Bundesärztekammer
Bundeszahnärztekammer

Trust Service Practice Statement

for the

Identity Verification Service

KammerIdent

Version: 1.3

Date: 19.10.2020

Content

Document status and approval			
Author, contact person			
	Dirk Schladweiler, consultant, Bundesärztekammer		
	Jochen Gottsmann, consultant, Bundeszahnärztekammer		
Approval	**Date**	**Name, department, company**	**Version** **Status**
TSPS	2020-10-19	Norbert Butz, Head of Department 5 - Digitization in Health Care, Bundesärztekammer	1.3 (2020-10-19) Approved
Sicherheitskonzept	2020-10-19	Norbert Butz, Head of Department 5 - Digitization in Health Care, Bundesärztekammer	2.7 (2020-01-31) Approved
Approval	**Date**	**Name, department, company**	**Version** **Status**
TSPS	2020-10-19	René Krouský, Deputy Chief Executive Officer and corporate attorney, Bundeszahnärztekammer	1.3 (2020-10-19) Approved
Sicherheitskonzept	2020-10-19	René Krouský, Deputy Chief Executive Officer and corporate attorney, Bundeszahnärztekammer	2.7 (2020-01-31) Approved

Version history				
Version	**Date**	**Author**	**Change**	**Remarks**
1.3	2020-10-19	Dirk Schladweiler	Table added to Document status and approval and version history Clarification in chapter 1.5 regarding risk, including risk assessment and residual risks in the security concept (Sicherheitskonzept) In chapter 1.5.4 designation of the authorizing authority for CPS and security concept, including risk management	

1 Introduction

This document is the Trust Service Practice Statement (TSPS) of the Bundesärztekammer and the Bundeszahnärztekammer for the KammerIdent identification service. It is structured according to RFC 3647 but is not a full Certification Practice Statement (CPS) because the processes of KammerIdent only cover the aspects of identity proofing for the issuance of qualified certificates and do not offer other certification services.

The purpose of this document is to serve as a base for compliance with eIDAS, the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and the ETSI standards ETSI EN 319 401, ETSI EN 319 411-1, and ETSI EN 319 411-2.

The Bundesärztekammer (German Medical Association) and the Bundeszahnärztekammer (German Dental Association) are coordinating as workgroups of the *Landesärztekammern (*State Chambers of Physicians) and the (Landes-)Zahnärztekammern, (German federal states' dental chambers) the issuing of electronic Health Professional Cards (Heilberufsausweise) for physicians and dentists which can be used for applications supporting electronic data transmission and which can also be used for qualified electronic signatures according to eIDAS.

The Health Professional Cards are issued by the State Chambers of Physicians and Dental Chambers; the qualified certificates can be obtained by physicians and dentist from their preferred certification service providers.

1.1 Overview

The issuance of qualified certificates requires a reliable process for the identification of applicants. The identification must be compliant with the requirements of eIDAS. The identity verification process must be defined in the security concept of the certification service providers.

According to eIDAS, Article 24,1, Certification Service Providers[1] may delegate tasks to third parties. The chambers are then considered as third parties commissioned by the Certification Service Providers (CSPs) to perform identity verification through the KammerIdent identity verification process. CSPs may also use other procedures for identity proofing, e.g. *POSTIDENT*®, or other procedures defined in the CSP's security concept.

KammerIdent is performed in chambers of physicians and dentists.

In individual cases the KammerIdent identity verification may be performed outside the chambers, e.g. during conferences or conventions or in the customer's rooms, provided that the respective locality permits an appropriate protection of privacy during the identification process (mobile KammerIdent).

In addition to performing identity verification the KammerIdent process also permits receiving application documents from applicants and forwarding them to the CSPs. This does not

[1] Note: throughout this document the term CSP (Certification Service Provider) is used instead of the term TSP (Trust Service Provider) as defined in eIDAS. The reason is that KammerIdent serves as a base for issuing qualified certificates (which is a certification service) and not as a base for other trust services (like the provision of time stamps or validation services).

include any checks of those documents. Verification of additional documents must be performed by the CSPs.

