Verpflichtungserklärung

der abrufberechtigten Stelle mittels Browser-Dialog

Stand: Januar 2021

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

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 Clients und Terminalservern ist nur die maximal mögliche Absicherung der eingesetzten Terminalserver-Architektur zulässig. Sofern möglich, sollte eine TLS-Verschlüsselung entsprechend der TR-2102-2[1] genutzt werden.

Werden Terminalserver und die Endgeräte, 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 sind eine durchgängige Verschlüsselung bis zum jeweiligen Endgerät sowie eine sichere gegenseitige Authentifizierung sicherzustellen. Hierbei sind die Vorgaben der Technischen Richtlinien TR-2102[2] 1 bis 4, sowie der BSI-Standard zur Internet-Sicherheit (ISi-VPN[3]) 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 grundsätzlich dienststellenbezogen. Es ist sicher zu stellen, dass nur berechtigte Nutzer diesen Zugang nutzen.

---

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf;jsessionid=D3B4A731FCB88B722B71CE1381C148BD.2_cid351?__blob=publicationFile&v=6

[2] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[3] https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html

Für den Zugriff auf die ZEVIS-Dialoganwendungen ist auf Terminalservern oder anderen Systemen auf denen mehrere Mitarbeiter parallel arbeiten für jeden Anwender ein eigenes TLS-Zertifikat zu nutzen. Auf Systemen, auf denen Mitarbeiter abwechselnd arbeiten, ist sicherzustellen, dass jederzeit ermittelt werden kann, welcher Mitarbeiter zu einem definierten Zeitraum von diesem System aus auf KBA-Dialoganwendungen zugegriffen hat .Auf einem System, auf denen Mitarbeiter abwechselnd arbeiten, kann daher ein Zertifikat von verschiedenen Mitarbeitern genutzt werden, wenn die Mitarbeiter verschiedene Benutzerkennungen für die Anmeldung am PC / IT-System nutzen und eine Protokollierung der An- und Abmeldungen am System erfolgt.
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) Änderungen der IP-Adresse
b) Anschriftenänderungen und Änderungen der Ansprechpartner
c) Änderungen (Wegfall, Hinzukommen, qualitative Änderungen) der abrufenden Stellen
d) sonstigen Umständen, die für den Zugriff bedeutsam sind bzw. die die Nichteinhaltung der genannten Mindestanforderungen zur Folge haben, insbesondere im Kompromittierungsfall.

Bei einem Missbrauch oder bereits bei dem Verdacht auf Missbrauch von erteilten Zugangs-daten sowie bei IT-Sicherheitsvorfällen ist das KBA unverzüglich zu benachrichtigen und die Verwendung von neuen Zugangsdaten zwingend erforderlich.
Zu Bürozeiten von 7:00 Uhr bis 16:00 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.

(Bezeichnung und Anschrift der abrufberechtigten Dienststelle)

(Ort, Datum)

(Unterschrift Behördenleiter/Amtsleiter und Dienststempel)