Kraftfahrt-
Bundesamt

Informationen zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden

Stand: 11.2018

Zentrale
Register

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-Dialoganwendungen des KBA erfolgt auf Basis der jeweils gültigen Datenübermittlungsstandards bzw. –Vorschriften (SDÜ).

Die Nutzung der Online-Dialoganwendungen des KBA ist aktuell über das Protokoll HTTP ergänzt durch ein VPN (Virtual Private Network, realisiert auf Basis des Produkts PrivateWire) möglich. **Ab 01.01.2017 ist die Nutzung über das NdB-Verbindungsnetz / DOI-Netz auch über das Protokoll HTTPS in Verbindung mit Client-seitigen Zertifikaten möglich.** Die Nutzung erfolgt dabei

- entweder über die vom KBA bereitgestellten Dialogoberflächen (KBA-Portal) mittels eines HTML- und XML-fähigen Browsers (Browser-Dialog)
- oder über die vom KBA zur Verfügung gestellten XML-Schnittstellen für die Programm-zu-Programm-Kommunikation (Server- oder Client-Anwendung).

Wichtiger Hinweis:

Der Hersteller-Support für das Produkt PrivateWire (Client und Gateway) wurde zum 31.12.2016 durch die Fa. Algorithmic Research (Docusign) offiziell aufgekündigt. **Das Produkt wird in der bisherigen Form nicht weiterentwickelt. Das KBA wird die derzeitige Version von PrivateWire bis 31.12.2019 unterstützen. Eine neue PrivateWire Version 5.0 kann ab Frühjahr 2017 bei Nutzung eines Zertifikats eingesetzt werden.**

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 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 i-KFZ-Anwendung die Möglichkeit, eigene dezentrale Portale über das Internet an das KBA anzuschließen und darüber Nutzern zu ermöglichen, Fahrzeuge außer Betrieb zu setzen (1. Stufe) und in einer späteren Stufe auch an- bzw. 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.

Die Datenkommunikation mit dem KBA ist derzeit über nachfolgende Netzanbindungen möglich.

1. ISDN-Wählleitung mit Ende-zu-Ende Verschlüsselung (auslaufend)

Die Datenkommunikation/der Dialog mit dem KBA kann über das öffentliche ISDN-Netz unter Nutzung des TCP/IP-Protokolls erfolgen.

Die Rechner werden entweder über einen ISDN-Router oder direkt über eine ISDN-Karte und eine ISDN-Leitung mit dem KBA verbunden. Für die bei dieser Art der Datenübermittlung aus Datenschutz- und Datensicherheitsgründen erforderliche Verschlüsselung und Authentifizierung ist auf dem PC das Produkt PrivateWire Client der Firma Algorithmic Research (AR), das in Deutschland von der Fa. Applied Security vertrieben wird, einzusetzen. Voraussetzung für den Einsatz des Verschlüsselungsprodukts PrivateWire ist ein PC mit einem Windows-Betriebssystem. Diese Verschlüsselungslösung besteht aus einer Verschlüsselungs-Software (PrivateWire Client), einem USB-Chipkartenleser (Cherry ST2000-U) und einer USB-Chipkarte. Verschlüsselungs-Software und Chipkartenleser können über einen Rahmenvertrag über die Firma Applied Security beschafft werden. Die Chipkarten mit einer Gültigkeit von drei Jahren sind beim KBA zum Preis von derzeit 60,00 € (inkl. MwSt.) pro Stück zuzüglich Versandkosten erhältlich. Weitere Informationen hierzu erhalten Sie nach Antragstellung.

Bei der Datenübermittlung per File-Transfer ist die Verschlüsselung mittels der File-Transfer Software openFT (mit Crypt-Modul) ab Version 9.0 (BS2000) bzw. Version 8.1 (Windows und Unix) oder ein vergleichbares Produkt, das die gleichen Kriterien bei der Verschlüsselung und Authentifizierung gegenüber openFT erfüllt, zugelassen. Sobald ak-

tuellere Versionen mit verbesserten Schutzmöglichkeiten verfügbar sind, muss auf diese umgestellt werden.

Da die Unterstützung von ISDN-Wählleitungen durch die Telekommunikations-Diensteanbieter mittelfristig eingestellt wird, sollte dieser Kommunikationsweg für neue Zugänge nicht mehr gewählt werden. Das TLS-Verfahren 1.2 mit Clientauthentifizierung wird hierbei nicht unterstützt.