The chambers also confirm the membership in occupational groups, e.g. they confirm that a person is a physician. This kind of confirmation does not underlie the eIDAS-regulation. Therefore, confirmations of membership in occupational groups are not covered in this TSPS.

1.2 Document Name and Identification

This document is the “Trust Services Practice Statement of Bundesärztekammer and Bundeszahnärztekammer for the identification procedures KammerIdent”

Version: 1.3

Date: 19.10.2020

This document comes into effect when it is published.

It is going out of force when it is replaced by an amended version.

1.3 PKI Participants

No stipulation. KammerIdent realizes only identity verification.

1.4 Certificate Usage

No stipulation. KammerIdent realizes only identity verification.

1.5 Policy Administration

The organizations administering this document conduct a review of practices at least once a year, including responsibilities for maintaining the TSP's Declaration of Practice and the information security policy 'Sicherheitskonzept', including risk assessment and residual risks.

1.5.1 Organization administering the document

This TSPS is jointly administered by:

- Bundesärztekammer, Dezernat 5 Telemedizin und Telematik
- Bundeszahnärztekammer, Projektleitung eZahnarztausweis

1.5.2 Contact Person

Bundesärztekammer
Dezernat 5 – Digitalisierung in der Gesundheitsversorgung
Herbert-Lewin-Platz 1
10623 Berlin

Bundeszahnärztekammer
Projektleitung eZahnarztausweis
Chausseestr. 13
10115 Berlin

1.5.3 Person determining TSPS suitability for the policy

The suitability of the TSPS is determined jointly by Bundesärztekammer and Bundeszahnärztekammer.

1.5.4 TSPS approval procedures

The TSPS is approved by Bundesärztekammer and Bundeszahnärztekammer.

For the Bundesärztekammer, the Head of Department 5 - Digitization in Health Care is responsible for the approval.

For the Bundeszahnärztekammer, the Deputy Chief Executive Officer and corporate attorney is responsible for the approval.

Same rule applies for approval of risk assessment (with residual risks) and information security policy, both included in the document “Sicherheitskonzept”.

1.6 Definitions and Acronyms

1.6.1 Definitions

Applicant	A natural person that applies for (or seeks renewal of) a (qualified) Certificate.
Certificate	Certificate for electronic signature is an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person
Certificate Revocation List (CRL)	A list with certificates that have been revoked in order to make them invalid.
Certification Authority (CA)	A public agency or institution or natural or legal person authorized to provide electronic certification, time-stamping and electronic signature services.
Certification Practice Statement (CPS)	A CPS is a statement of the practices which a certification authority employs in issuing certificates. In general, CPSs also describe practices relating to all certificate lifecycle services (e.g., issuance, management, revocation, and renewal or re-keying), and CPSs provide details concerning other business, legal, and technical matters.
Certification Service Provider	A Trust Service Provider offering certification services, e.g. issuance, management, revocation, renewal, status service for certificates.
European Telecommunications Standards Institute	An independent, non-profit standardization organization in the telecommunications industry (equipment makers and network operators) in Europe. ETSI produces globally-applicable standards for Information and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technology.
Issuing CA	A unit in a CA’s structure which issues electronic certificates in response to RA-approved certificate requests. It also executes certificate revocations, generates, operates and publishes

