Kraftfahrt-
Bundesamt

Informationen zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden

Stand: 01.2020

Information zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden

Die Datenübermittlung über das TCP/IP-Protokoll von und zu den zentralen Registern des Kraftfahrt-Bundesamtes (KBA) per File-Transfer sowie die Nutzung der Online-Dialogverfahren des KBAs erfolgt auf Basis der jeweils gültigen Datenübermittlungsstandards bzw. –Vorschriften (SDÜ).

Die Nutzung der Online-Dialogverfahren des KBA ist über das **NdB-Verbindungsnetz** (NdB-VN) mit dem Protokoll HTTPS in Verbindung mit **clientseitigen Zertifikaten** möglich. Die Nutzung erfolgt dabei

- entweder über die vom KBA bereitgestellten Dialoganwendungen (KBA-Portal) mittels eines HTML- und XML-fähigen Browsers (Browser-Dialog)
- oder über die vom KBA zur Verfügung gestellten Webservices für die Programm-zu-Programm-Kommunikation (durch Anwendungsserver oder Client-Anwendungen).

Für den **File-Transfer** wird vom KBA derzeit das File-Transfer-Protokoll FT–NEA (openFT) über TCP/IP unterstützt. Der File-Transfer mit dem beim KBA hostseitig eingesetzten Produkt openFT muss mit einer File-Transfer-Software, die mit openFT (mit Crypt-Modul ab Version 12.1) oder einem vergleichbaren Produkt kommunizieren kann, durchgeführt werden. Der Einsatz eines File-Transfer Produkts bietet:

- Erstellung von Vorlagen zur automatisierten Übertragung
- erweiterte Möglichkeiten zur automatisierten Übertragung
- Komprimierung bei der Datenübertragung
- revisionssichere Protokollierungsfunktionen

Für die **Übermittlung von FAER-Namensänderungen** über das Internet bietet das KBA einen Dienst auf Basis des **OSCI**-Transportprotokolls (Version 1.2) an.
Außerdem besteht im Rahmen der **internetbasierten Kfz-Anwendung** die Möglichkeit, eigene dezentrale Portale über das Internet an das KBA anzuschließen und darüber Nutzern zu ermöglichen, Fahrzeuge außer Betrieb zu setzen sowie an- und umzumelden. Die Anbindung an diese Verfahren ist in gesonderten Dokumenten beschrieben.

Für jede Datenart gelten eigene Übermittlungsrichtlinien, die den SDÜ´s der jeweiligen Datenart zu entnehmen sind.

Der Zugriff auf die zentralen Register des KBAs für die zum Dialog berechtigten öffentlichen Stellen erfolgt über das Verbindungsnetz des Bundes und der Länder (NdB-VN).

Abweichend davon erfolgt der Zugriff auf die Dialoganwendungen sowie der File-Transfer durch Polizeibehörden des Bundes und der Länder in der Regel über das Polizeinetz CNP/ON.

Die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) betreibt das NdB-VN als Standleitungs-Verbundnetz verschiedener Ländernetze der Bundesrepublik Deutschland. Die Anbindung an das NdB-VN erfolgt entweder über ein regional zuständiges Landesrechenzentrum, ein kommunales Rechenzentrum oder über einen lokalen NdB-VN-Anschluss, der über ndb-vn@bdbos.bund.de beantragt werden kann.
Für die Datenkommunikation mit dem KBA ist im Rahmen der Datenschutz- und Datensicherheitsaspekte insbesondere der Ende-zu-Ende-Sicherheit der Einsatz einer Verschlüsselungslösung entsprechend der TR-02102 des BSI zu gewährleisten. Der Zugriff auf die Webanwendung sowie Webservices erfolgt mit HTTPS auf Basis einer TLS-Verschlüsselung (TLS 1.2 und höher) mit Client-Authentisierung über dateibasierte Client-Zertifikate, welche beim KBA zum Preis von derzeit 80,00 € (inkl. MwSt.) pro Stück inkl. Versandkosten erhältlich und für 3 Jahre gültig sind.
Das Verfahren entspricht den Vorgaben des BSI gemäß der technischen Richtlinie TR-02102 des BSI sowie dem Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS) [MTLS].

