Fachverfahrens	Ja	Ja	Ja
Indirekt am Zulassungsprozess beteiligte Verfahren	Ja	Ja	Ja

Tabelle 11: Penetrationstests Fallszenario 8.2.1

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben aus Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

8.2.2 Anforderungen an den Betreiber des i-Kfz-Portals:

In diesem Fall müssen vom Portalbetreiber alle allgemeinen Sicherheitsanforderungen bezogen auf das i-Kfz-Portal sowie die Sicherheitsanforderungen an die Schnittstellen A, F, H und Xi beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-1	A-6.2.1-1
A-6.1-2	A-6.2.1-2
A-6.1-3	A-6.2.1-3
A-6.1-4	A-6.2.1-4
A-6.1-5	A-6.2.1-5
A-6.1-6	A-6.2.6-1
A-6.1-7	A-6.2.6-2
A-6.1-8	A-6.2.6-3
A-6.1-9	A-6.2.7-1
A-6.1-10	A-6.2.7-2
A-6.1-11	A-6.2.7-3
A-6.1-12	A-6.2.7-4
A-6.1-13	A-6.2.8-1
A-6.1-14	A-6.2.8-2
	A-6.2.8-3
	A-6.2.8-4

Tabelle 12: Anforderungen Fallszenario 8.2.2

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung entsprechend Nummer 7.2 bestätigt werden. Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund des i-Kfz-Portals vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[10]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Ja	Ja	Ja
Systeme des Fachverfahrens	Nein	Nein	Nein
Indirekt am Zulassungsprozess beteiligte Verfahren	Nein	Nein	Nein

Tabelle 13: Penetrationstests Fallszenario 8.2.2

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben aus Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

8.3 Zulassungsbehörde betreibt die Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren (ein Dienstleister betreibt das i-Kfz-Portal) – Anbindung des i-Kfz-Portals über das NdB-VN (Schnittstellen Xn und Yn), Anbindung der indirekt am Zulassungsprozess beteiligten Verfahren über das Internet (Schnittstellen Xi und Yi)

[10] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.

Die Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren (vergleiche § 19 FZV) werden von der Zulassungsbehörde betrieben. Ein externer Dienstleister betreibt nur das i-Kfz-Portal.

	i-Kfz-Portal	*Systeme der Fachverfahren*	*Indirekt am Zulassungsprozess beteiligte Verfahren*
Externer Dienstleister	x		
Zulassungsbehörde		x	x

Tabelle 14: Penetrationstests Fallszenario 8.3

Die Anbindung des i-Kfz-Portals an die Systeme der Fachverfahren findet über das NdB-VN statt, es wird die Komponente Portal-NdB-VN-Cnn mit den Schnittstellen Xn und Yn verwendet. Die Anbindung der indirekt am Zulassungsprozess beteiligten Verfahren an die Systeme der Fachverfahren findet über die Zulassungsbehörden-Internet-DMZ statt, es wird die Komponente Internet-Cnn mit den Schnittstellen Xi und Yi verwendet.

8.3.1 Anforderungen an die Zulassungsbehörde:

In diesem Fall müssen von der Zulassungsbehörde alle allgemeinen Sicherheitsanforderungen bezogen auf die Systeme der Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren, außer A-6.1-1, sowie die Sicherheitsanforderungen an die Schnittstellen C, D, Xi, Yi, Xn und Yn beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-2	A-6.2.3-1
A-6.1-3	A-6.2.3-2
A-6.1-4	A-6.2.3-3
A-6.1-5	A-6.2.4-1
A-6.1-6	A-6.2.4-2
A-6.1-7	A-6.2.8-1
A-6.1-8	A-6.2.8-2
A-6.1-9	A-6.2.8-3
A-6.1-10	A-6.2.8-4
A-6.1-11	A-6.2.9-1
A-6.1-12	A-6.2.9-2
A-6.1-13	A-6.2.9-3
A-6.1-14	A-6.2.10-1
	A-6.2.10-2
	A-6.2.10-3
	A-6.2.11-1
	A-6.2.11-2
	A-6.2.11-3

Tabelle 15: Anforderungen Fallszenario 8.3.1

Hinweis! Die „indirekt am Zulassungsprozess beteiligten Verfahren“, wie zum Beispiel die Wunschkennzeichenreservierung, sind meist über das Internet erreichbar. Daher müssen die Schnittstellen Xi und Yi genutzt und auch die Anforderungen an Xi und Yi geprüft werden.

