Elektronischer Heilberufsausweis (eHBA)

Spezifikationen

- Certificate Policy - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL - Rahmenvorgaben der gematik für die Sicherheit des Ausgabeprozesses
- Gemeinsame Policy für die Ausgabe der Heilberufsausweise von BÄK und anderen Kartenherausgebern [CP-HBA]
- Spezifikation des elektronischen Heilberufsausweises - HBA-Objektsystem

Anbieterspezifische Spezifikationen

Certificate Practice Statements

- D-Trust[1)]
- medisign[2)]
- SHC
- T-Systems[3)]

Allgemeine Geschäftsbedingungen

- D-Trust[4)]
- medisign
- SHC[5)]
- T-Systems

Was ist der eHBA?

Ein **eHBA** ist eine Chipkarte, die X.509-Zertifikate enthält, die nach [CP-HBA] ausgestellt wurden. Die Zertifikate des eHBA bilden hierbei die kryptografische Identität einer Person ein der elektronischen Welt ab. Die Nutzung der privaten Schlüssel eines eHBA sind nur nach vorheriger und erfolgreicher PIN-Eingabe möglich.

Ein **Endnutzerzertifikat** ist eine Zertifikat, das zu einem im eHBA gespeicherten privaten Schlüssel gehört und auf den Ausweisinhaber als Zertifikatsinhaber ausgestellt ist.

Prozess der Kartenherausgabe

Akteure/Rollen

Die Definitionen richten sich nach der [CP-HBA].

Kartenherausgeber

Für die Ausgabe eines eHBA zuständige Stelle gem. § 340 SGB V (i.d.R. sind das die Länderberufskammern). Ein Kartenherausgeber (KHG) gibt den eHBA nur für einen bestimmten Kreis an Antragstellern heraus und bedient sich dabei der Hilfe eines oder mehrerer Anbieter. Diese Zusammenarbeit ist vertraglich vereinbart.

Antragsteller

Eine natürliche Person, die einen eHBA bei einem für ihn zuständigen KHG bzw. Anbieter beantragt.

Anbieter

Ein qualifizierter Vertrauensdienstanbieter (VDA) nach eIDAS, der für einen KHG tätig ist und die Zertifikate nach CP-HBA ausstellt. Ein Anbieter kann sich auch eines eines qualifizierten VDA bedienen. In diesem Fall sorgt der Anbieter dafür, dass die Rechte und Pflichten, die durch eIDAS geregelt sind, auch für diese Vertragskonstellation gewährleistet werden. Ein Anbieter kann für mehrere KHG, auch unterschiedlicher Sektoren, tätig sein.

Anbieterspezifische Prozessinfos

- D-Trust
- medisign
- SHC
- T-Systems

Betriebspartner der Anbieter

D-Trust

- IDEMIA (Kartenpersonalisierer und -produzent) (G2.1)
- Giesecke & Devrient (Kartenpersonalisierer und -produzent) (G2.0)

medisign

- Giesecke & Devrient (Kartenpersonalisierer und -produzent)
- DGN (eigener Gesellschafter) (VDA)
- Rhenus Docs to Data (Scan-Dienstleister und Archivierung)

SHC

- Eviden (VDA)
- IDEMIA (Kartenpersonalisierer und -produzent)
- Dokuhaus (Scan-Dienstleister und Archivierung)

T-Systems

keine

Schlüsselpaare

Anwendungsbereich	Schlüsselpaar bzw. Zertifikat
Qualifizierte elektronische Signatur	C.HP.QES
Authentifizierung	C.HP.AUT
Ver- bzw. Entschlüsselung	C.HP.ENC

Austausch von eHBA

Ab dem 1. Januar 2026 dürfen eHBA der Generation 2.0 aus Sicherheitsgründen[6)] nicht mehr eingesetzt werden, da diese nur den Verschlüsselungsalgorithmus RSA 2048-Bit verwenden. Davon ist eine große Anzahl der derzeit im Umlauf befindlichen elektronischen Heilberufsausweise betroffen. Ein Austausch dieser Karten ist noch im Laufe dieses Jahres erforderlich. Im Wesentlichen handelt es sich dabei um eHBA der Anbieter D-Trust/Bundesdruckerei und DGN/medisign.