	certificate revocation lists and/or OCSP status services.
Online Certificate Status Protocol (OCSP)	The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the validity status of electronic certificates.
Qualified Certificate	A Qualified Certificate for electronic signature is certificate for electronic signatures which is issued by a qualified trust service provider and meets the requirements laid down in Annex I of eIDAS.
Registration Authority (RA)	A Registration Authority (RA) is responsible for processing certificate requests received from applicants. The RA checks requests for validity and compliance with the CPS and relevant certificate policies and authenticates the identity of the applicant. The RA forwards the request to the CA to sign and issue a certificate to the applicant.
Relying Party	A natural or legal person that relies upon an electronic identification or a trust service
Trust Service	According to eIDAS a Trust Service is an electronic service which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services.
Trust Service Provider	A Trust Service Provider is a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider. A CA is an example of a Trust Service Provider.
Trust Service Practice Statement (TSPS)	A TSPS is a statement of the practices which a Trust Service Provider exercises for providing the Trust Services. In general, TSPSs describe practices relating to all certificate lifecycle services (e.g., issuance, management, revocation, and renewal or re-keying). If a TSP only covers some aspects of certificate issuing processes a TSPS only addresses the services provided.

1.6.2 Acronyms

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List

CSP	Certification Service Provider
eIDAS	Regulation on electronic identification and trust services; In detail: REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
ETSI	European Telecommunications Standards Institute
OCSP	Online Certificate Status Protocol
RA	Registration Authority
TSP	Trust Service Provider

2 Publication and Repository Responsibilities

2.1.1 Repositories

No stipulation. KammerIdent realizes only identity verification.

2.1.2 Publication of certificate information

No stipulation. KammerIdent realizes only identity verification.

2.1.3 Time or frequency of publication

The latest version of this TSPS is available for download on the websites of Bundesärztekammer and Bundeszahnärztekammer. Previous versions of the TSPS will be held available on these sites as well.

BÄK: http://www.e-arztausweis.de/policies/tsps_policy.html

BZÄK: http://policies.bzaek.de.

New versions will be published whenever relevant modifications have been made.

The websites of the chambers are publically available 24 hours a day, 7 days per week. Upon system failure or other kinds of outages, the chambers will restore proper functionality without delay.

3 Identification and Authentication

3.1 Naming

No stipulation. KammerIdent realizes only identity verification.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

No stipulation. KammerIdent realizes only identity verification.

3.2.2 Authentication of organization entity

No stipulation, KammerIdent realizes only identity verification for natural persons. KammerIdent does not authenticate organizations.

3.2.3 Authentication of individual identity

The identity of the applicant is checked against an official, government-issued photo ID document.
According to eIDAS Article 24 the attributes of the natural person to whom the qualified certificate is to be issued are verified directly by the physical presence of the natural person.

All identification datas - like first and last name, date and place of birth, address (if available on the ID document), number of the ID document - is filled into an identification form which is then forwarded to the CSP issuing the qualified certificate. The amount of this data from the ID document compares with the data in the system of the Chamber ensures that the applicant is unique.

The Chamber confirms affiliation to the relevant professional group and releases the production.

3.3 Identification and Authentication for Re-key Requests

No stipulation. KammerIdent realizes only identity verification.

Re-key requests are handled by the CSP.

3.4 Identification and Authentication for Revocation Requests

No stipulation. KammerIdent realizes only identity verification.

Revocation requests are handled by the CSP.

4 Certificate Life-Cycle Operational Requirements

No stipulation. KammerIdent realizes only identity verification.

The operational requirements regarding processing of certificate applications, certificate issuance, certificate validation though CRL or OCSP services, and certificate revocation are managed by the CSP.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

Identification with KammerIdent takes place in a room in a chamber. If the applicant has not filled out the application documents in advance a workstation can be used to fill out and print the KammerIdent identification forms. Since this workstation neither has access to the CSP's network nor permanently stores the applicant's data the workstation is protected according to

the chamber's standard protection mechanisms. The availability of such a workstation is optional; it is not a warranted service.

Completed paper forms with application and identification data are stored in a locked cabinet. Only KammerIdent officers have access to the cabinet.

The premises of the chambers are locked outside of business-hours.

5.2 Procedural Controls

The paper-based identification protocols of the KammerIdent process are collected by the KammerIdent officers and sent to the CSP enclosed in envelopes by regular mail. It is permitted to include additional documents related with the application for a qualified certificate.