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung entsprechend Nummer 7.2 bestätigt werden. Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund der Systeme der Fachverfahren und die indirekt am Zulassungsprozess beteiligten Verfahren vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[11]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Nein	Nein	Nein
Systeme des Fachverfahrens	Ja	Ja	Ja
Indirekt am Zulassungsprozess beteiligte Verfahren	Ja	Ja	Ja

Tabelle 16: Penetrationstests Fallszenario 8.3.1

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben aus Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

[11] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.

8.3.2 Anforderungen an den Betreiber des i-Kfz-Portals:

In diesem Fall müssen vom Betreiber des i-Kfz-Portals neben den NdB-VN-Nutzerpflichten alle allgemeinen Sicherheitsanforderungen bezogen auf das i-Kfz-Portal sowie die Sicherheitsanforderungen an die Schnittstellen A, F, H und Xn beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-1	A-6.2.1-1
A-6.1-2	A-6.2.1-2
A-6.1-3	A-6.2.1-3
A-6.1-4	A-6.2.1-4
A-6.1-5	A-6.2.1-5
A-6.1-6	A-6.2.6-1
A-6.1-7	A-6.2.6-2
A-6.1-8	A-6.2.6-3
A-6.1-9	A-6.2.7-1
A-6.1-10	A-6.2.7-2
A-6.1-11	A-6.2.7-3
A-6.1-12	A-6.2.7-4
A-6.1-13	A-6.2.10-1
A-6.1-14	A-6.2.10-2
	A-6.2.10-3

Tabelle 17: Anforderungen Fallszenario 8.3.2

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung entsprechend Nummer 7.2 bestätigt werden. Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund des i-Kfz-Portals vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[12]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Ja	Ja	Ja
Systeme des Fachverfahrens	Nein	Nein	Nein
Indirekt am Zulassungsprozess beteiligte Verfahren	Nein	Nein	Nein

Tabelle 18: Penetrationstests Fallszenario 8.3.2

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben aus Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

8.4 Zulassungsbehörde betreibt die Systeme der Fachverfahren (ein Dienstleister betreibt das i-Kfz-Portal und die indirekt am Zulassungsprozess beteiligten Verfahren) – Anbindung beider an die Systeme der Fachverfahren über das Internet (Schnittstellen Xi und Yi)

Nur die Systeme der Fachverfahren werden von der Zulassungsbehörde betrieben. Ein externer Dienstleister betreibt das i-Kfz-Portal und die indirekt am Zulassungsprozess beteiligten Verfahren (vergleiche § 19 FZV) beziehungsweise Portale.

	i-Kfz-Portal	*Systeme der Fachverfahren*	*Indirekt am Zulassungsprozess beteiligte Verfahren*
Externer Dienstleister	x		x
Zulassungsbehörde		x	

Tabelle 19: Fallszenario 8.4

Die Anbindung des Betreibers des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren an die Systeme der Fachverfahren findet über die Zulassungsbehörden-Internet-DMZ statt, es wird die Komponente Internet-Cnn mit den Schnittstellen Xi und Yi verwendet.

Hinweis: Wenn für die indirekt am Zulassungsprozess beteiligten Verfahren nicht derselbe Dienstleister wie der für das i-Kfz-Portal genutzt wird, dann ist das Fallszenario 8.2 oder 8.3 zu wählen. Für die indirekt am Zulassungsprozess beteiligten Verfahren kann dann wie in den Nummern 7.2 und 7.4 aufgezeigt auf bereits durchgeführte Prüfungen des Dienstleisters verwiesen werden.