Die eHBA der Nachfolgegeneration 2.1 verfügen zusätzlich über den Verschlüsselungsalgorithmus ECC (Elliptic Curve Cryptography), der ab 2026 den alten RSA-Algorithmus ablösen wird. Diese Verschlüsselung entspricht nicht nur dem aktuellen Stand der Technik, sondern gewährleistet auch die Zukunftsfähigkeit und Performance der Telematikinfrastruktur. Die Kartengeneration ist auf der Rückseite des elektronischen Heilberufsausweises, oben rechts unter dem CE-Zeichen vermerkt und kann mit einem Blick geprüft werden. Für Ausweise der Generation 2.1 ist kein Austausch notwendig.

Der anstehende Massentausch stellt einen erheblichen Aufwand dar – sowohl für die Kartenanbieter als auch für die herausgebenden Ärztekammern.

Frühzeitiges Handeln verhindert Nutzungsausfälle

Die Anbieter werden die betroffenen Ärztinnen und Ärzte in mehreren Informationswellen gezielt anschreiben und über das notwendige Vorgehen informieren. Die Verfahren zum Kartentausch unterscheiden sich im Detail zwischen den Anbietern. Die Anbieter informieren darüber hinaus auf eigenen Webseiten[7)] ausführlich zum Thema. eHBA der Generation 2.0 ohne ECC-Unterstützung werden automatisch zum 31.12.2025 gesperrt. Daher sollten Ärztinnen und Ärzte in jedem Falle rechtzeitig auf das Anschreiben Ihres Anbieters reagieren und den für den Austausch notwendigen Schritten folgen. . Wer den Austausch nicht rechtzeitig vornimmt, kann TI-Anwendungen, für die ein eHBA benötigt wird, wie bspw. das E-Rezept oder die elektronische Arbeitsunfähigkeitsbescheinigung (eAU), nicht mehr nutzen. In diesem Fall wird die Beantragung eines neuen eHBA notwendig, was ggf. mit Wartezeiten und zusätzlichem Aufwand für erneute Identifikation und Freigabe verbunden ist.

Auswirkungen auf den Praxisbetrieb und Kosten

Sofern der eHBA rechtzeitig getauscht wird, hat die Umstellung auf die Folgegeneration mit ECC keine Auswirkungen auf den laufenden Betrieb von TI-Anwendungen. Frühzeitige Reaktion sichert somit die berufliche Handlungsfähigkeit und entlastet zugleich die Ärztekammern im Hinblick auf die Freigabeprozesse.

Besonderheiten beim Austausch beim Anbieter SHC

Die eHBA der Anbieter T-Systems und SHC sind bereits von der neueren Generation 2.1 und damit

nicht von dem Algorithmuswechsel betroffen. Allerdings verwenden einige eHBA des Anbieters SHC einen theoretisch als unsicher geltenden Chip. Daher müssen die betroffenen Karten bis zum 30.06.2026 ausgetauscht werden. Das Verfahren ist für die Ärztinnen und Ärzte kostenlos und ähnelt dem für den Austausch der eHBA der Generation 2.0. Der Anbieter SHC wird die betroffenen Ärztinnen und Ärzte voraussichtlich ab August 2025 anschreiben und auch auf seiner Webseite über Details des Austauschprozesses informieren. Auch hier empfiehlt es sich, zeitnah auf das Anschreiben zu reagieren.

FAQ

Warum muss ich mich umständlich identifizieren, um einen Ausweis zu erhalten?

Über die Identifikation wird die reale Identität mit der virtuellen Identität, die durch den eHBA präsentiert wird, verknüpft. Da der eHBA zudem Träger einer QES ist, gelten hier besondere gesetzliche Auflagen in Bezug auf die Sicherheit des Ausgabeprozesses. Daher sind nur gemäß dieser gesetzlichen Vorgaben zertifizierte Identverfahren zulässig. POSTIDENT zählt bspw. dazu, auch die Identifizierung über die Online-Ausweisfunktion des Personalausweises, nicht jedoch das Video-Ident.[8)]

Wird der eHBA finanziert?

