Trust Service Practice Statement (TSPS) der DAkkS

Prüfpolicy für Attributsbestätigungen in Siegelzertifikaten mit digitalem Akkreditierungssymbol und Hoheitszeichen

Version 1.1

01.09.2023

Susanne Kuch; Prof. Dr. Raoul Kirmes ©

1 Prüfpolicy DAkkS-Siegelzertifikate

1.1 Zweck des Trust Service Practice Statement – TSPS

Zweck dieses *Trust Service Practice Statement (TSPS*) ist es die Kriterien des Zugangs, der Beantragung, Sperrung und Verifikation von Siegelzertifikaten die dem DAkkS-Zertifikatsprofil entsprechen und die Ermittlung des Akkreditierungsstatus durch Verifikation der Zertifikate darzulegen. Die –DAkkS-TSPS ergänzt die zertifikatsprofilspezifischen Aspekte der Dokumentation des Vertrauensdienstes der die PKI betreibt. Nähere Angaben zur Hierarchie der Dokumente in der PKI werden in Kapitel 4 dargelegt.

1.2 Impressum

Herausgeber Deutsche Akkreditierungsstelle © 2023

Am Spittelmarkt 10, 10117 Berlin

Kurzbezeichnung DAkkS

1.3 Dokumentenidentifikation

Dokumententyp	Trust Service Practice Statement (TSPS)
Name dieses Dokuments	Trust Service Practice Statement (TSPS) der DAkkS
Untertitel:	Prüfpolicy für Attributsbestätigungen in Siegelzertifikaten mit digitalem Akkreditierungssymbol und Hoheitszeichen
Anwendungsbereich	Fortgeschrittene Siegel auf Basis von qualifizierten Zertifikaten (X.509 Zertifikate), die ein digitales, maschinenlesbares Hoheitszeichen der Akkreditierung des Zertifikatsinhabers enthalten und die zur Nutzung auf Ergebnisberichten und Bestätigungen bestimmt sind.
Kurzname dieses Dokuments	DAkkS-TSPS
Referenz für dieses Dokument	[DAKKS_TSPS]
Version	1.1 vom 01.09.2023
Object Identifier (OID)	1.3.6.1.4.1.59749.2.1 {= DAkkS TSPS}

1.4 Struktur des Dokuments

Die Struktur dieses Dokumentes ist an den Aufbau des Internet-Standard RFC 3647 „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework“ angelehnt, um eine einfache Lesbarkeit und Vergleichbarkeit mit anderen TSPS und CPs zu erreichen. Aufgrund der Besonderheiten des DAkkS-Zertifikatsprofils sind Abweichungen erforderlich. Zudem werden nicht alle Aspekte des RFC 3647 angesprochen. Aspekte des RFC 3647 die nicht in der DAkkS-TSPS

dokumentiert sind, werden in der Dokumentation des Vertrauensdienstes, der die PKI betreibt, dargelegt. Nähere Angaben zur Hierarchie der Dokumente in der PKI werden in Kapitel 4 dargelegt.

1.5 Versionshistorie

Version	Datum	Änderung	Editor
0.1	28.01.2023	Initiale Version	KIR/SKU
1.0	31.03.2023	Veröffentlichte Version	KIR/SKU
1.1	**01.09.2023**	**Veröffentlichte Version** ▪ Editorische Anpassungen ▪ Anpassung von 2.1.4 auch auf juristische Personen	KIR/SKU

Die aktuell gültige, veröffentlichte Version ist **fett** markiert.

Inhalt

2 Überblick

2.1 Rollen und Instrumente der Akkreditierungsinfrastruktur

2.1.1 National Accreditation Body (NAB)

Der National Accreditation Body (NAB) ist eine befugte Stelle (authoritative body) im Sinne von Tz. 4.7 der ISO/IEC 17000, die vom WTO-Mitgliedsstaat in dem sie ihren Sitz hat beauftragt worden ist, Akkreditierungen im Sinne von Tz. 7.7 der ISO/IEC 17000 durchzuführen.

2.1.2 DAkkS = National accreditation body of the Federal Republic of Germany

Die Deutsche Akkreditierungsstelle ist gemäß § 1 AkkStelleG, § 1 AkkStelleGBV i.V.m VO (EG) 765/2008 die in Deutschland zuständige Behörde für die Akkreditierung von Konformitätsbewertungsstellen.

2.1.3 Konformitätsbewertungsstelle /Conformity assessment body (CAB)

Eine Konformitätsbewertungsstelle ist eine juristische Person im Sinne von Tz. 4.6 der ISO/IEC 17000, die Konformitätsbewertungstätigkeiten im Sinne von Tz. 4.3 bis 4.5 der ISO/IEC 17000 durchführt, jedoch keine Akkreditierung.

2.1.4 Kunde der Konformitätsbewertungsstelle (Customer)

Ein Kunde einer Konformitätsbewertungsstelle ist eine natürliche oder juristische Person, die Gegenstand der Konformitätsbewertung ist oder die den Gegenstand der Konformitätsbewertung im Sinne von Tz. 4.2 der ISO/IEC 17000 bereitstellt und Interesse am Ergebnis der Aussage hat.

