Telekom Security HBA

[HPC107] Informationen zum HBA

Deutsche Telekom Security GmbH
TC Solutions

öffentlich

Version:	02.00	Gültig ab:	01.07.2020
Status:	Freigegeben	Letztes Review:	01.07.2020

Mit Veröffentlichung dieses Dokumentes verlieren alle bisherigen Versionen ihre Gültigkeit!

Änderungen

Version	Stand	Bearbeiter	Änderungen / Kommentar
1.0	15.08.2018	SK	erste freigegebene Version
1.1	07.01.2019	AK	Entfall Verweis auf Nutzungsbedingungen
1.2	28.01.2020	AK	Anpassung Kapitel 4.2
1.2	03.02.2020	DD	Freigabe
1.3	29.06.2020	AK	Anpassungen aufgrund der Ausgründung der Telekom Security
1.4	01.07.2020	Telekom Security	Formale QS
02.00	01.07.2020	Telekom Security	Freigabe

Inhaltsverzeichnis

1 Vorwort

Sehr geehrte Kundin, sehr geehrter Kunde,

der elektronische Arzt-, Zahnarzt-, Psychotherapeuten- oder Apothekerausweis (auch genannt Heilberufsausweis (HBA)) ist ein personenbezogener Ausweis im Chipkartenformat, der an Heilberufler ausgegeben wird. Er beinhaltet neben seiner Funktion als Sichtausweis eine Reihe elektronischer Zertifikate zur Authentifizierung, Ver- und Entschlüsselung von Daten und zur Erstellung qualifizierter elektronischer Signaturen.

Er ermöglicht damit den Zugriff auf Daten der elektronischen Gesundheitskarte (eGK) (z.B. auf Notfalldaten) und im Rahmen von Anwendungen der Telematikinfrastruktur die sichere und rechtsverbindliche Kommunikation zwischen Leistungserbringern (KOM-LE).

Der Gesetzgeber hat mit entsprechenden Rechtsvorschriften die Möglichkeit geschaffen, als Äquivalent zur eigenhändigen Unterschrift die qualifizierte elektronische Signatur einzusetzen.

Strenge Prüfkriterien an Technik und Organisation schaffen ein hohes Sicherheitsniveau für die qualifizierte elektronische Signatur gemäß der EU-Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS).

Die vorliegenden Informationen sollen Ihnen den Einstieg in die Welt der elektronischen Signatur mit einem Heilberufsausweis (HBA) erleichtern.

Darüber hinaus sind in diesem Dokument in Kapitel 5 Hinweise zur Nutzung des HBA aufgeführt, die sich aufgrund der eIDAS-Verordnung ergeben.

Lesen Sie die Informationen und Hinweise vor der Antragsstellung bitte sorgfältig durch und wenden Sie sich bei Fragen an unsere Supportline.

Unsere Kontaktdaten für Ihre Fragen:

- Telefonisch: + 49 800 1183307 (kostenlose Servicenummer)
- Sperrhotline: 116 116*, International: +49 30 4050 4050
- Per E-Mail: service.map@telekom.de
- Per Brief: Deutsche Telekom Security GmbH
  Trust Center Services – HBA
  Postfach 12 51
  D-57236 Netphen

2 Informationen zur elektronischen Signatur

2.1 Was ist eine elektronische Signatur?

Die handschriftliche Unterschrift verbindet ein Papierdokument mit dem Unterzeichner. Der Unterzeichner schließt z.B. einen Vertrag durch Unterzeichnung mit seiner eigenhändigen Unterschrift. Ebenso verbindet die elektronische Signatur einen Unterzeichner mit elektronischen Daten z.B. einem Textdokument so, dass man diese Zuordnung sicher nachprüfen kann. Im Gegensatz zur handschriftlichen Unterschrift, für die der Unterzeichner „Papier und Stift“ benötigt, nutzt er bei der elektronischen Signatur mathematische Verfahren.

2.2 Wie funktioniert die elektronische Signatur?

Das Public-Key-Verfahren bildet in der Regel die Grundlage für die elektronische Signatur. Für das Verfahren benötigt man ein spezielles Schlüsselpaar. Daten, die mit dem einen Schlüssel verschlüsselt werden, können nur mit dem dazugehörigen anderen Schlüssel entschlüsselt werden. Diese Eigenschaft nutzt man für die Erstellung einer elektronischen Signatur und deren Überprüfung.