Kurz: Der eHBA in der **ambulanten vertragsärztlichen Versorgung** wird über die TI-Pauschale finanziert. In der **stationären Versorgung** erhält ein Krankenhaus für jeden im Krankenhaus tätigen Mitarbeiter pauschal 46,52 € pro Jahr, wobei das Krankenhaus im Innenverhältnis die Weiterleitung des Betrags an den jeweiligen ärztlichen Mitarbeiter gewährleisten muss.

Lang: Ambulante Einrichtungen erhalten eine monatliche Pauschale, um die Installation und den Betrieb der TI zu finanzieren. Diese Regelung und die Höhe der Pauschale hat das Bundesministerium für Gesundheit (BMG) per Rechtsverordnung festgelegt und auf Drängen der KBV und der Kassenärztlichen Vereinigungen mehrmals angepasst. Laut BMG sollen mit der Pauschale alle Kosten des Anschlusses und des Betriebes der TI erstattet werden. Gemäß § 10 Absatz 2 dieser TI-Festlegung erhöht sich die monatliche TI-Pauschale jeweils zum 1. Januar eines Jahres entsprechend der Veränderung des Punktwertes des Orientierungswertes gemäß § 87 Absatz 2e SGB V. In einem Dokument der KBV kann die Entwicklung der monatlichen Pauschalen nachvollzogen werden.

Die Finanzierung des eHBA in der stationären Versorgung richtet sich nach der TI-Finanzierungsvereinbarung für Krankenhäuser [9)]. Die Kosten für den HBA gehören gem. § 9 Abs. 3 zu den „Kosten im laufenden Betrieb“. Ein Krankenhaus erhält „nach Wahl“ für jeden im Krankenhaus tätigen ärztlichen Mitarbeiter eine Pauschale in Höhe von 46,52 € pro Jahr. Bei Wahl dieser Option muss das Krankenhaus im Innenverhältnis die Weiterleitung des Betrags an die jeweiligen ärztlichen Mitarbeiter gewährleisten. Die Pauschale deckt gegenwärtig etwa 11% der jährlich anfallenden Kosten für einen HBA bei allen HBA-Anbietern.

Was kostet ein eHBA?

Kurz: Die Kosten bei allen derzeitigen HBA-Anbietern unterscheiden sich nur marginal und liegen

zwischen etwa 83 € und 92 € netto pro Jahr.

Lang: Die Kosten bei allen derzeitigen HBA-Anbietern unterscheiden sich nur marginal und liegen zwischen etwa 83 € und 92 € netto pro Jahr. Details in der folgenden Tabelle:

	Preise (netto) zum Vergleich								Förderung
	5-Jahre (Laufzeit)		Jahr		Quartal		Monat		%
	Gesamt	gefördert	Gesamt	gefördert	Gesamt	gefördert	Gesamt	gefördert	
D-Trust	**420,17 €**	232,60 €	84,03 €	46,52 €	21,01 €	**11,63 €**	7,00 €	3,88 €	55,36%
medisign	465,03 €	232,60 €	**93,01 €**	46,52 €	23,25 €	**11,63 €**	7,75 €	3,88 €	50,02%
T-Systems	420,00 €	232,60 €	84,00 €	46,52 €	**21,00 €**	**11,63 €**	7,00 €	3,88 €	55,38%
SHC	413,62 €	232,60 €	**82,72 €**	46,52 €	**20,68 €**	**11,63 €**	6,89 €	3,88 €	56,24%

Links zu den Preisinformationen der einzelnen HBA-Anbieter:

- D-TRUST
- medisign
- SHC
- T-Systems

Wie lange ist ein eHBA gültig?

Kurz: Ein eHBA ist maximal 5 Jahre gültig.

Lang: Die Gültigkeit eines eHBA beträgt derzeit maximal 5 Jahre. Diese maximale Laufzeit ist für Signaturkarten üblich, da die Sicherheit der mit den Zertifikaten verbundenen Schlüsseln in der Regel mit zunehmendem Zeitraum abnimmt und die Schlüssel daher regelmäßig erneuert werden sollten. Die gematik formuliert (als SOLL-Anforderung) entsprechend auch 5 Jahre als Maximallaufzeit.[10)]. Die Gemeinsame Policy für die Ausgabe der Heilberufsausweise (S. 19) referenziert auf [gemSpec_Krypt] bzgl. der maximalen Gültigkeitsdauer von X.509-Zertifikaten.

