Eviden Trustcenter

Trust Service Provider
für das deutsche Gesundheitswesen

PKI Disclosure Statements
HBA

Dokument-OID: 1.3.6.1.4.1.6189.4.2.7

Version	01.01.00
Stand	15.08.2025
Dokument	ETC_PDS_gematik_HBA
Status	Freigegeben
Vertraulichkeit	Öffentlich
Autor(en)	S. Moser
Eigentümer	R. Vennemann

1 PKI Disclosure Statements

1.1 Geltungsbereich

Dieses Dokument beinhaltet die PKI Disclosure Statements zur Ausstellung von X.509 und CV Zertifikaten für den Heilberufeausweis HBA.

Die Endbenutzerzertifikate werden für natürliche Personen auf qualifizierten elektronischen Signaturerstellungseinheiten gemäß Policy QCP-N bzw. QCP-N-QSCD gemäß [ETSI EN 319 411-2] ausgestellt.

1.2 Dokumentenname und Dokument-OID

Dokumentname:	PKI Disclosure Statements HBA Zertifikatsdienste des Eviden Trustcenter als TSP im Rahmen des deutschen Gesundheitswesens
Dokument-OID:	1.3.6.1.4.1.6189.4.2.7 PEN Eviden Germany GmbH - Trustcenter (1.3.6.1.4.1.6189).gematik(4).PDS(2). PDS HBA Eviden(7)

Dieses Dokument PKI Disclosure Statements ist ein Auszug aus:

- Certification Practice Statements HBA Zertifikatsdienstes
  des Eviden Trustcenter als TSP im Rahmen des deutschen Gesundheitswesens
  Dokument-OID: 1.3.6.1.4.1.6189.4.1.7

1.3 Kontaktadressen

Der folgende Ansprechweg besteht hinsichtlich dieser Richtlinie:

Postadresse:	Eviden Trustcenter Lohberg 10 49716 Meppen
E-Mail:	gesundheitskarte@atos.net

Weitere Informationen können von der angegebenen Web Seite geladen werden:

Web-Adresse TSP ETC:	https://pki.trustcenter-services.com

1.4 Anwender der ausgestellten Zertifikate

Der Anwender der HBA Karte und der darauf befindlichen Zertifikate ist eine natürliche Person (z. B. Arzt, Apotheker, Psychotherapeut, Zahnarzt), die einen HBA bei einem für ihn zuständigen Kartenherausgeber beantragt. Aufgrund der persönlichen Bindung ist der Anwender mit dem Antragsteller und dem Zertifikatsinhaber identisch.

1.5 Ausgestellte Zertifikate

Nicht-qualifizierte X.509 Zertifikate mit den zugehörigen privaten Schlüsseln können von Zertifikatinhabern für Anwendungen zur Authentisierung sowie zur Daten- bzw. Nachrichtenentschlüsselung genutzt werden. Weiterhin können Zertifikate mit dem beinhalteten öffentlichen Schlüssel zur Validierung von Authentisierungen sowie zur Daten- und Nachrichtenverschlüsselung genutzt werden. Ein Einsatz der Zertifikate ist im Rahmen der gematik Telematikinfrastruktur zugelassen.

Der Einsatz des qualifizierten X.509 Zertifikates für qualifizierte elektronische Signatur ist für QES Anwendungen zugelassen. Der Einsatz ist nicht auf die gematik Telematikinfrastruktur beschränkt.

CV Zertifikate mit den zugehörigen privaten Schlüsseln können für Gerät-zu-Gerät Authentisierungen im Rahmen der gematik Telematikinfrastruktur genutzt werden.

Tabelle 1 Verwendung der HBA Zertifikate und Schlüssel

Typ	Zertifikat	Nutzung
X.509	C.HP.AUT	Zertifikat und privater Schlüssel für die Signaturerstellung bzw. für Authentisierung des Karteninhabers. Nutzung nur nach Eingabe einer PIN.
	C.HP.ENC	Zertifikat und privater Schlüssel für die Ver-/Entschlüsselung von Daten durch den Karteninhaber. Nutzung nur nach Eingabe einer PIN.
	C.HP.QES	Zertifikat und privater Schlüssel für qualifizierte elektronische Signatur (QES). Nutzung nur nach Eingabe einer PIN.
CVC	C.HP.AUTR_CVC	Zertifikat und privater Schlüssel für die gesicherte Card-to-Card-Authentifizierung.
	C.HP.AUTD_SUK_CVC	Zertifikat und privater Schlüssel für die gesicherte Card-to-Card-Authentifizierung.
	PuK.CVC-RCA	Öffentlicher Schlüssel dieser CVC Root CA wird auf der HBA als Vertrauensanker für administrative Zwecke gespeichert.