[12] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.

8.4.1 Anforderungen an die Zulassungsbehörde:

In diesem Fall müssen von der Zulassungsbehörde alle allgemeinen Sicherheitsanforderungen bezogen auf die Systeme der Fachverfahren, außer A-6.1-1, sowie die Sicherheitsanforderungen an die Schnittstellen C, D, Xi und Yi beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-2	A-6.2.3-1
A-6.1-3	A-6.2.3-2
A-6.1-4	A-6.2.3-3
A-6.1-5	A-6.2.4-1
A-6.1-6	A-6.2.4-2
A-6.1-7	A-6.2.8-1
A-6.1-8	A-6.2.8-2
A-6.1-9	A-6.2.8-3
A-6.1-10	A-6.2.8-4
A-6.1-11	A-6.2.9-1
A-6.1-12	A-6.2.9-2
A-6.1-13	A-6.2.9-3
A-6.1-14	A-6.2.3-2

Tabelle 20: Anforderungen Fallszenario 8.4.1

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung entsprechend siehe Nummer 7.2 bestätigt werden. Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund der Systeme der Fachverfahren vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[13]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Nein	Nein	Nein
Systeme des Fachverfahrens	Ja	Ja	Ja
Indirekt am Zulassungsprozess beteiligte Verfahren	Nein	Nein	Nein

Tabelle 21: Penetrationstests Fallszenario 8.4.1

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben in Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

8.4.2 Anforderungen an den Betreiber des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren:

In diesem Fall müssen vom Betreiber des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren alle allgemeinen Sicherheitsanforderungen, bezogen auf das i-Kfz-Portal und die indirekt am Zulassungsprozess beteiligten Verfahren sowie die Sicherheitsanforderungen an die Schnittstellen A, F, H und Xi beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-1	A-6.2.1-1
A-6.1-2	A-6.2.1-2
A-6.1-3	A-6.2.1-3
A-6.1-4	A-6.2.1-4
A-6.1-5	A-6.2.1-5
A-6.1-6	A-6.2.6-1
A-6.1-7	A-6.2.6-2
A-6.1-8	A-6.2.6-3
A-6.1-9	A-6.2.7-1
A-6.1-10	A-6.2.7-2
A-6.1-11	A-6.2.7-3
A-6.1-12	A-6.2.7-4
A-6.1.13	A-6.2.8-1

[13] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-14	A-6.2.8-2
A-6.1-11	A-6.2.8-3
	A-6.2.8-4

Tabelle 22: Anforderungen Fallszenario 8.4.2

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung bestätigt werden (siehe Nummer 7.2). Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[14]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Ja	Ja	Ja
Systeme des Fachverfahrens	Nein	Nein	Nein
Indirekt am Zulassungsprozess beteiligte Verfahren	Ja	Ja	Ja

Tabelle 23: Penetrationstests Fallszenario 8.4.2

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben aus Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

8.5 Zulassungsbehörde betreibt die Systeme der Fachverfahren (ein Dienstleister betreibt das i-Kfz-Portal und die indirekt am Zulassungsprozess beteiligten Verfahren) – Anbindung beider an die Systeme der Fachverfahren über das NdB-VN (Schnittstellen Xn und Yn)

Nur die Systeme der Fachverfahren werden von der Zulassungsbehörde betrieben. Ein externer Dienstleister betreibt das i-Kfz-Portal und die indirekt am Zulassungsprozess beteiligten Verfahren (vergleiche § 19 FZV) beziehungsweise Portale.

	i-Kfz-Portal	*Systeme der Fachverfahren*	*Indirekt am Zulassungsprozess beteiligte Verfahren*
Externer Dienstleister	x		x
Zulassungsbehörde		x	

Tabelle 24: Fallszenario 8.5

Die Anbindung des Betreibers des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren an die Systeme der Fachverfahren findet über das NdB-VN statt, es wird die Komponente Portal-NdB-VN-Cnn mit den Schnittstellen Xn und Yn verwendet.

