Verpflichtungserklärung

für autonome Datenübermittlung (Eigenbetrieb) oder des Betreibers einer Kopfstelle

Stand: Januar 2023

§ 1

Bedingungen und Mindestanforderungen für den Betrieb bzw. die Datenkommunikation über eine Kopfstelle:

(1) Die Datenkommunikation mit dem Kraftfahrt-Bundesamt (KBA) kann über das NdB-Verbindungsnetz (NdB-VN) und an dieses Netz angeschlossene Landesverwaltungsnetze erfolgen. Der Zugriff auf die Online-Dialoganwendungen des KBAs kann entweder unter Nutzung der KBA-Browser-Dialoge (KBA-Portal) oder die vom KBA zur Verfügung gestellten Webservices erfolgen.

Der Zugriff auf die Webservices durch Anwendungen /Anwendungsserver über das NdB-Verbindungsnetz und ggf. angeschlossene Landesverwaltungsnetze erfolgt über HTTPS auf Basis einer TLS-Verschlüsselung (TLS 1.2 und höher) mit Authentisierung über ein dateibasiertes Zertifikat.

(2) Bei der Nutzung der Webservices durch Anwendungsserver ist für die erforderliche Verschlüsselung und Authentifizierung die TLS-Verschlüsselung bzw. das TLS-Zertifikat lediglich auf einem Anwendungs-Server notwendig, über den bzw. von dem eine automatisierte verschlüsselte Datenkommunikation zum KBA erfolgt („Kopfstellenlösung“).

Es ist ausreichend, wenn pro Anwendungsserver ein TLS-Zertifikat eingesetzt wird. Bilden mehrere Anwendungsserver einen Verbund, ist auch die Absicherung über ein gemeinsames TLS-Gateway mit nur einem Zertifikat zulässig. Bei der Nutzung eines TLS-Gateways sind die Zugriffe auf die IP-Adressen der berechtigten Systeme zu begrenzen.

Die Nutzung eines zentralen Verschlüsselungsgateways mit einem einzelnen Zertifikat, das im Backend eine beliebige Anzahl von Nutzern des Browser-Dialogs (ohne Anwendungsserver) bedient, ist nicht gestattet.

(3) Bei dem Einsatz eines Anwendungsservers ist die interne Kommunikation zwischen den Arbeitsplätzen und dem Server in eigener Zuständigkeit des externen Kommunikationspartners unter Einhaltung organisatorischer und sicherheitstechnischer Mindestanforderungen abzusichern. Werden Daten der KBA-Anfragen und -Mitteilungen an mehr als einen Server übertragen (z.B. zentraler Log-Server), ist die Kommunikation zu allen Servern, an die entsprechende Daten gesendet werden, unter Einhaltung organisatorischer und sicherheitstechnischer Mindestanforderungen abzusichern. Diese Maßnahmen orientieren sich an den für Bundesbehörden verpflichtenden Mindeststandards und an den technischen und organisatorischen Maßnahmen, die bei der Verarbeitung personenbezogener Daten beachtet werden müssen. Darüber hinaus tragen die Maßnahmen dem **hohen Schutzbedarf** der KBA-Registerdaten Rechnung.

Diese Mindestanforderungen lauten:

a) Zugangs-, Zugriffs - und Weitergabekontrolle

(I) Es sind die erforderlichen organisatorischen und sicherheitstechnischen Maßnahmen zu treffen, um die Vertraulichkeit und Integrität der Daten auf dem Weg zwischen dem jeweiligen Endgerät/Client und dem Anwendungsserver/TLS-Gateway zu gewährleisten und eine unbefugte Nutzung des Zugangs zu verhindern.

Die Kommunikation zwischen den Clients und dem Anwendungsserver ist durchgängig vom Eingabegerät (Client oder Thin-Client) bis zum Anwendungsserver/TLS Gateway zu verschlüsseln. Die Verschlüsselung hat, sofern die Protokolle TLS oder IPSEC eingesetzt werden, entsprechend der TR-02102-2 des BSI bzw. TR-02102-3 des BSI zu erfolgen.

Werden Daten der KBA-Anfragen oder -Mitteilungen an weitere Server (z. B. zentraler Log-Server, TLS-Gateway) auf anderen IT-Systemen übermittelt, ist die Kommunikation zu diesen Servern ebenfalls entsprechend zu verschlüsseln. Werden die Server auf einem System betrieben, ist eine unverschlüsselte Kommunikation über das Loopback-Device zulässig.