Die HBA-Anbieter können kürzere Laufzeiten mit den Kartenherausgebern vereinbaren.[11)]

Was ist der Unterschied zwischen einem eHBA der Generation 2.0 und 2.1?

- Aktualisierte kryptographische Schlüssel unter Nutzung eines neuen Verfahrens (ECC statt RSA), wobei auch die alte Schlüsselgeneration noch auf der Karte ist.
- Stapelsignatur auch ohne Konnektor möglich

Kann ich bereits einen eHBA der G2.1 bestellen?

Derzeit geben alle Anbieter ausschließlich HBA G2.1 aus. Die alten G2.0-Karten werden bis Ende 2025 ausgetauscht.

Wozu benötige ich im KH einen HBA?

- Technisch zum Aufbringen einer persönlichen QES (vermutlich insbesondere beim

Entlassmanagement)
    - Anlegen eines NFD
    - Signatur eines in der vertragsärztlichen Versorgung vergüteten Arztbriefes (KIM-Kontext)
    - eAU
    - Anlegen eines E-Rezeptes
- Rechtlich wegen § 339 für jeden Zugriff auf folgende medizinische Anwendungen (also wohl fast jeder Arzt, der bspw. Dienst in der Notaufnahme tut)
    - ePA
    - Hinweise
    - eMP
    - NFD
    - E-Rezept (Anschlussmedikation verordnen im Entlassmanagement oder in der Onkologie mit der Verordnung von Zytostatika, ggf. i.V.m. der Verordnung von parenteraler Ernährung, und der entsprechenden Einbindung der KHApotheke in den elektronischen Abrechnungsprozess spätestens ab 1.1.2022.)

Hinweise der DKG insbesondere hier in Kap. 3.5.

Wie lang müssen die PINs für den HBA sein?

PIN.CH: 6-8 Zeichen PIN.QES: 6-8 Zeichen

Was passiert bei falscher PIN-Eingabe für den HBA?

Hier gibt es Unterschiede zwischen den Transport-PINs, der PIN.CH (für AUT und ENC) und der PIN.QES.

- Für die Änderung der beiden Transport-PINs haben Sie jeweils nur 3 Fehlversuche. Nach dreimaliger Falscheingabe der Transport-PINs ist Ihre Karte unwiederbringlich gesperrt.
- Nachdem Sie Ihre persönlichen PINs erfolgreich gesetzt haben, können Sie Karten-PIN nach dreimaliger Falscheingabe durch die Eingabe eines PUK (Personal Unblocking Key), den Sie im Transport-PIN-Brief finden, neu setzen.
- Die Signatur-PIN kann durch den PUK entsperrt, jedoch nicht neu gesetzt werden.

Der PUK kann insgesamt nur zehnmal genutzt werden; die dreimalige Falscheingabe des PUK führt dazu, dass dieser unbrauchbar wird.

Was muss ich tun, nachdem ich den eHBA und den zugehörigen PIN-Brief erhalten haben

Sie müssen den eHBA und den zugehörigen PIN-Brief als getrennte Sendung erhalten haben, bevor sie ihren HBA in Betrieb nehmen können.

Sie müssen nun

- den eHBA aktivieren und
- ihn zur Nutzung freischalten.

- **Aktivierung**: Umwandlung der beiden Transport-PINs aus dem PIN-Brief in selbstgewählte PINs
- **Freischaltung**: Mit der Freischaltung bestätigen Sie, dass Sie Ihren Ausweis erhalten haben und die Transport-PINs erfolgreich in persönliche PINs ändern konnten. Zudem werden die Zertifikate Ihres eHBA im Statusdienst veröffentlicht, damit ihre aktuelle Gültigkeit abgefragt werden kann. Erst nach diesem Schritt ist Ihr Ausweis einsatzbereit.

Die Verfahren dazu sind anbieterspezifisch und die Anbieter bieten dafür jeweils detaillierte Anleitungen:

- D-TRUST
- medisign
- T-Systems (nur Freischaltung, keine Aktivierung wird beschrieben)
- SHC (nur Freischaltung, keine Aktivierung)

Was unterscheidet die einzelnen HBA-Anbieter?

