

## Für die Aktivierung Ihres eHBA halten Sie bitte bereit:

- Ihren **elektronischen Heilberufsausweis**
- Ihren **PIN-Brief**
- Ihr Primärsystem mit Telematikinfrastruktur-Anbindung (PTV3-Konnektor) muss eHealth-fähig sein.

## 2 Aktivierung und Einsatz

### 2.1 eHBA aktivieren

Die Aktivierung des elektronischen Heilberufsausweises durch die Initialisierung der PIN erfolgt über Ihr Primärsystem (z.B. PVS) in Verbindung mit einem für die Telematikinfrastruktur zugelassenen PTV3-Konnektor. **Bitte beachten Sie, dass der eHBA erst mit einem eHealth-fähigen PTV3-Konnektor innerhalb der Telematikinfrastruktur nutzbar ist.** Bei Rückfragen zur Aktivierung des eHBA wenden Sie sich bitte direkt an Ihren Anbieter des Primärsystems.

- Die Vorgehensweise kann systemabhängig variieren. In jedem Fall werden aber folgende Eingaben erforderlich: Geben Sie die Transport-PINs (PIN.QES und PIN.CH) aus Ihrem PIN-Brief in das Eingabefeld „PIN.QES Transport-PIN“ bzw. „PIN.CH Transport-PIN“ ein.
- Vergeben Sie zwei neue Wunsch-PINs (6-8 Zeichen): Die PIN.QES dient zur Erzeugung rechtsverbindlicher elektronischer Unterschriften (qualifizierte Signatur). Mit der PIN.CH schalten Sie alle anderen Anwendungen frei, wie z. B. die Anmeldung an Anwendungen oder die Entschlüsselung von Dokumenten.

**Achtung: Wenn Sie Ihre Transport-PINs in drei aufeinanderfolgenden Versuchen falsch eingeben, werden diese endgültig gesperrt. Die Transport-PINs können durch die PUKs nicht zurückgesetzt bzw. entsperrt werden.**

### Alternative Aktivierung

Sollten Sie aktuell keine Möglichkeit zur Aktivierung des eHBA über Ihr Primärsystem haben (siehe oben), so können Sie diesen mit Hilfe eines **handelsüblichen Kartenlesegerätes** sowie des **D-TRUST Card Assistant** aktivieren. In diesem Fall wenden Sie sich bitte an unseren eHealth-Support unter **ehealth-support@bdr.de** oder **+49 (0) 30 2598-4050**

### Hinweise zur PIN-Vergabe

Sie haben jederzeit die Möglichkeit, eine neue PIN zu setzen. Ändern Sie Ihre PIN immer dann, wenn Sie den Verdacht haben, dass eine unberechtigte Person von Ihrer PIN Kenntnis erlangt haben könnte.

**Beachten Sie bitte die folgenden Ratschläge zur Auswahl einer geeigneten PIN.**

- Die Zahlenkombination der PIN muss aus 6-8 Zeichen und den Ziffern 0-9 bestehen.
- Wählen Sie eine Buchstaben-/Ziffernkombination, die Sie leicht merken können.

- Verwenden Sie keine Kombinationen, die Ihnen leicht zugeordnet werden können, wie z. B. Geburtsdatum, Hochzeitsdatum oder Telefonnummer.
- Vermeiden Sie triviale Zahlenkombinationen wie 123456, 111111 usw.

**Notieren Sie sich Ihre PIN nach Möglichkeit nicht. Verwahren Sie Ihre PIN nie zusammen mit Ihrem eHBA.**

### 2.2 PIN entsperren

Wenn Sie eine Ihrer PINs in drei aufeinanderfolgenden Versuchen falsch eingeben, können Sie diese mit Hilfe der zugehörigen PUK (PUK.QES bzw. PUK.CH) entsperren. Sie haben nach dem Entsperren erneut 3 Versuche zur Eingabe der entsperrten PIN.

Falls Sie die PIN.CH vergessen haben, können Sie mithilfe der zugehörigen PUK.CH während des Entsperrens eine neue PIN.CH vergeben. Für die normale PIN-Änderung bei Kenntnis der bisherigen PIN sollten Sie die PUK nicht verwenden.

Die PIN.QES kann **nur** unter Angabe der aktiven PIN.QES, welche während der Aktivierung vergeben wurde, geändert werden.

**Wenn Sie die ursprüngliche PIN.QES endgültig vergessen oder verloren haben, kann die QES-Funktion (Erzeugung rechtsverbindlicher elektronischer Unterschriften) des eHBA nicht mehr genutzt werden.**

### Hinweise zur PUK

**Die PUK selbst kann nicht geändert werden.**

Aus Sicherheitsgründen kann eine PUK insgesamt nur zehnmal eingegeben werden. Dabei wird nicht zwischen richtiger und falscher PUK-Eingabe unterschieden!

Haben Sie eine PUK zehnmal verwendet, ist keine weitere Entsperrung der zugehörigen PIN mehr möglich. In diesem Fall benötigen Sie einen neuen eHBA. Kontaktieren Sie unseren Support oder beantragen Sie gleich einen neuen Ausweis im [Antragsportal](#).

### 2.3 Zertifikate auf dem eHBA sperren

**Achtung: Die Sperrung der Zertifikate kann nicht rückgängig gemacht werden!**

Bei Verlust Ihrer Karte beauftragen Sie bitte im [Antragsportal](#) die Sperrung der Zertifikate, um Missbrauch vorzubeugen.

**Beachten Sie bitte:** Sind die Zertifikate auf Ihrer Karte gesperrt oder ist deren Gültigkeit abgelaufen, sollten Sie aus Sicherheitsgründen den Chip der Karte physikalisch zerstören (z. B. durch Zerschneiden). Es wird empfohlen, zuvor alle verschlüsselten Daten zu entschlüsseln und zu sichern.