Nutzung der Dialoganwendungen

Voraussetzung für die Nutzung ist die Unterstützung von TLS 1.2 oder höher durch das Betriebssystem und den eingesetzten Webbrowser. Als Hilfestellung kann hier neben den Herstellerinformationen auch der Leitfaden des BSI zur Migration auf TLS 1.2 [HLTLS] herangezogen werden[1]. Darüber hinaus wird bei der Nutzung des KBA-Browser-Dialogs für jeden PC bzw. Anwender ein Client-Zertifikat benötigt. Nutzen mehrere Personen einen Arbeitsplatz, muss von der abrufberechtigten Stelle die Nachvollziehbarkeit der Abrufe jeder Person sichergestellt werden.
Das Zertifikat muss auf jedem zugreifenden Client eingespielt werden. Abweichend davon ist bei einem direkten Zugriff von einem System von dem mehrere Mitarbeiter gleichzeitig auf die Registerverfahren zugreifen, für jeden Nutzer ein eigenes Zertifikat zu installieren und zu nutzen. Dies gilt insbesondere für den Einsatz von Terminalservern.

[1] eine Fortschreibung für TLS 1.3 erfolgt nicht.

Die Nutzung eines zentralen Verschlüsselungsgateways mit einem einzigen Zertifikat, das im Backend eine beliebige Anzahl von Nutzern des Browser-Dialogs (ohne Anwendungsserver) bedient, ist nicht gestattet.
Weitere Informationen hierzu erhalten Sie im Rahmen der Antragstellung.

Da es sich bei der Verschlüsselung um eine Ende-zu-Ende-Verschlüsselung handelt, wird darauf hingewiesen, dass beim Einsatz von zwischengeschalteten Application-Firewalls (Proxy-Firewalls) zum NdB-VN technische Probleme auftreten können. Weitere Einzelheiten klären Sie bitte frühzeitig mit dem Technischen Support des Kraftfahrt-Bundesamtes ab.

Anbindung über eine Kopfstelle bzw. Nutzung der Webservices

Der Zugriff auf die Webservices durch Anwendungen oder Anwendungsserver über das NdB-Verbindungsnetz (NdB-VN) erfolgt über HTTPS auf Basis einer TLS-Verschlüsselung (TLS 1.2 und höher) mit Authentisierung über ein dateibasiertes Zertifikat für Webservices. Es ist ausreichend, wenn pro Anwendungsserver nur ein TLS-Zertifikat eingesetzt wird. Bilden mehrere Anwendungsserver einen Verbund, ist auch die Absicherung über ein gemeinsames TLS-Gateway mit nur einem Zertifikat zulässig. 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. Wird ein TLS-Gateway genutzt, sind die Zugriffe auf die IP-Adressen der berechtigten Systeme zu begrenzen.

Bei Einsatz eines Anwendungsservers über HTTPS ist die interne Kommunikation zwischen den Arbeitsplätzen und dem Server in eigener Zuständigkeit des externen Kommunikationspartners unter Einhaltung der nachfolgenden organisatorischen und sicherheitstechnischen 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.

1. 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.
Hinweis: Ab dem 01.01.2023 sind für andere Kommunikationsprotokolle die Vorgaben der TR-02102-1 einzuhalten und muss die Verschlüsselungsstär-

ke bei asymmetrischer Verschlüsselung mindestens 3.072-Bit (RSA-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 in einem Sicherheitskonzept (s. Punkt 6) 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]).
Bei der Übermittlung von Daten außerhalb der Behördengebäude sind vom BSI für die Übermittlung von VS-NfD eingestuften Daten zugelassene Verschlüsselungsgeräte zu nutzen (s. Anschlussbedingungen für das Verbindungsnetz).
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 des BSI) 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**.

(IV) 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 hier auch 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 KBAs nur durch berechtigte Nutzer (für deren Aufgabenerfüllung erforderlich) dieser Dienststelle durchgeführt werden können. 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.