- Preise und Preiszusammensetzung (marginal, einmalige Einrichtungsgebühr medisign)
- Abrechnungszeiträume
- Angebotene Identverfahren über das verpflichtende POSTIDENT (und Kammerident für Sachsen) hinaus
- Zusammenarbeit mit unterschiedlichen PVS-Herstellern
- Ausgegebene Kartengenerationen

Wird der eHBA mit der TI 2.0 nicht überflüssig?

- Keineswegs, wie inzwischen auch die gematik betont
- Zunächst wird die Migration zur TI 2.0 nicht als Big Bang erfolgen können, der Zeithorizont ist angesichts des jetzigen Standes und der vergangenen Entwicklungszeiten auch eher optimistische geschätzt, trotz des vielfach beschworenen höheren Tempos seit BMG-Übernahme der gematik und verstärkter Digitalisierungsgesetzgebung durch jens Spahn. (Machbarkeitsstudie, Schritt- für Schritt-Migration)
- Smartcards wie der eHBA sind aktuell das sicherste Mittel private Schlüssel sicher aufzubewahren. Da der HBA Schlüssel trägt, die eine QES ermöglichen gelten hier höchste Sicherheitsanforderungen, die derzeit kaum erreichbar ist mit alternativen Hardware-Token wie beispielsweise einem Smartphone mit eSIM oder Secure Element.
- Ein wird Arzt nicht jedesmal sein Handy zücken wollen, um sich zu authentifizieren und dann zu signieren, verschlüsseln.
- Auch sogenannte digitale Identitäten sind in der Regel von der Smartcard abgeleitet in das Handy transportiert.
- Es wird also aufgrund fehlender Alternativen für eine absehbare Zeit (mind. 5 Jahre, also der Gültigkeitszeitraum eines HBAs) keine Alternative für bestimmte Szenarien zum eHBA geben, so dass er in jedem Fall auch weiter als Authentifizierungsmittel verwendet werden wird. Für die QES ist kein alternatives Verfahren in Sicht ggf. ein von der gematik angebotener Fernsignaturdienst. Zudem ermöglicht die Komfortsignatur, bei dauerhaft gestecktem HBA, benutzerfreundliches Arbeiten. Es kann zusätzlich alternative, abgeleitete Identitäten auf dem Smartphone geben.

Kann ich mehrere eHBA beantragen?

Ja, dies unterstützen alle Anbieter und Kammern. In einem Antragsprozess sind derzeit 2 Ausweise möglich.

Benötige ich ein erneutes Ident, wenn mein eHBA ausläuft?

Ja, das betrifft sowohl die notwendige Beantragung eines Folgeausweises nach Ablauf der regulären Gültigkeit, als auch den Austausch wegen Algorithmenwechsels oder Auslaufen eines Zertifikats für die Kartenplattform.

Wird Video-Ident für die Identifikation im Ausgabeprozess des HBA verwendet?

Nein. Das Verfahren gilt als unsicher und ist schon länger für die Ausgabe von QES-Zertifikaten verboten. Auch die SMC-B-Ausgabe erfolgt ohne Video-Ident-Verfahren. Die DKTIG nutzt noch bis 30.09.2022 das Video-Ident-Verfahren, danach ausschließlich POSTIDENT und eID.

Welche ausländischen Ausweisdokumente werden beim POSTIDENT-Verfahren unterstützt?

Dazu gibt die POSTIDENT-Ausweisliste detailliert Auskunft.

Kann ich meine Signatur-PIN von zu Hause aus an eine Kartenterminal in meiner Praxis (remote) übertragen, in dem der eHBA steckt, um bspw. ein E-Rezept von zu Haus aus zu signieren?

Nein, das ist aus Sicherheitsgründen untersagt und wird von den zugelassenen Kartenterminals auch technisch unterbunden, obwohl es der eHBA selbst ermöglicht.

Was tun, wenn ich aus nicht selbstverschuldeten Gründen (bspw. Lieferschwierigkeiten der Anbieter) noch keine Folgekarte für meinen eHBA habe, der alte eHBA aber bereits abgelaufen ist?

Für diesen Fall sind die gängigen Ersatzverfahren zu verwenden, die auch bei technischen Problemen mit der Telematikinfrastruktur zum Einsatz kommen.