Hinweis: Wenn für die indirekt am Zulassungsprozess beteiligten Verfahren nicht derselbe Dienstleister wie der für das i-Kfz-Portal genutzt wird, dann ist das Fallszenario 8.2 oder 8.3 zu wählen. Für die indirekt am Zulassungsprozess beteiligten Verfahren kann dann wie in den Nummern 7.2 und 7.4 aufgezeigt auf bereits durchgeführte Prüfungen des Dienstleisters verwiesen werden.

8.5.1 Anforderungen an die Zulassungsbehörde:

In diesem Fall müssen von der Zulassungsbehörde alle allgemeinen Sicherheitsanforderungen bezogen auf die Systeme der Fachverfahren, außer A-6.1-1, sowie die Sicherheitsanforderungen an die Schnittstellen C, D, Xn und Yn beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-2	A-6.2.3-1
A-6.1-3	A-6.2.3-2
A-6.1-4	A-6.2.3-3
A-6.1-5	A-6.2.4-1
A-6.1-6	A-6.2.4-2
A-6.1-7	A-6.2.10-1
A-6.1-8	A-6.2.10-2
A-6.1-9	A-6.2.10-3
A-6.1-10	A-6.2.11-1
A-6.1-11	A-6.2.11-2

[14] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-12	A-6.2.11-3
A-6.1-13	
A-6.1-14	

Tabelle 25: Anforderungen Fallszenario 8.5.1

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung entsprechend siehe Nummer 7.2 bestätigt werden. Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund der Systeme der Fachverfahren vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[15]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Nein	Nein	Nein
Systeme des Fachverfahrens	Ja	Nein	Ja
Indirekt am Zulassungsprozess beteiligte Verfahren	Nein	Nein	Nein

Tabelle 26: Penetrationstests Fallszenario 8.5.1

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben aus Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

8.5.2 Anforderungen an den Betreiber des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren:

In diesem Fall müssen vom Betreiber des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren, neben den NdB-VN-Nutzerpflichten, alle allgemeinen Sicherheitsanforderungen bezogen auf das i-Kfz-Portal und die indirekt am Zulassungsprozess beteiligten Verfahren sowie die Sicherheitsanforderungen an die Schnittstellen A, F, H und Xn beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-1	A-6.2.1-1
A-6.1-2	A-6.2.1-2
A-6.1-3	A-6.2.1-3
A-6.1-4	A-6.2.1-4
A-6.1-5	A-6.2.1-5
A-6.1-6	A-6.2.6-1
A-6.1-7	A-6.2.6-2
A-6.1-8	A-6.2.6-3
A-6.1-9	A-6.2.7-1
A-6.1-10	A-6.2.7-2
A-6.1-11	A-6.2.7-3
A-6.1-12	A-6.2.7-4
A-6.1-13	A-6.2.10-1
A-6.1-14	A-6.2.10-2
	A-6.2.10-3

Tabelle 27: Anforderungen Fallszenario 8.5.2

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung entsprechend Nummer 7.2 bestätigt werden. Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[16]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Ja	Ja	Ja
Systeme des Fachverfahrens	Nein	Nein	Nein
Indirekt am Zulassungsprozess beteiligte Verfahren	Ja	Ja	Ja

Tabelle 28: Penetrationstests Fallszenario 8.5.2

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben aus Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

[15] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.
[16] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.

8.6 Zulassungsbehörde betreibt die indirekt am Zulassungsprozess beteiligten Verfahren (ein Dienstleister betreibt das i-Kfz-Portal und die Systeme der Fachverfahren) – Anbindung indirekt am Zulassungsprozess beteiligter Verfahren über das Internet (Schnittstellen Xi und Yi)

Nur die indirekt am Zulassungsprozess beteiligten Verfahren (vergleiche § 19 FZV) werden von der Zulassungsbehörde betrieben. Ein externer Dienstleister betreibt das i-Kfz-Portal und die Systeme der Fachverfahren.

	i-Kfz-Portal	*Systeme der Fachverfahren*	*indirekt am Zulassungsprozess beteiligte Verfahren*
Externer Dienstleister	x	x	
Zulassungsbehörde			x

Tabelle 29 Fallszenario 8.6

Die Anbindung der indirekt am Zulassungsprozess beteiligten Verfahren an die Systeme der Fachverfahren findet über die Internet-DMZ statt, es wird die Komponente Internet-Cnn mit den Schnittstellen Xi und Yi verwendet.

