Verpflichtungserklärung

des Betreibers einer Kopfstelle

Stand: April 2019

§ 1

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

Die Datenkommunikation mit dem Kraftfahrt-Bundesamt (KBA) kann über das Verwaltungs-/ Behördennetz DOI oder über eine von dem externen Kommunikationspartner beauftragte Standleitung erfolgen. Der Zugriff auf die Online-Dialoganwendungen des KBA kann entweder unter Nutzung der KBA-Browser-Dialoge (KBA-Portal) oder der XML-Schnittstellen für die Programm-zu-Programm-Kommunikation erfolgen. Für die bei dieser Art der Datenübermittlung aus Datenschutz- und Datensicherheitsgründen erforderliche Verschlüsselung und Authentifizierung kann bis zum 31.12.2019 das Produkt PrivateWire in der aktuellen Version 4.2 der Firma Algorithmic Research (AR), das in Deutschland von der Fa. Applied Security GmbH vertrieben wird, eingesetzt werden. Unter Einsatz eines Zertifikats kann ab Frühjahr 2017 das PrivateWire Produkt in der Version 5.0 genutzt werden.

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 ohne PrivateWire erfolgen.

(2) Bei der Nutzung der XML-Schnittstellen im Rahmen einer Programm-zu-Programm Kommunikation ist für die erforderliche Verschlüsselung und Authentifizierung die TLS-Verschlüsselung lediglich auf einem Kopfstellen-Server (Verschlüsselungs- und/oder Anwendungs-Server) notwendig, über den bzw. von dem eine automatisierte verschlüsselte Datenkommunikation erfolgt („Kopfstellenlösung“). Um bei dieser Lösung einen automatisierten Verbindungsaufbau zu ermöglichen, wird für die Authentifizierung über die Tastatur das einzugebende Passwort auf dem Server in einem gesonderten und verschlüsselten Eintrag abgelegt.

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.

(3) Bei Einsatz einer "Kopfstelle" (nur bei Kommunikation mit den XML-Schnittstellen des KBA möglich!) oder eines Anwendungsservers über HTTPS ist die interne Kommunikation zwischen den Arbeitsplätzen und dem Server in eigener Zuständigkeit des externen Kommunikationspartners unter Einhaltung organisatorischer und sicherheitstechnischer Mindestanforderungen abzusichern. Diese Maßnahmen sind geeignete technische und organisatorische Maßnahmen entsprechend Art. 5 Abs. 1 f) Datenschutzgrundverordnung (DS-GVO). Darüber hinaus tragen die Maßnahmen dem hohen Schutzbedarf der KBA-Registerdaten Rechnung.

Diese Mindestanforderungen lauten:

a) Zugangs- und Zugriffskontrolle

(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. zum Anwendungsserver/TLS-Gateway zu gewährleisten und unbefugte Nutzungen der Kopfstelle zu verhindern.

Hinweis: Grundsätzlich ist zur Erfüllung dieser Anforderungen eine durchgängige Verschlüsselung vom jeweiligen Endgerät/Client bis zur "Kopfstelle" bzw. zum Anwendungsserver/TLS-Gateway sowie eine sichere gegenseitige Authentifizierung zwischen Anwendungs-Server und Client-PC erforderlich[1]. Die Verschlüsselungsstärke sollte 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 TLS-Verschlüsselung (Entsprechend der BSI-Richtlinie TR-02102-2) in Verbindung mit Zertifikaten auf den Servern (generell zu bevorzugen). Bei Nutzung von RDP (Windows Remote Desktop Protocol) ist dies vorzugsweise ebenfalls die TLS-Verschlüsselung (Entsprechend der BSI-Richtlinie TR-02102-2) 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, 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) 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, dabei muss die fachliche Zuständigkeit identisch sein. 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.

b) Passwortverwendung

Das personenbezogene Passwort bei der Anmeldung am Anwendungs-Server 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.

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

c) 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 des Fachverfahrens nachvollziehbar zu protokollieren (kann bei einem Verfahren nach Buchst. a, Abschnitt ii, Satz 4 entfallen). Es ist zusätzlich eine Protokollierung der systemtechnischen Zugriffe (IP-Adresse, Port) der Kopfstelle 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.

d) System-und netztechnische Sicherheit

Die systemtechnischen Komponenten (Verschlüsselungs-Server und Anwendungs-Server) 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 Punkt f)) darzulegen, welche Maßnahmen zur Erreichung eines angemessenen Schutzniveaus ergriffen wurden. Dabei sind die im Modul „Sicherer Fernzugriff auf lokale Netze“ (ISi-Fern, BSI-Standards zur Internet-Sicherheit[2]) beschriebenen Maßnahmen zu beachten.

e) Räumliche Sicherheit

Die Unterbringung der systemtechnischen Komponenten (Verschlüsselungs-Server und Anwendungs-Server) ist räumlich und organisatorisch so abzusichern, so dass gewährleistet ist, dass nur autorisierte Personen Zugang zur „Kopfstelle" und/oder den Anwendungs-Servern/TLS-Gateways haben.

f) Sicherheitskonzept

Für die Zulassung einer Kopfstelle muss dem KBA ein formloses Sicherheitskonzept vorliegen, in dem die detaillierte Umsetzung der geforderten organisatorischen und sicherheitstechnischen Mindestanforderungen beschrieben ist. Das Sicherheitskonzept ist bei Änderungen jeglicher Art fortzuschreiben und dem KBA in der aktuellen Form vorzulegen.

Das KBA ist berechtigt, jederzeit ein aktuelles Sicherheitskonzept anzufordern.

g) Zulassungsbescheid

Die Aufnahme des Wirkbetriebes der Kopfstelle darf erst nach Erhalt des vom KBA ausgestellten Zulassungsbescheides erfolgen.

(4) Für die Programm-zu-Programm-Kommunikation 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“ zu beachten.

(5) Bei einem Missbrauch oder bereits bei dem Verdacht auf Missbrauch von erteilten Zugangsdaten sowie IT-Sicherheitsvorfällen ist das KBA unverzüglich zu benachrichtigen und die Verwendung von neuen Zugangsdaten zwingend erforderlich.

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

Zu Bürozeiten Montag bis Donnerstag von 7:00 Uhr bis 16:00 Uhr und Freitag von 7:00 Uhr bis 15:00 Uhr wenden Sie sich bitte an die Anwenderbetreuung unter Tel.: 0461-316-1717, außerhalb der Bürozeiten erreichen Sie unseren Benutzerservice unter Tel.: 0461-316-1400.

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- oder 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.

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

(Bezeichnung und Anschrift des Betreibers der Kopfstelle)

(Ort, Datum)

(Unterschrift Behördenleiter/Amtsleiter und Dienststempel)

Anlage 1
zur Verpflichtungserklärung des Betreibers einer Kopfstelle

Stand: April 2019

Der Betreiber der Kopfstelle

_____

_____

(Bezeichnung und Anschrift)

erklärt:

Die für die Programm-zu-Programm-Kommunikation mit dem Kraftfahrt-Bundesamt 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)