2. DOI Anbindung

Die Datenkommunikation mit dem KBA kann auch über das Verbindungsnetz des Bundes und der Länder (DOI-Netz) erfolgen.

Das Bundesverwaltungsamt betreibt das DOI Netz als Standleitungs-Verbundnetz verschiedener Ländernetze der Bundesrepublik Deutschland. Die Anbindung an das DOI Netz erfolgt entweder über ein regional zuständiges Landesrechenzentrum, ein kommunales Rechenzentrum oder über einen lokalen DOI-Anschluss, der über ndb-vn@bdbos.bund.de beauftragt werden kann. Für die Datenkommunikation mit dem KBA über das DOI Netz gelten bezüglich der Datenschutz- und Datensicherheitsaspekte die Aussagen der Datenübermittlung per ISDN-Leitung analog. Insbesondere ist auch hier eine Ende-zu-Ende-Sicherheit durch den Einsatz einer Verschlüsselungslösung (zur Verschlüsselung und Authentifizierung, vgl. Pkt. 1.) zu gewährleisten.

Da die Herstellerunterstützung für das Produkt PrivateWire Client zum Ende des Jahres 2016 offiziell ausläuft, sollte die VPN-Anbindung über PrivateWire Clients für neue Zugänge nicht mehr genutzt werden. **Seitens des KBA wird diese Zugangsmöglichkeit zum 31.12.2019 eingestellt.**

Alternativ kann ab 01.01.2017 die Datenkommunikation auch über HTTPS auf Basis einer TLS-Verschlüsselung (TLS 1.2) mit Client-Authentisierung über dateibasierte Client-Zertifikate erfolgen. Das Verfahren entspricht den Vorgaben des BSI gemäß der technischen Richtlinie TR-02102[1] sowie dem Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden[2]. Voraussetzung für die Nutzung ist die

[1] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
[2] https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/SSL-TLS-Protokoll/SSL-TLS-Protokoll.html

Unterstützung von TLS 1.2 durch das Betriebssystem und den eingesetzten Webbrowser - dies ist bei aktuellen Produkten in der Regel der Fall. Als Hilfestellung kann hier neben den Herstellerinformationen auch der Leitfaden des BSI zur Migration auf TLS 1.2[3] herangezogen werden. Darüber hinaus wird bei der Nutzung des KBA-Browser-Dialogs für jeden PC bzw. Anwender ein Client-Zertifikat benötigt, welches beim KBA zum Preis von derzeit 80,00 € (inkl. MwSt.) pro Stück inkl. Versandkosten erhältlich ist. Dies gilt auch beim Einsatz von Terminalservern.
Das Zertifikat muss auf jedem zugreifenden Client eingespielt werden und ist für 3 Jahre gültig. Abweichend davon ist bei einem direktem Zugriff von einem System von dem mehrere Mitarbeiter gleichzeitig auf die Registerverfahren zugreifen, für jeden Nutzer ein eigenes Zertifikat zu installieren und zu nutzen.
Weitere Informationen hierzu erhalten Sie im Rahmen der Antragstellung.

Bei der Datenübermittlung per File-Transfer ist die Verschlüsselung mittels der File-Transfer Software openFT (mit Crypt-Modul) ab Version 9.0 (BS2000) bzw. Version 8.1 (Windows und Unix) oder ein vergleichbares Produkt, das die gleichen Kriterien bei der Verschlüsselung und Authentifizierung gegenüber openFT erfüllt, zugelassen. Sobald aktuellere Versionen mit verbesserten Schutzmöglichkeiten verfügbar sind, muss auf diese umgestellt werden.

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 DOI-Netz technische Probleme auftreten können. Weitere Einzelheiten klären Sie bitte frühzeitig mit dem Technischen Support des Kraftfahrt-Bundesamtes ab.

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Migrationsleitfaden_Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile&v=3