E-Rezept
Papierrezept: Verschreibungspflichtige Arzneimittel werden auf dem Vordruck Muster 16 verordnet („rosa Rezept“).

eAU
Signatur mittels SMC-B statt eHBA (vgl. § 2 Abs. 4 BMV-Ä Anlage 2b Vereinbarung über die

Verwendung digitaler Vordrucke in der vertragsärztlichen Versorgung.)

eArztbrief
Erstellung eines Arztbriefes in Papierform

ePA
Um auf die ePA zuzugreifen, ist der eHBA keine technische Voraussetzung. Ärztliche Praxen und Krankenhäuser müssen bzw. mussten aber nachweisen, dass sie über die für den Zugriff auf die ePA erforderlichen Komponenten verfügen.[12)] Dazu gehört auch der eHBA (für mindestens ein Ärztin oder einen Arzt) der Praxis. Dies ist in der Regel bereits erfolgt und ein kurzzeitig fehlender eHBA sollte keine negativen Auswirkungen auf den Praxisbetrieb haben. Rechtlich gilt allerdings weiter: Zugriff auf Daten der Anwendung nur, wenn der Zugreifende einen eHBA besitzt (§ 339 Abs. 3 SGB V) oder von einem anderen eHBA-Inhaber autorisiert ist (§ 339 Abs. 5 SGB V).

Sonstige

Signieren aus dem Home Office:
https://www.apotheke-adhoc.de/nachrichten/detail/e-health/ti-tablet-e-rezepte-zu-hause-signieren/#

Cherry hat ein PIN-Pad auf den Markt gebracht, mit dem man von zu Hause aus auf die Telematikinfrastruktur (TI) zugreifen kann. Das Gerät bietet laut Hersteller vielfältige Einsatzmöglichkeiten auch für Apothekerinnen und Apotheker:
https://www.apotheke-adhoc.de/nachrichten/detail/e-health/pin-pad-anwendungsfaelle-in-der-apotheke/

1)
Repository unter: https://www.d-trust.net/en/support/repository.
2)
„Repository“: https://www.medisign.de/support/zertifikate/zertifikatsrichtlinien/.
3)
Repository unter: https://telesec.de/de/service/downloads/pki-repository.
4)
Produktblatt u.a. Infos: https://www.d-trust.net/de/loesungen/ehba.
5)
Absprungseite: https://shc-care.de/kontakt-services/support/downloads/358.
6)
Pressemeldung der zuständigen Behörde:
https://www.elektronische-vertrauensdienste.de/EVD/DE/Aktuelles/Meldungen/anbieter/RSA2048.html.
7)
Bundesdruckerei:
https://www.d-trust.net/de/support/ehba#Austauschaktion%20eHBA%20Generation%20G2.0
medisign: https://www.medisign.de/blog/ehba-und-smc-b-der-generation-2-0-werden-ausgetauscht/ .
8)
Ach wenn die BNetzA als zuständige deutsche Regulierungsbehörde auf ihrer Webseite das Video-Ident als zulässig für die Beantragung qualifizierter Zertifikate ansieht, gilt dies nur für einmalig nutzbare Zertifikate (Ad-hoc-Zertifikate), die innerhalb 24 Stunden nach Ausstellung widerrufen werden. Zudem wird explizit ausgeschlossen solche Zertifikate für die Beantragung weiterer (bspw. länger laufender) Zertifikate oder andere Idents verwendet werden. (s. Nr. 10 b) bzw. 11 b) in den beiden Videoident-Verfügungen).
9)
Vereinbarung zwischen dem GKV-Spitzenverband (Spitzenverband Bund der Krankenkassen) und der Deutschen Krankenhausgesellschaft zur Finanzierung der bei den Krankenhäusern entstehenden

Ausstattungs- und Betriebskosten im Rahmen der Einführung und des Betriebs der Telematikinfrastruktur gem. § 291a Abs. 7a SGB V zum 1.1.2019
10)

gemSpec_Krypt, S. 9, Anforderung GS-A:3080
11)

gemSpec_Krypt, Kap. 2.1.1.1. Dies wird insbesondere genutzt, wenn bereits bekannt ist, dass kryptographische Algorithmen oder Zertifikate von Kartenplattformen auslaufen werden.
12)

§ 341 Abs. 6 bzw. 7 SGB V.