Hinweis! Wenn für die Systeme der Fachverfahren nicht derselbe Dienstleister wie der für das i-Kfz-Portal genutzt wird, dann ist das Fallszenario 8.2 oder 8.3 zu wählen. Für die Systeme der Fachverfahren kann wie in den Nummern 7.2 und 7.4 aufgezeigt auf bereits durchgeführte Prüfungen des Dienstleisters verwiesen werden.

8.6.1 Anforderungen an die Zulassungsbehörde:

In diesem Fall müssen von der Zulassungsbehörde alle allgemeinen Sicherheitsanforderungen bezogen auf die indirekt am Zulassungsprozess beteiligten Verfahren, außer A-6.1-1, sowie die Sicherheitsanforderungen an die Schnittstelle Xi beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-2	A-6.2.8-1
A-6.1-3	A-6.2.8-2
A-6.1-4	A-6.2.8-3
A-6.1-5	A-6.2.8-4
A-6.1-6	
A-6.1-7	
A-6.1-8	
A-6.1-9	
A-6.1-10	
A-6.1-11	
A-6.1-12	
A-6.1-13	
A-6.1-14	

Tabelle 30: Anforderungen Fallszenario 8.6.1

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung entsprechend Nummer 7.2 bestätigt werden. Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund der indirekt am Zulassungsprozess beteiligten Verfahren vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[17]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Nein	Nein	Nein
Systeme des Fachverfahrens	Nein	Nein	Nein
Indirekt am Zulassungsprozess beteiligte Verfahren	Ja	Ja	Ja

Tabelle 31: Penetrationstests Fallszenario 8.6.1

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben aus Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

[17] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.

8.6.2 Anforderungen an den Betreiber des i-Kfz-Portals und der Systeme der Fachverfahren:

In diesem Fall müssen vom Betreiber des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren alle allgemeinen Sicherheitsanforderungen bezogen auf das i-Kfz-Portal und die Systeme der Fachverfahren sowie die Sicherheitsanforderungen an die Schnittstellen A, C, D, F, H, Xi und Yi beachtet werden.

Allgemeine Sicherheitsanforderungen	*Sicherheitsanforderungen an die Schnittstellen*
A-6.1-1	A-6.2.1-1
A-6.1-2	A-6.2.1-2
A-6.1-3	A-6.2.1-3
A-6.1-4	A-6.2.1-4
A-6.1-5	A-6.2.1-5
A-6.1-6	A-6.2.3-1
A-6.1-7	A-6.2.3-2
A-6.1-8	A-6.2.3-3
A-6.1-9	A-6.2.4-1
A-6.1-10	A-6.2.4-2
A-6.1-11	A-6.2.6-1
A-6.1-12	A-6.2.6-2
A-6.1-13	A-6.2.6-3
A-6.1-14	A-6.2.7-1
	A-6.2.7-2
	A-6.2.7-3
	A-6.2.7-4
	A-6.2.8-1
	A-6.2.8-2
	A-6.2.8-3
	A-6.2.8-4
	A-6.2.9-1
	A-6.2.9-2
	A-6.2.9-3

Tabelle 32: Anforderungen Fallszenario 8.6.2

Die Anforderungen müssen in Form eines Audits alle drei Jahre geprüft und deren Erfüllung entsprechend Nummer 7.2 bestätigt werden. Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz für den Informationsverbund des i-Kfz-Portals und der indirekt am Zulassungsprozess beteiligten Verfahren vorliegt, müssen nur die zusätzlichen Anforderungen gemäß Nummer 7.3 geprüft werden.