Bei der Kommunikation zwischen Clients und Terminalservern ist die maximal mögliche Absicherung der eingesetzten Terminalserver-Architektur zu verwenden.

Bei Nutzung des ICA-Protokolls (Citrix) erfolgt dies entweder über den Einsatz der TLS-Verschlüsselung (entsprechend der TR-02102-2 des BSI) in Verbindung mit Zertifikaten auf den Servern (ist generell zu bevorzugen) oder die SecureICA-Verschlüsselung (aktuell max. 128 Bit).

Bei Nutzung von RDP (Windows Remote Desktop Protocol) ist vorzugsweise ebenfalls die TLS-Verschlüsselung (entsprechend der TR-02102-2 des BSI) in Verbindung mit Serverzertifikaten oder ggf. die RDP-Verschlüsselung mit Verschlüsselungsstufe hoch (128 Bit) oder FIPS-140 einzusetzen.

Als ergänzende Absicherung ist nach Möglichkeit NLA (Network Level Authentication, eine zusätzliche Authentisierungsmethode vor dem eigentlichen Sitzungsaufbau) für die Terminalserver-Nutzer zu aktivieren.

Werden andere Kommunikationsprotokolle eingesetzt, muss die Verschlüsselungsstärke bei symmetrischer Verschlüsselung mindestens 256-Bit (AES-vergleichbar) und bei asymmetrischer Verschlüsselung mindestens 2.048-Bit (RSA-vergleichbar) bzw. 224-Bit (ECC-vergleichbar) betragen.

Es müssen geeignete Maßnahmen ergriffen werden, die einen Zugriff eines behördenfremden IT-Systems auf den Anwendungsserver unterbinden. Geeignete Maßnahmen wären z. B. die Beschränkung des Zugriffs auf Mitglieder (Computer) der Domäne, der flächendeckende Einsatz von Radius-Authentifizierung oder der Einsatz von Client-Zertifikaten beim Zugriff auf die Anwendung. Eine Beschränkung auf IP-Adressen ist nicht ausreichend. Diese Maßnahmen sind im Sicherheitskonzept (s. Punkt f) darzulegen.

Sollten die Anforderungen im Einzelfall durch andere Maßnahmen erfüllt werden, so ist dies gegenüber dem KBA stichhaltig zu begründen und detailliert darzulegen.
Die Angaben zur Verschlüsselung sind auch in einem Netzplan (siehe Punkt f) darzustellen, sodass die durchgängige Verschlüsselung (Verschlüsselungsverfahren und Verschlüsselungsstärke; bei TLS auch Version und Cipher-Suiten) und das genutzte Netz vom Client/Endanwender über die beteiligten Systeme bis zum KBA nachvollzogen werden kann. Falls vorhanden sind Außenstellen, Fernzugriffe, Telearbeit oder mobiles Arbeiten ebenfalls abzubilden.

(II) Für die Kommunikation vom Client/Endanwender bis zum KBA ist das NdB-Verbindungsnetz (NdB-VN) ggf. in Verbindung mit dem jeweiligen Landesverwaltungsnetz und/oder Standleitungen zu nutzen (s. §3 des IT-NetzG und Entscheidung 2015/03 des IT-Planungsrats [IT-Pla15/03]).
Sollten diese Anforderungen nicht realisierbar sein, ist dies stichhaltig zu begründen, die Absicherung der Verbindung detailliert zu beschreiben und ein vergleichbares Sicherheitsniveau (min. ein VPN entsprechend dem IT-Grundschutz [IT-Grund] und der TR-02102) sicherzustellen.

(III) Der Zugriff auf die Webservices des KBA mit HTTPS ist nur mit den vom KBA ausgestellten Client-Zertifikaten möglich.
Die Webserver des Kraftfahrt-Bundesamtes verfügen über ein, von einer allgemein als vertrauenswürdig anerkannten Zertifizierungsstelle ausgestelltes, Server-Zertifikat. Der Anwendungsserver muss die Gültigkeit des Server-Zertifikats beim Verbindungsaufbau überprüfen. Schlägt diese Überprüfung fehl, muss die Verbindung wieder abgebaut werden.
Bestehen in Folge eines Sicherheitsvorfalls Zweifel an der Vertraulichkeit des zum TLS-Client-Zertifikat gehörenden privaten Schlüssels, muss dieses **unverzüglich dem KBA unter der Telefonnummer 0461-316-1400 gemeldet werden.**