3. Anbindung über eine Kopfstelle bzw. mittels Programm-Programm-Kommunikation über Anwendungsserver

Bei Nutzung der XML-Schnittstellen für die Programm-zu-Programm-Kommunikation[4] über die unter Punkt 1. und 2. genannten Netzanbindungen kann die erforderliche automatisierte Verschlüsselung und Authentifizierung noch **bis 31.12.2019** durch den Einsatz des Produkts PrivateWire-Gateway[5] auf einem Kopfstellen-Server (PrivateWire-Verschlüsselungs- und/oder Anwendungs-Server, „PrivateWire-Kopfstellenlösung“) gewährleistet werden. Um bei dieser Lösung einen automatisierten Verbindungsaufbau zu ermöglichen, wird das für die Authentifizierung gegenüber der Chipkarte normalerweise über die Tastatur einzugebende Passwort auf dem Server in einem gesonderten und verschlüsselten Eintrag abgelegt.
Für den Einsatz von PrivateWire auf einem "Kopfstellen-Server" ist die Software PrivateWire-Gateway mit Chipkartenleser und Chipkarte einzusetzen. Diese Software bietet neben der Verschlüsselung und Authentifizierung die Möglichkeit einer systemtechnischen Protokollierung sowie zusätzliche Firewall-Funktionalitäten. Bei entsprechender erweiterter Lizenz kann auch die interne Verschlüsselung darüber realisiert werden. Die Verwendung vorhandener Chipkarten sowie des Chipkartenlesers „Private Safe“ ist nicht möglich.

Als Alternative zum Betrieb einer PrivateWire-Kopfstelle kann ab 01.01.2017 die Programm-Programm-Kommunikation über Anwendungsserver über das NdB-Verbindungsnetz / DOI-Netz auch über HTTPS auf Basis einer TLS-Verschlüsselung (TLS 1.2) mit Authentisierung über ein dateibasiertes Zertifikat erfolgen (weitere Informationen siehe auch 2.). Dann ist es 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.

Bei Einsatz einer „PrivateWire-Kopfstelle“ oder eines Anwendungsservers über HTTPS ist die interne Kommunikation zwischen den Arbeitsplätzen und dem Server in eigener Zuständigkeit des externen Kommunikationspartners unter Einhaltung der nachfolgenden

[4] Für den Browser-Dialog oder Filetransfer ist weiterhin eine Ende-zu-Ende Verschlüsselung erforderlich.
[5] Es ist nur die Windows-Version zum KBA-Gateway kompatibel.

organisatorischen und sicherheitstechnischen Mindestanforderungen abzusichern. Diese Maßnahmen orientieren sich an den technischen und organisatorischen Maßnahmen, die gemäß §9 Bundesdatenschutzgesetz von Stellen, welche personenbezogene Daten verarbeiten, erheben oder nutzen, 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 der "PrivateWire-Kopfstelle" bzw. dem Anwendungsserver/TLS-Gateway zu gewährleisten und eine unbefugte Nutzung des Zugangs zu verhindern.

Hinweis: Grundsätzlich ist zur Erfüllung dieser Anforderungen eine durchgängige Verschlüsselung vom jeweiligen Endgerät/Client bis zur "PrivateWire-Kopfstelle“ bzw. zum Anwendungsserver/TLS-Gateway sowie eine sichere gegenseitige Authentifizierung zwischen Anwendungsserver und Client-PC erforderlich[6]. Die Verschlüsselungsstärke muss bei symmetrischer Verschlüsselung mindestens 256-Bit (AES-vergleichbar) und bei asymmetrischer Verschlüsselung mindestens 2.048-Bit (RSA-vergleichbar) bzw. 224-Bit (ECC-vergleichbar) betragen.
Abweichend davon ist bei der Kommunikation zwischen Clients und Terminalservern die maximal mögliche Absicherung der eingesetzten Terminalserver-Architektur zulässig. Bei Nutzung des ICA-Protokolls (Citrix) erfolgt dies entweder über die SecureICA-Verschlüsselung (aktuell max. 128 Bit) oder den Einsatz der SSL-/TLS-Verschlüsselung in Verbindung mit Zertifikaten auf den Servern (generell zu bevorzugen). Bei Nutzung von RDP (Windows Remote Desktop Protocol) ist dies vorzugsweise ebenfalls die SSL-/TLS-Verschlüsselung in Verbindung mit Serverzertifikaten oder falls das nicht möglich ist, die RDP-Verschlüsselung mit Verschlüsselungsstufe hoch (128 Bit) oder FIPS-140. Als ergänzende Absicherung ist möglichst noch NLA (Network Level Authentication,

[6] Hierbei muss insbesondere die systemtechnische Einmaligkeit des Client-PC sichergestellt sein.

eine zusätzliche Authentisierungsmethode vor dem eigentlichen Sitzungsaufbau) für die Terminalserver-Nutzer zu aktivieren.
Sollten die Anforderungen im Einzelfall durch andere Maßnahmen erfüllt werden, so ist dies gegenüber dem KBA darzulegen.

(II) Der Zugriff auf die Webservices des KBA über 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**.