Die Penetrationstests sind alle zwei Jahre entsprechend Nummer 7.4 durchzuführen.

	IS-Kurzrevision[18]	*IS-Webcheck*	*Penetrationstest*
i-Kfz-Portal	Ja	Ja	Ja
Systeme des Fachverfahrens	Ja	Ja	Ja
Indirekt am Zulassungsprozess beteiligte Verfahren	Nein	Nein	Nein

Tabelle 33: Penetrationstests Fallszenario 8.6.2

Die Verwendung bereits durchgeführter Penetrationstests oder Sicherheitsüberprüfungen ist unter Einhaltung der Vorgaben aus Nummer 7.2 beziehungsweise Nummer 7.4 möglich.

9 Ansprechpersonen beim KBA

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

Technischer Support	
Telefon	(0461) 316 – 1400
E-Mail	KBA-ServiceDesk@kba.de

Tabelle 34: Kontaktdaten des technischen Supports

[18] Wenn eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz vorliegt, ist die IS-Kurzrevision nicht erforderlich.

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

Anwenderbetreuung	
Telefon	(0461) 316 – 1717
E-Mail	Anwenderbetreuung@kba.de
Anschrift	Kraftfahrt-Bundesamt Anwenderbetreuung 24932 Flensburg

Tabelle 35: Kontaktdaten der Anwenderbetreuung

Vorlagen zum Nachweis der Einhaltung von Mindestsicherheitsanforderungen können an die Verfahrensbetreuung gesendet werden:

Verfahrensbetreuung	
Telefon	(0461) 316 – 2525
E-Mail	211-Verfahrensbetreuung@kba.de
Anschrift	Kraftfahrt-Bundesamt Verfahrensbetreuung Sgb. 211 24932 Flensburg

Tabelle 36: Kontaktdaten der Verfahrensbetreuung

10 Quellen

AnVN	Anschlussbedingungen für das Verbindungsnetz, in der jeweils gültigen Fassung, http://www.intranet.doi-de.net/DE/Downloads/Rahmenvertrag-Leistungskatalog/rahmenvertrag-leistungskatalog_node.html
BDSG	Bundesdatenschutzgesetz (BDSG), Ausfertigungsdatum: 30. Juni 2017, zuletzt geändert durch Artikel 12 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626), http://www.gesetze-im-internet.de/bdsg_2018/
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, https://www.lfd.niedersachsen.de/download/71664/Orientierungshilfe_Mandantenfaehigkeit_AK_Technik_.pdf
BSI-ISI	BSI-Standards zur Internet-Sicherheit (ISi-Reihe) in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/6620942
BSI-ISI-LANA	BSI-Standards zur Internet-Sicherheit (ISi-Reihe): Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA) in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/6620942
BSI-ISI-SVR	BSI-Standards zur Internet-Sicherheit (ISi-Reihe): Absicherung eines Servers [ISi-Server]) in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/6620942
BSI-ISI-WEB-SVR	BSI-Standards zur Internet-Sicherheit (Isi-Reihe): Sicheres Bereitstellen von Web-Angeboten (Isi-Web-Server) in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/6620942
BSI-ITG-200-2	BSI-Standard 200-2: IT-Grundschutz Methodik, in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/10027846
BSI-ITG-ZERT	BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz: Zertifizierungsschema, in der jeweils gültigen Fassung; https://www.bsi.bund.de/dok/6617420
BSI-LF-PENTEST	BSI Praxis-Leitfaden: IT-Sicherheits-Penetrationstest, in der jeweils gültigen Fassung, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/Pen_Test_und_IS_Webcheck/pent-tests-und-is-webcheck_node.html
BSI-LF-REVISION	BSI Leitfaden IS-Revision, in der jeweils gültigen Fassung, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/ISRevision/Leitfaden/leitfaden_node.html
BSI-LF-WEBCHECK	BSI Praxis-Leitfaden: IT-Sicherheits-Webcheck, in der jeweils gültigen Fassung, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/Pen_Test_und_IS_Webcheck/pent-tests-und-is-webcheck_node.html
BSI-MS-CLOUD	Mindeststandard des BSI nach § 8 Absatz 1 Satz 1 BSIG zur Nutzung externer beziehungsweise Mitnutzung Cloud-Dienste in der Bundesverwaltung in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/11056716

