KVB
Kassenärztliche Vereinigung Bayerns

KV-Ident Plus

Informationsblatt zum Datenschutz bei Nutzung von KV-Ident Plus

Stand Oktober 2023

KV-Ident Plus ist ein so genanntes starkes Authentisierungsverfahren und bietet den KVB-Mitgliedern Zugang zu den webbasierten Informationsangeboten und Dienstleistungen der KVB sowie zum Sicheren Netz der KVen (SNK). Letzteres ist nur in Verbindung mit einer Installation der VPN-Software möglich. Der Besitz eines persönlichen KV-Ident Plus Tokens und das Wissen des Kennworts der persönlichen KVB-Benutzerkennung realisieren eine Zwei-Faktor-Authentisierung für die sichere Anmeldung im Mitgliederportal „Meine KVB“ bzw. den darin enthaltenen Online-Anwendungen sowie zum SNK.

Bei der Nutzung der webbasierten Informationsangebote und Dienstleistungen der KVB können alle Daten über eine Tunnelverbindung (VPN) oder ohne Tunnelverbindung über das Internet per SSL-Verschlüsselung an die KVB übermittelt werden. Die VPN-Software zum Aufbau der Tunnelverbindung, welche die KVB zu diesem Zweck zur Verfügung stellt, kann zur Nutzung von KV-Ident Plus über eine Tunnelverbindung auf einem Rechner installiert werden.

Für die Nutzung von KV-Ident Plus wird ein Rechner mit aktuellem Betriebssystem und Internetzugang sowie einem aktuellen Internet-Browser benötigt. Zusätzlich kann optional auf dem Rechner die von der KVB zur Verfügung gestellte VPN-Software installiert werden.

KV-Ident Plus gewährleistet die Sicherheit des Daten- und Informationsaustausches erst ab dem Zeitpunkt, ab dem der Tunnel aufgebaut ist. Bis zum Aufbau des Tunnels und der Authentisierung mit KV-Ident Plus bewegt sich der Nutzer im öffentlichen Internet. Hierfür und für eventuelle Auswirkungen von Schadprogrammen auf dem Rechner (z.B. Mitlesen von Tastatureingaben und Bildschirminhalten) übernimmt die KVB keine Haftung.

Für die Absicherung seines Rechners gegen unbefugte Zugriffe von Dritten ist der Nutzer selbst verantwortlich. In diesem Zusammenhang ist auf die Einhaltung der Anforderungen zur Gewährleistung der IT-Sicherheit[1] zu achten.

[1] RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT
Direktlink: https://hub.kbv.de/site/its

Gemäß dieser Anforderungen zur Gewährleistung der IT-Sicherheit sind vom Nutzer u.a. folgende IT-Sicherheitsmaßnahmen zu tätigen[2]:

- Einsatz von aktuellen Viren-Schutzprogrammen und regelmäßige Aktualisierung der eingesetzten Viren-Schutzprogramme.
- Einsatz einer Firewall. Eine Firewall ist eine Netzwerk-Sicherheitskomponente, die entscheidet, auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann, und welche Dienste des nicht sicheren (öffentlichen) Netzes, wie z. B. das Internet, aus dem privaten Netz heraus nutzbar sind. Sie gewährleistet somit die Einhaltung von Sicherheitsrichtlinien zwischen einem privaten und einem öffentlichen (nicht sicheren) Netz.

Bei der Teilnahme am KV-Ident Plus Verfahren der KVB obliegt es der Sorgfaltspflicht des Nutzers, für die eigene Rechnersicherheit zu sorgen. Die KVB weist ausdrücklich auf diese Sorgfaltspflicht hin. Bei Verwendung eines Rechners, der über einen direkten Zugriff auf Patientendaten oder einen anderen vernetzten Rechner mit Patientendaten verfügt, ist dieser nach gängigem Stand der Technik vom Internet zu schützen. Auf den Seiten des Bundesamts für Sicherheit in der Informationstechnik (www.bsi.de) werden die entsprechenden Empfehlungen dazu in aktueller Form vorgehalten und zur allgemeinen Nutzung zur Verfügung gestellt.

KV-Ident Plus bietet hohe Sicherheitsstandards durch die Kombination der Benutzerkennung und des Tokens bei der Authentisierung. Um den Datenverkehr wirksam zu schützen, ist ein sorgfältiger Umgang mit beiden Faktoren unbedingt notwendig. Aus diesem Grund ist es wichtig, ein sicheres Kennwort auszuwählen und dieses sicher aufzubewahren.

Folgende Sicherheitsregeln sind zur Auswahl eines sicheren Kennworts und zum Umgang mit der KVB-Benutzerkennung zu beachten:

- Ein sicheres Kennwort muss aus mindestens 12 Zeichen bestehen und mindestens eine Zahl, einen Groß- und einen Kleinbuchstaben sowie mindestens ein Sonderzeichen enthalten, und darf zudem nicht identisch mit dem alten Passwort sein.
- Dasselbe Kennwort darf nicht für mehrere unterschiedliche Online-Dienstleistungen benutzt werden.
- Das Kennwort ist geheim zu halten. Es darf nicht aufgeschrieben werden und unter keinen Umständen auf dem Rechner (Datei, Browser, etc) gespeichert werden.
- Das Kennwort darf keinem unbefugten Dritten überlassen werden.
- Beim Verlassen des Arbeitsplatzes muss eine Abmeldung von der jeweiligen Anwendung mittels des Buttons „Abmelden“ (oben rechts) erfolgen. Zudem ist der Browser vor dem Verlassen des Arbeitsplatzes zu schließen.

Bei der Vermutung, dass jemand Zugang zum Kennwort erlangt hat, ist die persönliche KVB-Benutzerkennung unverzüglich zu sperren oder sperren zu lassen.

[2] nicht abschließende Aufzählung

Eine Sperrung der KVB-Benutzerkennung kann vom Nutzer selbst durch eine absichtliche mehrfache Falscheingabe des Kennworts oder telefonisch über unseren eTec Support vorgenommen werden.

Folgende Sicherheitsregeln sind zudem für den Umgang mit dem KV-Ident Plus Token zu beachten:

- Der KV-Ident Plus Token darf nicht zugänglich für unbefugte Dritte aufbewahrt werden.
- Beim Verlassen des Arbeitsplatzes ist die bestehende Verbindung mit dem Button „Abmelden“ zu beenden. Zudem ist der Browser vor dem Verlassen des Arbeitsplatzes zu schließen.
- Der KV-Ident Plus Token darf keinem unbefugten Dritten überlassen werden.
- Der abgefragte Einmalcode des KV-Ident Plus Tokens darf niemals am Telefon genannt werden, noch auf Anfrage bei sogenannten Phishing E-Mails eingegeben.
- Bei Verlust des KV-Ident Plus Tokens muss dieser unverzüglich gesperrt oder beendet werden.

Über das Portal Token-Verwaltung kann der Nutzer jederzeit seine(n) KV-Ident Plus Token temporär sperren oder auch endgültig beenden.

Weitergehende Informationen zum Thema Datenschutz sowie die Erläuterung der Nutzerrechte können der KVB-Internetseite unter: https://www.kvb.de/mitglieder/praxisfuehrung/pflichten/datenschutz-in-der-praxis entnommen werden.