Verpflichtungserklärung

der abrufberechtigten Stelle für die Nutzung des KBA-Webportals mittels Browser

Stand: Juli 2023

Die Datenkommunikation mit dem Kraftfahrt-Bundesamt (KBA) erfolgt über das Verwaltungs-/Behördennetz NdB-VN auf die Online-Dialoganwendungen des KBA unter Nutzung der KBA-Webportale.

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 KBA zu gewährleisten und unbefugte Nutzungen zu verhindern.

Bei der Kommunikation zwischen Endgeräte/Clients und Terminalservern ist nur die maximal mögliche Absicherung der eingesetzten Terminalserver-Architektur zulässig. Sofern möglich, sollte eine TLS-Verschlüsselung entsprechend der TR-02102-2[1] genutzt werden.

Werden Terminalserver und die Endgeräte/Clients, mit denen die Anwender über diese Terminalserver auf Dialoganwendungen des Kraftfahrt-Bundesamtes zugreifen, an verschiedenen Standorten, bzw. in getrennten Liegenschaften betrieben, sind grundsätzlich zur Absicherung der Kommunikation zwischen diesen Standorten vom BSI für VS-NfD klassifizierten Daten zugelassene Verschlüsselungssysteme zu verwenden. Mindestens ist eine durchgängige Verschlüsselung bis zum jeweiligen Endgerät/Client sowie eine sichere gegenseitige Authentifizierung sicherzustellen. Hierbei sind die Vorgaben der Technischen Richtlinien TR-02102[2] 1 bis 4, sowie der BSI-Standard zur Internet-Sicherheit (ISi-VPN) einzuhalten.

Die über die Online-Dialoganwendungen bereitgestellten Daten dürfen nur für den angegebenen Zweck verwendet und nur an berechtigte Stellen weitergegeben werden.

Hard- und Software sind räumlich, organisatorisch und systemseitig durch geeignete Maßnahmen gegen unautorisierte Zugriffe zu schützen und auf einem aktuellen sicherheitstechnischen Stand zu halten. Zudem sind Schutzmaßnahmen gegenüber unberechtigten Zugriffen aus anderen Netzen (insbesondere dem Internet) vorzunehmen.

Die Vergabe, der vom KBA für die Authentifizierung gegenüber den Online-Dialoganwendungen vergebenen Zugangsdaten, erfolgt i. A. dienststellenbezogen. Es ist sicher zu stellen, dass nur

---

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr-02102.html

berechtigte Nutzer diesen Zugang nutzen. Bei Bekanntwerden, dass Zugangsdaten an Dritte weitergegeben wurden, werden diese unverzüglich vom KBA gesperrt. Aus Sicherheitsgründen werden die Zertifikate ebenfalls deaktiviert. Neue Zugangsdaten können unter Anwenderbetreuung@kba.de, neue Zertifikate unter Zertifikatsbeantragung@kba.de beantragt werden.

Für den Zugriff auf die ZEVIS-Dialoganwendungen ist auf Terminalservern oder Endgeräten/Clients, auf denen ein oder mehrere Mitarbeiter arbeiten, je ein TLS-Verschlüsselungs-Zertifikat zu nutzen.
Für die Zugriffe ist sicherzustellen, dass jederzeit ermittelt werden kann, welcher Mitarbeiter zu einem definierten Zeitraum von welchem System aus über welches Zertifikat auf KBA-Dialoganwendungen zugegriffen hat. Daher sind von den Mitarbeitern benutzerbezogen Benutzerkennungen für die Anmeldung am Terminalserver oder Endgerät/Client zu nutzen und eine Protokollierung der An- und Abmeldungen am System sicherzustellen.
Protokolldaten sind zum Schutz vor Manipulation sicher und konsistent zu erheben, zu speichern und vor dem Zugriff Unbefugter zu schützen. Zudem ist ihre ordnungsgemäße Entsorgung sicherzustellen“. Dies bedeutet insbesondere im Einzelnen:

- verschlüsselte Übertragung,
- gesicherte Speicherung und
- Gewährleistung eines Zugriffsschutzes

auf dem jeweils aktuellen Stand der Technik.
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, z. B. bis zur Übergabe an die Strafverfolgungsbehörden.
Alternativ können auf einem System, auf denen Mitarbeiter abwechselnd arbeiten, auch für jeden Mitarbeiter eigene Zertifikate genutzt werden.

Pflichten der erklärenden Stelle:

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

a) Anschriftenänderungen und Änderungen der Ansprechpartner

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

c) sonstigen Umständen, die für den Zugriff bedeutsam sind bzw. die die Nichteinhaltung der genannten Mindestanforderungen zur Folge haben, insbesondere im Kompromittierungsfall.

(2) Ist bei der erklärenden Stelle pro Zertifikat mehr als ein Endgerät/Client zugeordnet, so muss diese dem KBA gegenüber neben der Verpflichtungserklärung eine schriftliche Beschreibung der Einhaltung der o. g. Mindestanforderungen vorlegen. Dies betrifft insbesondere die Verschlüsselung vom Endgerät/Client zum Terminalserver sowie das Erheben der

Protokolldaten. Das KBA behält sich vor ein Sicherheitskonzept, das die Sicherheitsmaßnahmen detailliert beschreibt, anzufordern.

Bei einem Missbrauch oder bereits bei dem Verdacht auf Missbrauch von erteilten Zugangsdaten sowie bei 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.

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

(Bezeichnung und Anschrift der abrufberechtigten Dienststelle)

(Ort, Datum)

(Unterschrift Behördenleiter/Amtsleiter und Dienststempel)