Lists with all authorized KammerIdent officers including their signature specimens are handed out to all CSPs making use of KammerIdent. It is the CSP's responsibility to accept only those identification forms which are signed by one of the KammerIdent officers.

5.3 Personnel Controls

The chambers have employed staff with the necessary expertise, reliability, experience, and qualifications.

All KammerIdent officers receive at least every 12 months regular training regarding security and data protection regulations.

Appropriate disciplinary sanctions will be applied to personnel violating the KammerIdent policies or procedures.

The responsible person – like a security officer – for the local KammerIdent service is named by management and assigned the role of "Leiter Identifizierung" (Director of Identificaton). This role has the overall responsibility for administering the implementation of the security practices. The CSPs are informed about this assignment through an official letter.

All KammerIdent officers are formally appointed to their roles by the "Leiter Identifizierung" and are clearly identified. The persons providing the services are assigned the corresponding trusted roles "Identifizierungsmitarbeiter", "Bestätigungsmitarbeiter" and "Sperrmitarbeiter". Only Persons with this named roles managing the information and fulfil services. The overall role assignment shows the contact details of the person, the date of the current police clearance certificate, the date of the initial training and the date of the current training. The CSPs are informed about this assignment through an official letter.

Managerial personnel possess professional experience with the services provided and are familiar with security procedures for personnel with security responsibilities.

KammerIdent officers are held free from conflicts of interest that might prejudice the impartiality of operations.

5.4 Audit Logging Procedures

KammerIdent does not process electronic data; there is no electronic audit logging.

KammerIdent is a manual, paper-based service for identity validation.

For all identity verifications carried out the chambers retain a copy of the KammerIdent identification form to support internal revision processes. The copy of the KammerIdent identification is indefinitely archived in the person's file.

Because there is no electronic data processing stipulations related to

- types of events logged,
- frequency of processing log,
- retention period for audit log,
- protection of audit log,
- audit log backup procedures,
- audit collection system, and
- notification to event-causing subject

are not required.

A vulnerability assessment has been performed. It covers personal, organizational, technical, and other vulnerabilities.

5.5 Records Archival

No stipulation.

All records collected during the KammerIdent identity verification process are sent to the CSP. The CSP is responsible for archival.

5.6 Key Changeover

No stipulation.

There are no cryptographic keys involved in the KammerIdent identity verification process.

5.7 Compromise and Disaster Recovery

No stipulation.

KammerIdent is a manual, paper-based identification process. There are no requirements on availability. Temporary non-availability is tolerated.

5.8 CA or RA Termination

In case of termination of services the management responsible for KammerIdent will inform the relevant supervisory authority and other cooperating partners, especially the CSPs using KammerIdent for identity verification, as early as possible about this fact.

All documents collected in the identification of the applicants and clearly attributable to a CSP will be forwarded to the appropriate CSP immediately upon completion of the identification. There are no remaining identification documents in the chambers where KammerIdent is performed.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

No stipulation.

There are no cryptographic keys involved in the KammerIdent identity verification process.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

No stipulation.

There are no cryptographic keys involved in the KammerIdent identity verification process.

6.3 Other Aspects of Key Pair Management

No stipulation.

There are no cryptographic keys involved in the KammerIdent identity verification process.

6.4 Activation Data

No stipulation.

There are no cryptographic keys involved in the KammerIdent identity verification process.

Activation data for end-user qualified certificates are handled by the CSPs.

6.5 Computer Security Controls

Typically, applicants print and fill out their application forms and KammerIdent forms at home. Optionally, the KammeIdent officer may support the applicant if an applicant has not prepared the application form at home. For this purpose some KammerIdent officers have a standard personal computer available in their office. The only function of this computer in the KammerIdent process is to fill out and print the KammerIdent form.

The computer is not connected to the certification service provider's systems and it does not permanently store applicant's personal data or other sensible data.

The computer is secured according to the standard guidelines applicable for the chamber where the computer is located.