Bei der elektronischen Signatur erzeugt man zuerst einen digitalen Fingerabdruck des Dokuments. Der Fingerabdruck wird nun mit dem ersten Schlüssel verschlüsselt, das ist die elektronische Signatur. Das elektronisch signierte Dokument kann nun anderen Nutzern zugänglich gemacht werden. Der Unterzeichner stellt den zweiten Schlüssel nun den anderen Nutzern zur Prüfung der elektronischen Signatur zur Verfügung. Mit dem vorliegenden Schlüssel und dem Wissen, wem dieser Schlüssel zugeordnet ist, kann nun jeder eine sichere Überprüfung vornehmen. Man bezeichnet den ersten Schlüssel als Signaturschlüssel und den zweiten Schlüssel als Signaturprüfschlüssel.

2.3 Welche Rechtswirkung hat die elektronische Signatur?

Die qualifizierte elektronische Signatur ist der handschriftlichen Unterschrift in vielen Fällen gleichgestellt. Das bedeutet, dass in vielen Rechtsgeschäften der Einsatz der qualifizierten elektronischen Signatur neben der handschriftlichen Unterschrift möglich ist.

Ein Anwendungsbeispiel ist die qualifizierte elektronische Signatur eines Arztbriefes im Rahmen von KOM-LE. Mit dem HBA können aber auch rechtsverbindliche Signaturen in anderen Rechtsgeschäften geleistet werden. Informieren Sie sich bitte vorher, ob dies im jeweiligen Rechtsgeschäft zugelassen ist.

Durch die Nutzung Ihres Signaturschlüssels wird Ihnen die qualifizierte elektronische Signatur zugerechnet, d.h. Sie zeichnen verantwortlich wie bei einer handschriftlichen Unterschrift.

Die Ausgabe qualifizierter Zertifikate zur Erstellung qualifizierter elektronischer Signaturen geschieht auf Basis der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates („eIDAS“). In Deutschland gilt diese Verordnung unmittelbar und wird durch das Deutsche eIDAS-Durchführungsgesetz[1] (Vertrauensdienstegesetz, VDG) ergänzt. Im Vertragsverhältnis zwischen der Deutschen Telekom AG (vertreten durch Deutsche Telekom

[1] Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Security GmbH) als Vertrauensdiensteanbieter und dem Inhaber des HBA gilt deutsches Recht.

2.4 Wie wird das Schlüsselpaar einer Person zugeordnet?

Die Zuordnung von Person und Schlüssel wird durch ein qualifiziertes Zertifikat bestätigt, das auf dem HBA gespeichert ist. Ein Zertifikat ist eine Art elektronischer Ausweis. Die Identifikation der Person wird per PostIdent-Verfahren in Filialen der Deutschen Post oder bei einigen Kammern auch per KammerIdent-Verfahren durch Mitarbeiter der Kammern durchgeführt. Dabei muss die Person sich durch Personalausweis oder Reisepass ausweisen. Im Fall von KammerIdent ist auch der elektronische Aufenthaltstitel (EAT) als Ausweisdokument zugelassen.

2.5 Kann die qualifizierte elektronische Signatur eingeschränkt werden?

Es ist möglich, die qualifizierte elektronische Signatur durch Angaben im qualifizierten Zertifikat auf bestimmte Anwendungen in Art und Umfang zu beschränken.

Im Antragsformular können Sie Angaben zu einer monetären Einschränkung (z.B. 500 Euro) machen. Dies führt dazu, dass die monetäre Einschränkung im qualifizierten Zertifikat eingetragen wird, und nur Rechtsgeschäfte unter dem angegebenen Wert (z.B. 500 Euro) mit der qualifizierten elektronischen Signatur abgeschlossen werden dürfen.

Im Antragsformular können Sie Angaben zu weiteren Beschränkungen der qualifizierten elektronischen Signatur machen, die im qualifizierten Zertifikat eingetragen werden. Bitte beachten Sie, dass jegliche Beschränkungen nicht für die Anwendungen gemäß §291a SGB V gelten.

3 Informationen zum Herausgeber des HBA

3.1 Wer ist Herausgeber eines HBA?

Als Herausgeber für den HBA für Zahnärzte (auch als elektronischer Zahnarztausweis bezeichnet) fungiert die für den Zahnarzt zuständige Landeszahnärztekammer.

Als Herausgeber für den HBA für Ärzte (auch als elektronischer Arztausweis bezeichnet) fungiert die für den Arzt zuständige Landesärztekammer oder teilweise die Bezirksärztekammer.