Es ist eine personenbezogene Anmeldung mit Benutzerkennung und Passwort am jeweiligen Endgerät/Client (Domäne) und am entsprechenden Anwendungs-Server bzw. innerhalb des Fachverfahrens erforderlich, die Verwendung von Single-Sign-On ist auch hier zulässig.
Die Vergabe, der vom KBA für die Authentifizierung gegenüber den Online-Dialoganwendungen des KBAs erforderliche Benutzerkennung, erfolgt dienststellenbezogen, dabei muss die fachliche Zuständigkeit identisch sein. Es ist programmtechnisch und organisatorisch sicherzustellen, dass Zugriffe auf die Webservices bzw. die Daten des KBA nur durch berechtigte Nutzer (für deren Aufgabenerfüllung erforderlich) dieser Dienststelle durchgeführt werden können und bei personellen Veränderungen die nicht mehr benötigten Benutzerkennungen und Berechtigungen entfernt werden. Wird in Abweichung von diesem Verfahren mehr als eine dienststellenbezogene Benutzerkennung (in Abhängigkeit von der Anwenderzahl) verwendet, so ist sicherzustellen, dass jede Benutzerkennung einer konkreten Person zugeordnet wird und die Nachvollziehbarkeit der ordnungsgemäßen Verwendung gewährleistet ist. Die Weitergabe von Zugangsdaten an Dritte ist untersagt. Bei Bekanntwerden, dass Zugangsdaten an Dritte weitergegeben wurden, werden diese unverzüglich vom KBA gesperrt. Aus Sicherheitsgründen werden die Zertifikate ebenfalls deaktiviert.

b) Passwortverwendung

Das personenbezogene Passwort bei der Anmeldung am Anwendungs-Server bzw. innerhalb des Fachverfahrens muss eine Länge von mindestens 10 Zeichen haben. Dass Passwort muss mindestens einen Kleinbuchstaben, einen Großbuchstaben, eine Ziffer sowie ein Sonderzeichen enthalten. Die Verwendung der letzten fünf Passwörter sowie Passwörter aus gängigen Passwortlisten sind nicht erlaubt. Die Zugangskennung ist nach spätestens fünf Fehleingaben zu sperren oder es ist sicherzustellen, dass die erneute Eingabe des Passworts nach der dritten Fehleingabe erst nach frühestens 3 Minuten wieder möglich ist und dass die zuständigen Administratoren eine entsprechende Benachrichtigung erhalten. Ein Passwortwechsel ist grundsätzlich nach spätestens 6 Monaten durchzuführen. Sofern die Fachverfahren selbst oder die als Basis für den Betrieb dienende IT-Systemtechnik Mechanismen zum Einsatz bringen, die einen Kompromittierungsfall unmittelbar erkennen können (z.B. parallele Anmeldungen von verschiedenen Systemen oder Standorten, Häufung von Fehleingaben usw.) und ein schnelles Eingreifen erlauben ist es ausreichend das Passwort nur zu wechseln, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht. Bei der Verwendung von Single-Sign-On (generell zu bevorzugen) muss dies für die Anmeldung am jeweiligen Endgerät/Client (Domäne) ebenfalls sichergestellt werden.

Hinweis: Der Passwortwechsel für Zugangsdaten muss spätestens nach 90 Tagen erfolgen.

c) Protokollierung

Zugriffe aus der externen Anwendung heraus auf die Webservices des Kraftfahrt-Bundesamtes sind auf Seiten der externen Anwendung mit der jeweiligen personenbezogenen Benutzerkennung nachvollziehbar zu protokollieren. Der Benutzer und das genutzte Gerät müssen eindeutig identifizierbar sein. Es ist auch eine Protokollierung der Netzwerkzugriffe (IP-Adressen und Ports) auf den am Verfahren beteiligten Server erforderlich. Die Archivierung der Protokolldaten ist für mindestens 6 Monate sicherzustellen. Bei Sicherheitsvorfällen sind die Protokolldaten - auch über diesen Zeitraum hinaus - bis zum Abschluss der Untersuchungen, bis zur Übergabe an die Strafverfolgungsbehörden oder der Erteilung der Genehmigung zum Löschen der Protokolldaten durch die Strafverfolgungsbehörden aufzubewahren. Nutzen mehrere Anwendungsserver ein TLS-Gateway wird die Speicherung der Protokolle aller auf die KBA-Webservices zugreifenden Anwendungsserver auf einem Logserver empfohlen.