(III) 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 Vergabe der vom KBA für die Authentifizierung gegenüber den Online-Dialoganwendungen des KBA erforderliche ZEVIS-Benutzerkennung erfolgt dienststellenbezogen. Es ist programmtechnisch sicherzustellen, dass Zugriffe auf die XML-Schnittstellen nur durch berechtigte Nutzer dieser Dienststelle durchgeführt werden. Wird in Abweichung von diesem Verfahren mehr als eine dienststellenbezogene ZEVIS-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

Ab dem 01.12.2017 hat das vom KBA vergebene Passwort eine Gültigkeit von 90 Tagen. Eine Änderung des Passworts nach Ablauf der Gültigkeit ist nicht möglich, da die Kennung automatisch gesperrt wird.

Das Passwort muss eine Länge von mindestens 10 Zeichen haben und aus den Kleinbuchstaben a - z, den Großbuchstaben A - Z, den Ziffern 0 - 9 sowie den Sonderzeichen ! # $ % - / : = ? @ [ ] _ { } bestehen.

3. Protokollierung

Zugriffe aus der externen Anwendung heraus auf die XML-Schnittstellen des Kraftfahrt-Bundesamtes sind auf Seiten der externen Anwendung mit der jeweiligen personenbezogenen Benutzerkennung nachvollziehbar zu protokollieren. Es ist zusätzlich eine Protokollierung der systemtechnischen Zugriffe (IP-Adresse, Port) der Kopfstelle bzw. eine angemessene Protokollierung des Anwendungsservers/TLS-Gateways 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.

4. System- und netztechnische Sicherheit

Die systemtechnischen Komponenten (insbesondere PrivateWire-Verschlüsselungsserver, Anwendungsserver/TLS-Gateways) sind systemseitig durch geeignete Maßnahmen gegen unautorisierte Zugriffe zu schützen und auf dem aktuellen sicherheitstechnischen Stand (z. B. durch die Verwendung aktueller Patches) zu halten. Zudem sind Schutzmaßnahmen gegenüber unberechtigten Zugriffen aus anderen Netzen (insbesondere dem Internet) vorzunehmen. Sollten Fernzugriffe (z. B. von Herstellern oder Telearbeitern) auf diese Systeme möglich sein, ist im Sicherheitskonzept (siehe Nr. 6) darzulegen, welche Maßnahmen zur Erreichung eines angemessenen Schutzniveaus ergriffen wurden. Dabei sind die im Modul „Sicherer Fern-

zugriff auf lokale Netze“ (ISi-Fern, BSI-Standards zur Internet-Sicherheit[7]) beschriebenen Maßnahmen zu beachten.

5. Räumliche Sicherheit

Die Unterbringung der systemtechnischen Komponenten (PrivateWire-Verschlüsselungsserver, Anwendungsserver/TLS-Gateways) ist räumlich, organisatorisch und technisch abzusichern (Serverraum), so dass gewährleistet ist, dass nur autorisierte Personen Zugang zur "PrivateWire-Kopfstelle" und/oder den Anwendungsservern/TLS-Gateways haben.

6. Sicherheitskonzept

Es muss ein Sicherheitskonzept / Practise Statement (formlos) oder die für die betroffene Anwendung relevanten Teile eines Sicherheitskonzeptes vorliegen, in dem die detaillierte Umsetzung der geforderten organisatorischen und sicherheitstechnischen Mindestanforderungen beschrieben wird. Das Sicherheitskonzept ist bei Änderungen fortzuschreiben und dem KBA erneut vorzulegen.

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 eine vom externen Kommunikationspartner (d. h. der abrufberechtigten Stelle) unterschriebene Verpflichtungserklärung, in der dieser sich zur Umsetzung und Einhaltung der unter den Punkten 1. – 7. genannten Anforderungen verpflichtet. Ein Vordruck für die Verpflichtungserklärung wird nach Antragstellung für die Anbindung über eine Kopfstelle übersandt.

8. Zugangssperrung

Die Nichteinhaltung einer oder mehrerer der unter Punkt 1. bis 7. beschriebenen Voraussetzungen kann zum Widerruf des Zulassungsbescheides bei gleichzeitiger Sperrung der Zugangsberechtigung der Kopfstelle bzw. der Anwendungsserver/TLS-Gateways durch das KBA führen.

[7] https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Fern/isi-fern.html

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

Kraftfahrt-Bundesamt
24932 Flensburg
Internet: www.kba.de

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

Erschienen im August 2005
Stand: November 2017

Druck: Druckzentrum KBA

Bildquelle: www.shutterstock.de