Als Herausgeber für den HBA für Psychotherapeuten (auch als elektronischer Psychotherapeutenausweis bezeichnet) fungiert die für den Psychotherapeuten zuständige Landespsychotherapeutenkammer.

Als Herausgeber für den HBA für Apotheker (auch als Apothekerausweis bezeichnet) fungiert die für den Apotheker zuständige Landeskammer.

3.2 Welche Aufgaben hat der Herausgeber eines HBA?

Die Herausgeber des HBA geben in einer gemeinsamen Policy die Inhalte der Zertifikate und insbesondere die berufsbezogenen Attribute in den Zertifikaten des HBA vor.

Die Vorgaben der Herausgeber für das qualifizierte Zertifikat müssen immer im Einklang mit den gesetzlichen Vorgaben stehen.

Weiterhin fungieren die Herausgeber als sogenannte „Attribut-bestätigende Stellen“, die die Richtigkeit und korrekte Zuordnung der berufsbezogenen Attribute zur Person bestätigen. Erst nach erfolgter Bestätigung wird ein beantragter HBA produziert.

3.3 Welche berufsbezogenen Attribute sind in den Zertifikaten des HBA enthalten?

Die Zertifikate des HBA, insbesondere also auch das qualifizierte Zertifikat, enthalten den Namen des jeweiligen Herausgebers. Weiterhin enthalten sie

- beim elektronischen Arztausweis die Berufsbezeichnung „Ärztin/Arzt“,
- beim elektronischen Zahnarztausweis die Berufsbezeichnung „Zahnärztin/Zahnarzt“,
- beim elektronischen Psychotherapeutenausweis eine oder beide der Berufsbezeichnungen „Psychologische/-r Psychotherapeut/-in“, „Kinder- und Jugendlichenpsychotherapeut/-in“.
- beim elektronischen Apothekerausweis die Berufsbezeichnungen „Apotheker/-in“ oder eine andere der von der gematik festgelegten Berufsbezeichnungen (z.B. „Apothekerassistent/-in“)

Die Attribute sind fester unabänderlicher Bestandteil des qualifizierten Zertifikates und werden bei jedem Signiervorgang beigefügt.

3.4 Darf der Herausgeber eines HBA diesen sperren?

Da der Herausgeber als Attribut-bestätigende Stelle für die berufsbezogenen Attribute fungiert, hat er das Recht, ein Zertifikat zu sperren, z.B. wenn eine Approbation erlischt.

4 Informationen zum „Vertrauensdiensteanbieter“ (VDA)

4.1 Welche Aufgaben übernimmt ein VDA?

Der Vertrauensdiensteanbieter (auch Trust Center oder Trust Service Provider (TSP) genannt) stellt die benötigten Komponenten und Dienstleistungen für die qualifizierte elektronische Signatur zur Verfügung. Die Aufgaben werden nachfolgend beschrieben.

4.1.1 Prüfung der Antrags- und Identifizierungsdokumente des Kunden

Der VDA prüft nach Eingang der unterschriebenen Papieranträge die Anträge sowie das Identifikationsdokument.

4.1.2 Prüfung der Freigabedokumente der Kartenherausgeber

Der VDA prüft die qualifizierte elektronische Signatur des Freigabedokuments des Kartenherausgebers, mit dem die Antragsdaten und insbesondere die berufsbezogenen Attribute des Antragstellers bestätigt werden. Die qualifizierte elektronische Signatur des Freigabedokuments muss von einem berechtigten und registrierten Mitarbeiter des Kartenherausgebers stammen.

4.1.3 Produktion und Versand des HBA

Der VDA produziert den HBA in einer besonders gesicherten Umgebung. Alle kryptographischen Schlüssel des HBA werden in der Chipkarte generiert und nicht auslesbar gespeichert. Die Schlüssel können daher vom VDA weder gespeichert noch archiviert werden. Der HBA wird mit einer elektronischen Transportsicherung versehen und per sicherem Verfahren an den Antragsteller versendet. Die Produktion eines HBA inkl. des Versands erfolgt in der Regel spätestens innerhalb von 10 Arbeitstagen nach Freigabe durch den Kartenherausgeber.

Der Versand des PIN-/PUK-Briefes erfolgt zeitversetzt (mindestens drei Arbeitstage) mit separater Post.