Access to the computer is only possible for authorized employees of the chamber after successful authentication.

6.6 Life Cycle Security Controls

No stipulation.

Except for the personal computer for printing KammerIdent forms there are no technical systems used for KammerIdent.

In particular, there is no system development and no system life-cycle that needs to be managed or controlled.

6.7 Network Security Controls

No stipulation. KammerIdent does not require network access.

6.8 Timestamping

No stipulation. In the KammerIdent process no timestamps are issued nor elsewhere used.

7 Certificate, CRL, and OCSP Profiles

No stipulation.

KammerIdent only offers identification services and does not issue certificates or provide CRL or OCSP services.

8 Compliance Audit and Other Assessment

8.1 Frequency of compliance audit

The KammerIdent process is audited according to eIDAS, article 20, at least every 24 months by an independent conformity assessment body.

8.2 Identity/qualifications of auditor

Auditors fulfil the requirements of ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

8.3 Auditor's relationship to audited party

The conformity assessment body and its auditors are independent from the organizations performing KammerIdent. The conformity assessment body is accredited in accordance with point 13 of Article 2 of Regulation (EC) No 765/2008 to perform such audits and certifications.

8.4 Topics covered by audit

The auditors choose the control objectives to be covered in the assessment in accordance with eIDAS requirements and ETSI requirements.

8.5 Actions taken as a result of deficiency

Deficiencies will be remedied by the applicable chamber.

8.6 Communication of results

No stipulation.

9 Other Business and Legal Matters

9.1 Fees

No stipulation.

9.2 Financial Responsibility

According to eIDAS, article 13, the Trust Service Providers are liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations of eIDAS. The chambers have contractual agreements with the Trust Service Providers for the provision of identity verification using KammerIdent. Liability of the chambers is regulated in these contracts.

9.3 Confidentiality of Business Information

Except for data to be included in the qualified certificates and data which is publicly available all information and data collected during the KammerIdent process is considered confidential.

9.4 Privacy of Personal Information

In the KammerIdent process only data related to the issuance of qualified certificates is collected. Except from printing the KammerIdent form personal data is not processed.

All personnel involved in KammerIdent have responsibility for protecting confidential information from misuse.

Personal data is collected only directly from the applicant and only up to the amount required by legislation for the issuance of qualified certificates.

Personal data from the identity verification is transmitted only to the applicable certification service provider; it is not disclosed to other entities.

9.5 Intellectual Property Rights

No stipulation

9.6 Representations and Warranties

The operators of KammerIdent represent and warrant that all identity validation steps defined in this TSPS are performed accurately and reliably.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

The certification service providers have the overall responsibility for all processes used for the issuance of qualified certificates. They are responsible for all questions regarding the liability for qualified certificates.

Regulations regarding the liability for the identity verification process KammerIdent are laid down in contracts between the certification service providers and the operators of KammerIdent.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term of TSPS

This TSPS becomes effective when it is published on the website defined in chapter 2.1.3. Amendments become effective upon publication.

9.10.2 Termination of TSPS

This TSPS remains in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

All stipulations regarding the privacy of personal or other data remain effective after termination of this TSPS and the KammerIdent service.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

Amendments to this TSPS must be approved by the entity named in 1.5.4.

9.13 Dispute Resolution Procedures

KammerIdent only provides identity verification services in order to support the registration authorities of the CAs that issue the certificates. The chambers performing KammerIdent have no contractual agreements with end-users or relying parties.

For disputes with end-users and relying parties the dispute resolution procedures of the issuing CAs apply.

9.14 Governing Law

The laws of the Federal Republic of Germany apply.

9.15 Compliance with Applicable Law

The KammerIdent service complies with German Law. In addition, the identification services realized by KammerIdent are compliant with eIDAS and fulfill all requirements on identity verification defined in eIDAS.

9.16 Miscellaneous Provisions

No stipulation.

9.17 Other Provisions

No stipulation.