d) System- und netztechnische Sicherheit

Die systemtechnischen Komponenten (Clients, Server, Netzwerkkomponenten und insbesondere der Anwendungsserver/Verschlüsselungsserver/TLS-Gateway) sind systemseitig durch geeignete Maßnahmen gegen unautorisierte Zugriffe zu schützen und auf dem aktuellen sicherheitstechnischen Stand zu halten. Alle sicherheitsrelevanten Updates und Patches (für Clients, Server, Netzwerkkomponenten, Sicherheitsgateways, Betriebssysteme, Anwendungen usw.) sind schnellstmöglich einzuspielen.
Netzwerkseitig sind die systemtechnischen Komponenten (insbesondere der Anwendungsserver und/oder das TLS-Gateway) vor Zugriffen aus nicht zugriffsberechtigten Netzen zu schützen. Dies gilt insbesondere für Zugriffe aus dem Internet aber auch für Zugriffe aus anderen internen oder externen Netzen. Der Anwendungsserver und/oder das TLS-Gateway sind deshalb in einer demilitarisierten Zone (DMZ) zu platzieren.

Sollten Fernzugriffe (z. B. von Herstellern, Administratoren, Mobilen- oder Telearbeitern) auf diese Systeme möglich sein, ist im Sicherheitskonzept (siehe Buchstabe f) darzulegen, welche technischen und organisatorischen Maßnahmen (Authentisierung, Verschlüsselung, …) zur Erreichung eines angemessenen Schutzniveaus ergriffen wurden. Dabei sind die im Modul „Sicherer Fernzugriff auf lokale Netze“ (ISi-Fern, BSI-Standards zur Internet-Sicherheit) beschriebenen Maßnahmen und die Anforderungen aus dem Grundschutz (Bausteine des IT-Grundschutz-Kompendium, OPS.1.2.4 Telearbeit und OPS 2.4 Fernwartung) einzuhalten. Bei dem Fernzugriff sind vom BSI für die Übermittlung von VS-NfD eingestuften Daten zugelassene Verschlüsselungsgeräte/-lösungen zu nutzen.

e) Räumliche Sicherheit

Die Unterbringung der systemtechnischen Komponenten (insbesondere der Anwendungsserver/Verschlüsselungsserver/TLS-Gateway) ist räumlich, organisatorisch und technisch abzusichern (Serverraum), so dass gewährleistet ist, dass nur autorisierte und geschulte Personen Zugang zu den am Verfahren beteiligten Servern haben. Andere Personen (Betriebsfremde/Externe oder andere Mitarbeiter) dürfen den Zugang nur im Bedarfsfall und in Begleitung einer berechtigten Person erhalten.

f) Sicherheitskonzept

Es muss dem KBA ein formloses Sicherheitskonzept / Practise Statement oder die für die betroffene Anwendung relevanten Teile eines Sicherheitskonzeptes vorgelegt werden, in dem die detaillierte Umsetzung aller geforderten organisatorischen und sicherheitstechnischen Mindestanforderungen durch den Kopfstellenbetreiber bzw. externen Kommunikationspartner beschrieben wird. Diesem ist ein Netzplan mit allen relevanten Komponenten unter Aufführung der genutzten Verschlüsselung (Verschlüsselungsverfahren und Verschlüsselungsstärken; bei TLS auch Version und Cipher-Suiten) beizufügen.
Das Sicherheitskonzept ist bei Änderungen jeglicher Art fortzuschreiben und dem KBA in der aktuellen Version erneut vorzulegen.
Das KBA ist berechtigt, jederzeit ein aktuelles Sicherheitskonzept anzufordern.

g) Verpflichtungserklärung und Zulassungsbescheid

Die Aufnahme des Wirkbetriebes der Kopfstelle darf erst nach Erhalt des vom KBA ausgestellten Zulassungsbescheids erfolgen. Voraussetzung für die Erteilung des Zulassungsbescheids ist die Vorlage einer unterschriebenen Verpflichtungserklärung sowie ein vom KBA genehmigtes Sicherheitskonzept, welches die in § 1 Abs. 3 a) – e) beschriebenen Mindestsicherheitsanforderungen erfüllt.

(4) Für den Zugriff auf die Webservices ist das vom KBA herausgegebene Informationsblatt „Information zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden“ in der jeweils gültigen Fassung sowie die durch den IT-Planungsrat veröffentlichte „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ einzuhalten.

Bei einem Missbrauch oder bereits bei dem Verdacht auf Missbrauch von erteilten Zugangsdaten sowie IT-Sicherheitsvorfällen ist das KBA unverzüglich unter Tel.: 0461 316-1400 zu benachrichtigen und die Verwendung von neuen Zugangsdaten zwingend erforderlich.