4.1.4 Funktion zur Freischaltung des HBA

Der VDA stellt Ihnen eine Funktion zur Freischaltung Ihres HBA zur Verfügung. Mit der Freischaltung erklären Sie, dass Sie HBA und PIN-/PUK-Brief unversehrt erhalten haben. Die Freischaltung ist Voraussetzung zur Nutzung des HBA.

Gehen Sie dazu auf unser Portal: https://hba.telesec.de/tsp-applicant/

Wählen Sie den Menüpunkt „Karten verwalten“ und darin die Funktion „Erhaltene Karte freischalten“.

Hinweis: Hier benötigen Sie Ihre Kartennummer und das Freischaltepasswort, beides wurde Ihnen bei der Beantragung des HBA im Antragsdokument (PDF-Download) mitgeteilt.

4.1.5 Sperrung des HBA

Der VDA betreibt einen 24-Stunden-Sperrservice. Sie können die Sperrung Ihres HBA über verschiedene Wege veranlassen:

1) **Sperrung über das Antragsportal** https://hba.telesec.de/tsp-applicant/
Zur Sperrung über das Antragsportal benötigen Sie die **Referenznummer und das Sperrpasswort**, beides wurde Ihnen bei der Beantragung des HBA im Antragsdokument (PDF-Download) mitgeteilt.

2) **Sperrung durch die Sperrhotline**
Sollten Sie Ihre Zertifikate nicht über das Antragsportal sperren können, so können Sie die Sperrung auch durch die Sperrhotline des VDA unter der Tel-Nr. 116116 veranlassen. Zur Sperrung über die Sperrhotline benötigen Sie die **Referenznummer und das Sperrpasswort**, beides wurde Ihnen bei der Beantragung des HBA im Antragsdokument (PDF-Download) mitgeteilt.

3) **Schriftliche Sperrung per formlosem Schreiben an den VDA**
Sie können aber auch schriftlich eine Sperrung durchführen, dazu verwenden Sie bitte folgende Adresse:

Deutsche Telekom Security GmbH
Trust Center Services - HBA
Postfach 12 51
D-57236 Netphen

In diesem Fall ist die Angabe des Sperrkennworts nicht erforderlich. Diese Möglichkeit ist daher für den Fall gedacht, dass Sie Ihr Sperrkennwort nicht mehr kennen.

Die Sperrung eines HBA wird mit Angabe des Datums und der Zeit im Zertifikatsverzeichnis eingetragen. Eine rückwirkende Sperrung ist nicht möglich. Bitte beachten Sie, dass auch der Herausgeber zur Sperrung eines HBA berechtigt ist. Eine Sperrung kann nicht rückgängig gemacht werden.

4.1.6 Archivierung der Antragsunterlagen und Zertifikatshistorie

Die Antragsunterlagen sowie die Zertifikatshistorien mit den Protokollierungen aller relevanten Ereignisse werden gemäß den Anforderungen des Vertrauensdienstegesetzes (VDG) dauerhaft beim TSP aufbewahrt.

4.1.7 Betrieb von Verzeichnisdiensten

Die Zertifizierungsstelle stellt Online-Informationen zum Zertifikatsstatus 7x24 Stunden mit einer Verfügbarkeit von mindestens 99% monatlich via OCSP bereit.

4.2 Wer überwacht den Vertrauensdiensteanbieter?

Für die Ausgabe der qualifizierten Zertifikate gelten die Anforderungen der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates („eIDAS“, electronic IDentification, Authentication and Trust Services)

Zur Gewährleistung der eIDAS-Konformität des TSP X.509 QES HBA erfüllt der Zertifizierungsdienst die Anforderungen aus

- [ETSI EN 319 401]: General Policy Requirements for TSPs
- [ETSI EN 319 411-1]: General Policy and security requirements for TSPs
- [ETSI EN 319 411-2]: Requirements for TSPs issuing EU qualified certificates
- [ETSI EN 319 412-2]: Certificate profile for certificates issued to natural persons
- [ETSI EN 319 412-5]: Certificate Profiles: QCStatements

Die Erfüllung der o. g. Anforderungen zur Erlangung und zur Aufrechterhaltung des Status eines „Qualifizierten Vertrauensdiensteanbieters“ gemäß Art. 3 Nr. 20 eIDAS lässt der TSP mindestens jährlich eine Konformitätsbewertung durch eine akkreditierte Zertifizierungsstelle für Produkte, Prozesse und Dienstleistungen im Bereich „qualifizierte Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste im Anwendungsbereich der eIDAS“ vornehmen (gemäß ETSI EN 319403).