2. 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. Wenn die Zugangskennung nach spätestens fünf Fehleingaben gesperrt wird oder ab der dritten Fehleingabe die erneute Eingabe des Passworts erst nach mindestens 3 Minuten möglich ist und die zuständigen Administratoren eine entsprechende Benachrichtigung erhalten, müssen nur mindestens drei der vier beschriebenen Merkmale (Kleinbuchstaben, Großbuchstaben, Ziffer sowie Sonderzeichen) enthalten sein. Sofern die Fachverfahren

selbst oder sie als Nutzer als Basis für den Betrieb dienende IT-Systemtechnik Mechanismen zum Einsatz bringen, die einen Kompromittierungsfall unmittelbar erkennen können und ein schnelles Eingreifen erlauben oder eine Passwortmindestlänge von mindestens 14 Zeichen sichergestellt ist, kann der Passwortwechselzyklus 90 Tage betragen. Andernfalls ist ein Passwortwechsel von mindestens 42 Tagen notwendig. Die Verwendung der letzten fünf Passwörter ist nicht erlaubt. Bei der Verwendung von Single-Sign-On muss dies für die Anmeldung am jeweiligen Endgerät/Client (Domäne) ebenfalls sichergestellt werden.

3. 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.

4. 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 Nr. 6) 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.

5. 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.

6. 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 Kopfstellebetreiber 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.

7. 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 der Verpflichtungserklärung § 1 Abs. 3 a) – e) beschriebenen Mindestsicherheitsanforderungen erfüllt.

8. Zugangssperrung

Die Nichteinhaltung einer oder mehrerer der in der Verpflichtungserklärung beschriebenen Voraussetzungen kann zum Widerruf des Zulassungsbescheides bei gleichzeitiger Sperrung der Zugangsberechtigung der Kopfstelle durch das Kraftfahrt-Bundesamt führen.

Ansprechpartner beim Kraftfahrt-Bundesamt

Technische Informationen bezüglich der Netzanbindung und der Sicherheitsmaßnahmen erhalten Sie über:

Technischer Support

Tel.:	(0461) 316-1400
Fax:	(0461) 316-1420
E-Mail:	KBA-ServiceDesk@kba.de

Informationen zur Beantragung sowie Antragsunterlagen erhalten Sie über:

Anwenderbetreuung

Tel.:	(0461) 316-1717
Fax.:	(0461) 316-2942
E-Mail:	Anwenderbetreuung@kba.de

Quelle

[HLTLS] Handlungsleitfaden des BSI zur Migration auf TLS 1.2
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Migrationsleitfaden_Mindeststandard_BSI_TLS_1_2_Version_1_2.pdf?__blob=publicationFile&v=5

[ISi-Fern] Sicherer Fernzugriff auf das interne Netz (ISi-Fern) des BSI-Standards zur Internet Sicherheit (ISi-Reihe)
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Fern/isi-fern.html

[IT-Gund] IT-Grundschutz des BSI
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[IT-Pla15/03] Entscheidung des IT-Planungsrats vom 18. März 2015
https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2015/Sitzung_16.html?pos=3

[MTLS] Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_0.pdf?__blob=publicationFile&v=2

[OPS.1.2.4] IT-Grundschutz Baustein OPS.1.2.4 Telearbeit
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_2_4_Telearbeit.html

[OPS 2.4] IT-Grundschutz Baustein OPS.2.4 Fernwartung
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_2_4_Fernwartung.html

[TR-02102] BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[TR-02102-2] BSI TR-02102: Teil 2 – Verwendung von Transport Layer Security (TLS)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=6

[§3 IT-NetzG] Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder (IT-NetzG)
https://www.gesetze-im-internet.de/it-netzg/__3.html

Impressum

Herausgabe:
Kraftfahrt-Bundesamt
24932 Flensburg

Internet: www.kba.de

Fachliche Auskünfte und Beratung:

Telefon: 0461 316-1717
Telefax: 0461 316-2942
E-Mail: anwenderbetreuung@kba.de

Stand: Januar 2020

Druck: Druckzentrum KBA

Bildquelle: www.shutterstock.de

Wir punkten mit Verkehrssicherheit!