Die Verwendung der Zertifikate für andere als die hier genannten Zwecke ist nicht erlaubt.

1.6 Vertrauenswürdigkeit ausgestellter Zertifikate

Die zu den qualifizierten Zertifikaten gehörenden Schlüssel werden auf qualifizierten sicheren Signaturerstellungseinheiten generiert, gespeichert und genutzt. Diese Chipkarten sind nach Common Criteria Prüfstärke EAL4+ geprüft und beim BSI als qualifizierte elektronische Signaturerstellungseinheiten (QSCD) gelistet.

1.7 Sperrung der Zertifikate

Die Zertifikate müssen durch den Anwender in folgenden Fällen gesperrt werden:

- bei Verlust, Defekt oder Diebstahl der HBA Karte,
- bei Verdacht der unbefugten Nutzung eines privaten Schlüssels der HBA Karte,
- bei wesentlichen Änderungen in den Zertifikatsinhalten (z.B. Namensänderung nach Heirat),
- wenn ein ausgestelltes Zertifikat falsche Angaben enthält,

Darüber hinaus werden die Zertifikate durch den Kartenherausgeber gesperrt,

- wenn der Zertifikatsinhaber nicht mehr in seinem Beruf arbeitet.

Oder durch den VDA

- wenn ein ausgestelltes Zertifikat falsche Angaben enthält,
- wenn ein begründeter Verdacht des Missbrauchs besteht,
- wenn VDA seine Tätigkeit einstellt,
- wenn die HBA Karte die Anforderungen der gematik bzw. eIDAS-VO nicht mehr erfüllt
- bei Kompromittierung des privaten Schlüssels der ausstellenden CA,
- wenn VDA aus sonstigen Gründen zum Widerruf gesetzlich verpflichtet ist.

Wird das Zertifikat nicht durch Anwender gesperrt, so wird dieser rechtzeitig per E-Mail über den Zeitpunkt und den Grund der Sperrung informiert.

Der Anwender hat zwei Möglichkeiten die Zertifikate zu sperren:

- elektronisch über den bei Antragstellung dem Anwender zugewiesenen Link
- telefonisch über die Hotline

Die Sperrung kann nur unter Angabe eines gültigen Sperrkennwortes erfolgen.

1.8 Pflichten der Zertifikatsinhaber

Der Zertifikatsinhaber ist vertraglich zur Einhaltung der nachfolgend aufgeführten Verpflichtungen verpflichtet. Das Akzeptieren der Vertragsbedingungen wird durch den Anbieter dokumentiert. Aufgrund der persönlichen Bindung sind beim Heilberufsausweis der Antragsteller, der Ausweisinhaber und der Zertifikatsinhaber identisch.

Die Verpflichtungen beinhalten insbesondere:

a) Der Antragsteller macht korrekte, wahrheitsgetreue und vollständige Angaben zu den benötigten Informationen. Dies gilt insbesondere für den Registrierungsprozess.

b) Der Ausweisinhaber ergreift die notwendigen Vorsichtsmaßnahmen, um einen unbefugten Einsatz seiner privaten Schlüssel zu verhindern. Nach Ablauf des Gültigkeitszeitraums oder nach Sperrung der HBA Karte darf er die privaten Schlüssel nicht mehr nutzen. Er muss den Heilberufsausweis sicher vernichten bzw. unbrauchbar machen, wenn die Karte nicht mehr genutzt wird (bspw. durch das physische Zerstören des Chips der HBA Karte).

c) Der Ausweisinhaber hat den zuständigen Kartenanbieter umgehend zu informieren, wenn

   - der Heilberufsausweis nicht mehr unter seiner alleinigen Kontrolle steht,
   - der begründete Verdacht auf eine Kompromittierung der beinhalteten Schlüssel besteht,
   - wesentliche Informationen im Zertifikat fehlerhaft sind oder sich geändert haben (bspw. Name, Berufsgruppenattribut).

d) Der Ausweisinhaber nutzt die ausgestellten Schlüssel bzw. Zertifikate nur für die jeweils vorgesehenen Anwendungsbereiche (siehe Kap. 1.5).

e) Der Anwender berücksichtigt die Anforderungen an die Einsatzumgebung, die der Kartenherausgeber bzw. der Kartenanbieter für den Einsatz der Zertifikate definiert.