Die Überwachung der VDA ist der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) als zuständige Behörde übertragen.

Für die nonQES-Zertifikate des HBA gelten aufgrund der übergeordneten PKI außerdem folgende übergeordneten Policies:

- gematik: Certificate Policy, gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL [gemRL_TSL_SP_CP].
- [HBA] Bundesapothekerkammer, Bundesärztekammer, Bundespsychotherapeutenkammer, Bundeszahnärztekammer und Kassenzahnärztliche Bundesvereinigung: Gemeinsame Policy für die Ausgabe der HPC – Zertifikatsrichtlinie HPC [CP-HPC].

4.3 Informationsquellen

Bitte informieren Sie sich regelmäßig auf folgenden Websites:

- Informationen der Telekom Security zum HBA
  - Allgemeine Informationen: http://www.telesec.de
  - Online Antrag, Freischaltung und Sperrung: https://hba.telesec.de/tsp-applicant
- Informationen der zuständigen Aufsichtsbehörde: http://www.bundesnetzagentur.de
- Informationen der Bundeszahnärztekammer: http://www.bzaek.de
- Informationen der Bundesärztekammer: http://www.bundesaerztekammer.de
- Informationen der Bundespsychotherapeutenkammer: http://www.bptk.de

sowie auf der Website ihrer zuständigen Kammer.

5 Hinweise zur Nutzung des HBA

5.1 Anforderungen aufgrund der Multisignaturfähigkeit

Der Einsatz von Multisignaturkarten erfordert eine besondere Sicherheitsumgebung. Die Einsatzumgebung muss unter Berücksichtigung der vorliegenden Gegebenheiten und des geplanten Einsatzzweckes physisch und logisch so abgesichert werden, dass ein Missbrauch der Signaturfunktionalität und die Ausspähung der zugehörigen Signatur-PIN durch Angreifer mit hohem Angriffspotential praktisch ausgeschlossen sind und damit Ihre alleinige Kontrolle über den Prozess der Signaturerzeugung gegeben ist.

Zu den physischen Sicherungsmaßnahmen gehört der Schutz gegen unbefugten Zugriff auf die Karte, insbesondere bei einem unbeaufsichtigten Betrieb.

Zu den logischen Sicherungsmaßnahmen gehören die Sicherstellung, dass nur hinreichend geprüfte Produkte zur Signaturanwendung eingesetzt werden, sowie zusätzlich die folgenden Punkte:

- Ordnungsgemäße Installation des Produktes und Einhaltung der vorgesehenen Einsatzumgebung gemäß der Sicherheitshinweise aus den zugehörigen Handbüchern und den Bestätigungen,
- regelmäßige Überprüfung der Integrität des Produktes und der zugrunde liegenden Plattform (Hardware und Betriebssystem),
- Schutz der IT-Plattform vor Schadsoftware,
- vertrauenswürdige Sicherheitsadministration,
- vertrauenswürdige Netzinfrastruktur,
- vertrauenswürdige Anbindung an externe Kommunikationsnetze,
- Bei Nutzung der "entfernten PIN-Eingabe" muss sich der HBA in einem eHealth-Kartenterminal in einem gesicherten Bereich befinden und für die PIN-Eingabe ein eHealth-Kartenterminal genutzt werden, das unter Ihrer Kontrolle ist. Der gesicherte Bereich muss über hinreichend Schutz verfügen, um Ihre alleinige physische Kontrolle über den HBA zu gewährleisten. Insbesondere darf der HBA nicht entwendet werden können.

Auch bei dem Einsatz von Multisignaturkarten wird jede qualifizierte elektronische Signatur Ihnen zugerechnet.

5.2 Weitere Empfehlungen

- Nutzen Sie einen Kartenleser mit PIN-Pad.
- Halten Sie Ihren Computer immer auf dem aktuellen Sicherheitsstand.
- Nutzen Sie aktuelle Antiviren- und Firewallsoftware.
- Schützen Sie Ihren Computer durch Passwörter oder mittels Chipkarte vor unberechtigten Zugriff.
- Signieren Sie grundsätzlich nur Informationen, deren Inhalt Sie vorher geprüft haben.
- Bei Zweifel an der Erstellung einer qualifizierten elektronischen Signatur, prüfen Sie diese vor dem Versand selbst noch einmal nach.