BSI-MS-PROT	Mindeststandard des BSI nach § 8 Absatz 1 Satz 1 zur Protokollierung und Detektion von Cyber-Angriffen in der Bundesverwaltung, in der jeweils gültigen Fassung; https://www.bsi.bund.de/dok/11601834
BSI-MS-TLS	Mindeststandard des BSI nach § 8 Absatz 1 Satz 1 BSIG zur Verwendung von Transport Layer Security (TLS), in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/6623844
BSI-TR02102	BSI TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, in den jeweils gültigen Fassungen, https://www.bsi.bund.de/dok/6615148
BSI-TR02102-3	BSI Technische Richtlinie TR-02102-3: Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/6615148
BSI-TR03107-1	BSI Technische Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government, in der jeweils gültigen Fassung; https://www.bsi.bund.de/dok/6623610
BSI-TR03107-2	BSI Technische Richtlinie TR-03107-2: Elektronische Identitäten und Vertrauensdienste im E-Government, Teil 2: Schriftformersatz mit elektronischem Identitätsnachweis, in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/6623610
BSI-TR03124-1	BSI Technische Richtlinie TR-03124-1: eID-Client, Part 1: Specifications, in der jeweils gültigen Fassung, https://www.bsi.bund.de/dok/6615282
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO), Geltung ab 25. Mai 2018, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679
EIDAS-VO	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, Geltung ab 1. Juli 2016, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014R0910
FZV	Verordnung zum Neuerlass der Fahrzeug-Zulassungsverordnung und zur Änderung weiterer Vorschriften (Fahrzeug-Zulassungsverordnung – FZV), Referentenentwurf, Bearbeitungsstand: 15. Februar 2023
IznAaKBAfB	Informationen zur netztechnischen Anbindung an das KBA für Behörden, in der jeweils gültigen Fassung
KBA-ExtTU	KBA, Internetbasierte Fahrzeugzulassung (i-Kfz), Beschreibung der externen Testumgebung
KBAG	Gesetz über die Errichtung eines Kraftfahrt-Bundesamts (KBAG), Ausfertigungsdatum: 4. August 1951, zuletzt geändert durch Artikel 2 des Gesetzes vom 28. November 2016 (BGBl. I S. 2722), http://www.gesetze-im-internet.de/kbag/index.html
KBA-TDV	KBA, Testdatenverzeichnis für internetbasierte Fahrzeugzulassung
LIöV	Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung 2018 der Arbeitsgruppe des IT-Planungsrats „Informationssicherheit, Version 2.0 Stand 06.12.2018, https://www.it-planungsrat.de/fileadmin/beschluesse/2019/Beschluss2019-04_TOP12_Anlage_Leitlinie.pdf
OWASP Top 10	OWASP Top 10 Web Application Security Risks, in der jeweils gültigen Fassung, https://owasp.org/www-project-top-ten/
RFC2818	E. Rescorla, „HTTP over TLS“, in der jeweils gültigen Fassung
SDÜGK	Standards für die Datenübermittlung zur Nutzung der Großkundenschnittstelle für Großkunden, in der jeweils gültigen Fassung
SDÜiKP	Standards für die Datenübermittlung an das KBA – Datenaustausch mit i-Kfz-Portalen, in der jeweils gültigen Fassung
SDÜZulB	Standards für die Datenübermittlung an das KBA – Datenaustausch mit den Zulassungsbehörden, in der jeweils gültigen Fassung
StVGuaÄndG	Viertes Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze (4. StVGuaÄndG), Geltung ab 31. August 2013, http://www.buzer.de/gesetz/10899/index.htm
UP-LIöV	Umsetzungsplan – Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung 2018, Version 1.0 vom 5. Februar 2020, https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-05_TOP_09_Umsetzungsplan.pdf