1.9 Pflichten der Zertifikatsprüfer (Relying Parties)

Zertifikatsprüfer sind verpflichtet alle Zertifikate der Zertifikatskette gemäß ihrer Gültigkeitsmodelle zu prüfen. Die Gültigkeitsmodelle sind in Kapitel 2.4 der [gemKPT_PKI_TIP] definiert:

- TSP-X.509 nonQES: Schalenmodell,
- TSP-X.509 QES: Kettenmodell,

Die Validierung der Zertifikatskette muss die Prüfung des Sperrstatus der genutzten X.509 Zertifikate beinhalten. Es sollen die bereitgestellten Mechanismen genutzt werden:

- TSP-X.509 nonQES CA: gematik-TSL,
- TSP-X.509 QES CA-Zertifikate: BNetzA-VL,
- TSP-X.509 (nonQES und QES) CA- und EE-Zertifikate: OCSP-Responder bzw. bei Verfügbarkeit CRL.

Zertifikatsprüfer müssen die Beschränkungen für den Einsatz der kryptografischen Schlüssel beachten. Die Beschränkungen sind im Zertifikat in den Extensions "Key Usage" und sofern vorhanden "Extended Key Usage" definiert.

Zertifikatsprüfer sollen bei Verdacht auf oder festgestelltem Missbrauch von Zertifikaten den TSP darüber informieren. Dafür ist die Kontaktadresse in Kapitel 1.3 zu verwenden.

1.10 Haftung des Vertrauensdiensteanbieters

Der VDA ETC haftet nach den Vorgaben der gematik gemäß [gemRL_TSL_SP_CP] und [Eviden-Policy-CVC-ROOT]für ausgestellte nicht-qualifizierte X.509 und CV-Zertifikate.

Der VDA ETC haftet weiterhin nach den gesetzlichen Vorgaben gemäß Artikel 13 [eIDAS-VO] für ausgestellte qualifizierte X.509 Zertifikate.

Haftung besteht nur im Rahmen der gesetzlichen Vorgaben.

1.11 Richtlinien für die Zertifikatsdienste

Die Vorgaben zur Erstellung von Endbenutzer-Zertifikaten sind definiert in den Richtlinien Dokumenten:

Dokument	Referenz	URL
Policy der gematik-TSL	[gemRL_TSL_SP_CP]	https://gemspec.gematik.de/releases/
Policy der gematik CVC Root CA	[Eviden-Policy-CVC-ROOT]	
Spezifikation gematik PKI	[gemSpec_PKI]	
Policy der HBA Herausgeber	[CP-HPC]	**https://www.bundesaerztekammer.de/themen/aerzte/digitalisierung/elektronischer-heilberufsausweis-ehba/technische-spezifikationen**

1.12 Datenschutz

Der TSP Eviden Trustcenter hält die gesetzlichen Bestimmungen (siehe [DSG-VO], [BDSG2018]) zum Schutz der erhobenen personenbezogenen Daten ein. Der Umfang der zu erhebenden Daten ergibt sich aus den Vorgaben der gematik (siehe [gemSpec_PKI]) bzw. für QES aus den entsprechenden ETSI Normen ([ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2]).

Die Identifikationsdaten der Zertifikatsinhaber werden vertraulich behandelt. Die Zertifikatsinhaber werden über die Daten informiert, welche über sie erhoben, verarbeitet und gespeichert werden.

1.13 Kosten und Rückvergütungen

Keine Angaben.

1.14 Konfliktbeilegung

Es gilt grundsätzlich deutsches Recht, mit Ausnahme der [eIDAS-VO], welche als Europäischer Rechtsakt unmittelbare Wirkung entfaltet und Anwendungsvorrang vor den nationalen Regelungen genießt.