Wird ein Missbrauch bzw. ein Cyberangriff beim KBA bekannt, werden unverzüglich die Online-Zugangsdaten gesperrt. Aus Sicherheitsgründen werden Zertifikate ebenfalls deaktiviert. Nach erfolgter schriftlicher Bestätigung der geschädigten Stelle, dass eine sichere Datenkommunikation wieder möglich ist, können Zugangsdaten unter Anwenderbetreuung@kba.de sowie Zertifikate unter Zertifikatsbeantragung@kba.de neu beantragt werden.

(5) Die erklärende Stelle verpflichtet sich zur Einhaltung der angeführten für sie maßgeblichen Bedingungen.

§ 2

Pflichten der erklärenden Stelle:

(1) Die erklärende Stelle verpflichtet sich zur unverzüglichen Mitteilung von:

a) Änderungen ihres Sicherheitskonzeptes und/oder Änderungen der Infrastruktur, die Auswirkungen auf die Einhaltung der organisatorischen und sicherheitstechnischen Mindestanforderungen haben

b) Änderungen der IP-Adresse

c) Anschriftenänderungen und Änderungen der Ansprechpartner

d) Änderungen (Wegfall, Hinzukommen, qualitative Änderungen) der abrufenden Stellen

e) sonstigen Umständen, die für den Zugriff bedeutsam sind bzw. die die Nichteinhaltung der unter § 1 genannten Mindestanforderungen zur Folge haben (insbesondere im Kompromittierungsfall von geheimen Schlüsseln).

(2) Die erklärende Stelle verpflichtet auch von Ihr beauftragte Subunternehmen und/oder Wartungspersonal zur Einhaltung der unter § 1 und § 2 Abs. 1 genannten Standards. Sie trägt vollumfänglich die Verantwortung für diese. Sie teilt dem KBA auf der Anlage 1 mit, welche Subunternehmer Sie für diese Applikation einsetzt.

§ 3

(1) Bei Beendigung des Datentransfers zwischen der erklärenden Stelle und dem KBA auf Dauer, verpflichten sich beide Kommunikationspartner zu Geheimhaltung über die jeweiligen Ihnen bekannt gewordenen Interna des Anderen. Diese Verpflichtung erstreckt sich auch auf Subunternehmer, die von dem jeweiligen Kommunikationspartner beauftragt wurden.

(2) Alle sicherheitsrelevanten Unterlagen, Soft- und Hardwareprodukte sind sicher zu verwahren und dem KBA ggf. auf dessen Verlangen zurückzugeben.

(3) Die unter § 1 und § 2 Abs. 1 genannten Standards werden vom KBA aktualisiert und sind - ggf. nach angemessener Übergangsfrist – von der erklärenden Stelle anzuwenden.

§ 4

Schluss- und Übergangsbestimmungen:

(1) Die Bestimmungen dieses Dokumentes orientieren sich am jeweils aktuellen Stand der Informationssicherheitstechnik.

(2) Die erklärende Stelle hat, nach Aufforderung durch das KBA, innerhalb einer Frist von 12 Monaten ein aktuelles Sicherheitskonzept zur Prüfung vorzulegen. In besonderen Fällen kann diese Frist kürzer ausfallen.

(3) Die Nichteinhaltung dieser Verpflichtungserklärung kann zum Widerruf des Zulassungsbescheides bei gleichzeitiger Sperrung der Zugangsberechtigung durch das Kraftfahrt-Bundesamt führen.

(Bezeichnung und Anschrift der erklärenden Stelle)

(Ort, Datum)

(Unterschrift der erklärenden Stelle)

Anlage 1

zur Verpflichtungserklärung des Betreibers einer Kopfstelle

Der Betreiber der Kopfstelle

_____

_____

(Bezeichnung und Anschrift)

erklärt:

Die für den Zugriff auf die Webservices des Kraftfahrt-Bundesamtes über eine Kopfstelle vorgegebenen organisatorischen und sicherheitstechnischen Mindestanforderungen werden eingehalten.

Zum Abruf berechtigte Haupt- oder Nebenstelle (Dienststellen, PLZ, Ort, Straße, Hausnummer)	Ansprechpartner (fachlich u. technisch) (Name, Tel.-Nr., E-Mail-Adresse)

_____ (Ort, Datum)

_____ (Unterschrift Behördenleiter/Amtsleiter und Dienststempel, ggf. Kopfstellenbetreiber)