Für die Prüfung von Beschwerden und die Beilegung von Meinungsverschiedenheiten ist die Schiedsstelle des Eviden Trustcenters zuständig.

Die Schiedsstelle ist erreichbar unter:

Postadresse: Eviden Trustcenter
Lohberg 10
49716 Meppen

E-Mail: gesundheitskarte@atos.net

1.15 Konformität mit geltendem Recht

Der TSP Eviden Trustcenter ist bei der gematik registriert. Im Rahmen dieser Registrierung wurde das IT-Sicherheitskonzept sowie seine Umsetzung beim Betrieb durch einen von der gematik zugelassenen Gutachter überprüft und abgenommen. Eine erfolgreiche Prüfung ist die Voraussetzung für die Aufnahme bzw. den Verbleib des CA-Zertifikates der HBA-CA in die gematik-TSL.

Zusätzlich erfolgt eine Konformitätsprüfung nach [eIDAS-VO] durch eine von der BNetzA zugelassene Konformitätsbewertungsstelle. Eine erfolgreiche Prüfung ist die Voraussetzung für die Aufnahme bzw. den Verbleib des CA-Zertifikates der HBA-qCA in die BNetzA-VL.

Beide Prüfungen werden regelmäßig wiederholt bzw. können im Verdachtsfall durch die gematik bzw. die BNetzA angeordnet werden.

2 Verzeichnisse

2.1 Änderungsverzeichnis

Version	Datum	Änderung	Autor
01.00.00	22.04.2024	Erstellung dieses PDS durch Duplizieren des Atos HBA PDS 1.3.6.1.4.1.6189.4.2.3, Version 01.03.00 v. 28.08.2023 und Anpassung an die sich durch die Ausgliederung von Eviden Germany GmbH aus Atos Information Technology GmbH erforderlichen Änderungen	
01.01.00	15.08.2025	Abschnitt 1.11 – URL gematik aktualisiert; Abschnitt 2.3 - [CP-HPC] und [eIDAS-VO] aktualisiert	

2.2 Abkürzungen

ETC	Eviden Trustcenter
BDSG	Bundesdatenschutzgesetz
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statements
CRL	Certificate Revocation List (Sperrliste)
CVC	Card Verifiable Certificate
dGW	Deutsches Gesundheitswesen
EE	End Entity
eIDAS	Electronic Identification and Trust Services for Electronic Transactions in the European Market
eIDAS-VO	eIDAS-Verordnung
EN	European Norm
ETSI	European Telecommunications Standard Institute
EU	European Union
HBA	Heilberufeausweis
HPC	Health Profesional Card (Heilberufeausweis)
OCSP	Online Certificate Status Protocol
PEN	Private Enterprise Number
PKI	Public Key Infrastructure
QES	Qualifizierte elektronische Signatur
QSCD	Qualifizierte elektronische Signaturerstellungseinheit (Qualified Signature Creation Device)
TC	Trustcenter
TI	Telematikinfrastruktur

TSL	Trust-Service Status List
TSP	Trust Service Provider
URL	Unified Ressource Locator
VDA	Vertrauensdiensteanbieter
VO	Verordnung

2.3 Referenzen

[Eviden-Policy-CVC-ROOT]	Eviden: Übergeordnete Ausgabe-Policy für CV-Zertifikate (ECC)
[BDSG2018]	Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), am 25.05.2018 in Kraft getreten
[CP-HPC]	Gemeinsame Policy für die Ausgabe der Heilberufsausweise, Version: 2.4.0 vom 19.09.2024, gemeinsam herausgegeben von der Bundesapothekerkammer, der Bundesärztekammer, der Bundes-psychotherapeutenkammer, der Bundeszahnärztekammer, der gematik , der Bezirksregierung Münster und dem Deutschen Handwerkskammertag
[DSG-VO]	VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
[eIDAS-VO]	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 (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910), zuletzt geändert durch die Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401183&qid=1751875963046)
[ETSI EN 319 401]	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers; V2.3.1 (2021-05)
[ETSI EN 319 411-1]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements; V1.3.1 (2021-05-25)
[ETSI EN 319 411-2]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; V2.4.1 (2021-11)
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemRL_TSL_SP_CP]	gematik: Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_PKI]	gematik: Spezifikation PKI