2.1.5 Bestätigung (Attestation)

Eine Aussage einer Konformitätsbewertungsstelle (CAB) im Sinne von Tz. 7.3 der ISO/IEC 17000 ist, dass der Gegenstand einer Konformitätsbewertung im Sinne von Tz. 4.2 der ISO/IEC 17000 bestimmte festgelegte Anforderungen oder Erwartungen im Sinne von Tz. 5.1 der ISO/IEC 17000 erfüllt.

2.1.6 Elektronische Bestätigung (eAttestation)

Eine elektronische Bestätigung ist eine elektronisch bereitgestellte Aussage einer Konformitätsbewertungsstelle (CAB) im Sinne von Tz. 7.3 der ISO/IEC 17000, z.B. als PDF-Dokument oder als maschinenlesbares Format wie z.B. XML. Werden Konformitätserklärungen digital bereitgestellt (eAttestation), muss die Konformitätsbewertungsstelle die Integrität und Authentizität der elektronischen Bestätigung gewährleisten können. Dies erfolgt durch fortgeschrittene digitale Siegel auf Basis qualifizierter Zertifikate, die dem DAkkS-Zertifikatsprofil entsprechen.

2.1.7 Akkreditierungssymbol und Hoheitszeichen (accreditation symbol/ national emblem)

Ein Akkreditierungssymbol im Sinne von Tz. 3.12 der ISO/IEC 17011 wird durch eine Akkreditierungsstelle (NAB) vergeben und durch akkreditierte Konformitätsbewertungsstellen (CAB) auf den Bestätigungen und elektronischen Bestätigungen verwendet, um die Akkreditierung der ausstellenden CAB anzuzeigen. Wenn die Akkreditierungsstelle (NAB) hoheitlich arbeitet, wie alle nationalen Akkreditierungsstellen im Sinne von Art. 2 Nr. 11 VO (EG) 765/2008 in der europäischen Union und im EWR, kann das Symbol mit einem staatlichen Hoheitszeichen verbunden sein oder dieses repräsentieren.

2.1.8 Digitales Akkreditierungssymbol/ Hoheitszeichen

Wird ein digitales Akkreditierungssymbol mit oder ohne Hoheitszeichen im Sinne von Tz. 3.12 der ISO/IEC 17011 den akkreditierten Konformitätsbewertungsstellen elektronisch bereitgestellt, muss die Akkreditierungsstelle gemäß Tz. 4.3.3. lit. a und c) sowie Tz. 4.3.5 ISO/IEC 17011 die Integrität und Authentizität des Akkreditierungssymbols mit oder ohne Hoheitszeichen gewährleisten können, denn mit dem Symbol ist die Vermutungswirkung nach Art. 11 Abs. 2 VO (EG) 765/2008 verbunden. Dies erfolgt durch kryptographische Verfahren zum Schutz der Zertifikate unter der Verantwortung eines qualifizierten Vertrauensdienstes wie Kap. 2.3.1 dargelegt.

2.2 Übersicht zur Architektur für eAttestation

Die Kunden einer akkreditierten Konformitätsbewertungsstelle (**CAB**) sind die Nutzer der Konformitätserklärungen (**Attestation**), die mit dem Akkreditierungssymbol gekennzeichnet sind, denn Konformitätserklärungen akkreditierter Konformitätsbewertungsstellen werden gemäß des Art. 11 Abs. 2, 2. Alternative VO (EG) 765/2008 im europäischen Binnenmarkt sowie im EWR gegenseitig anerkannt. Auch auf Grundlage vorhandener Gegenseitigkeitsabkommen des TBT-Abkommens der WTO kann eine gegenseitige Anerkennung auch international über das Akkreditierungssymbol genutzt werden.

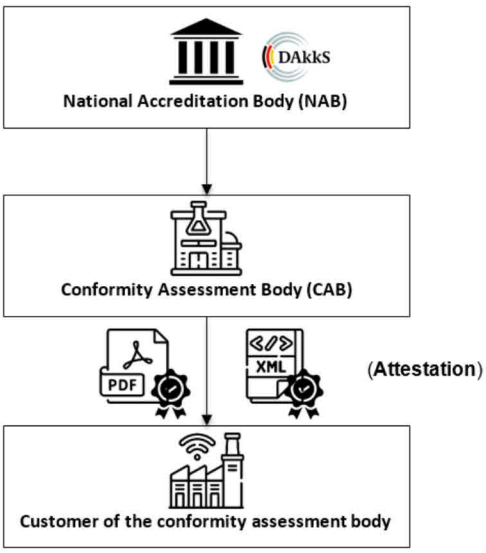


Abbildung 1: Rollen im Bereich der Akkreditierung - eigene Darstellung DAkkS

Die akkreditierten Konformitätsbewertungsstellen führen Konformitätsbewertungstätigkeiten durch, für die sie Bestätigungen (**Attestation**) im Hinblick auf einen Gegenstand der Konformitätsbewertung erteilen.

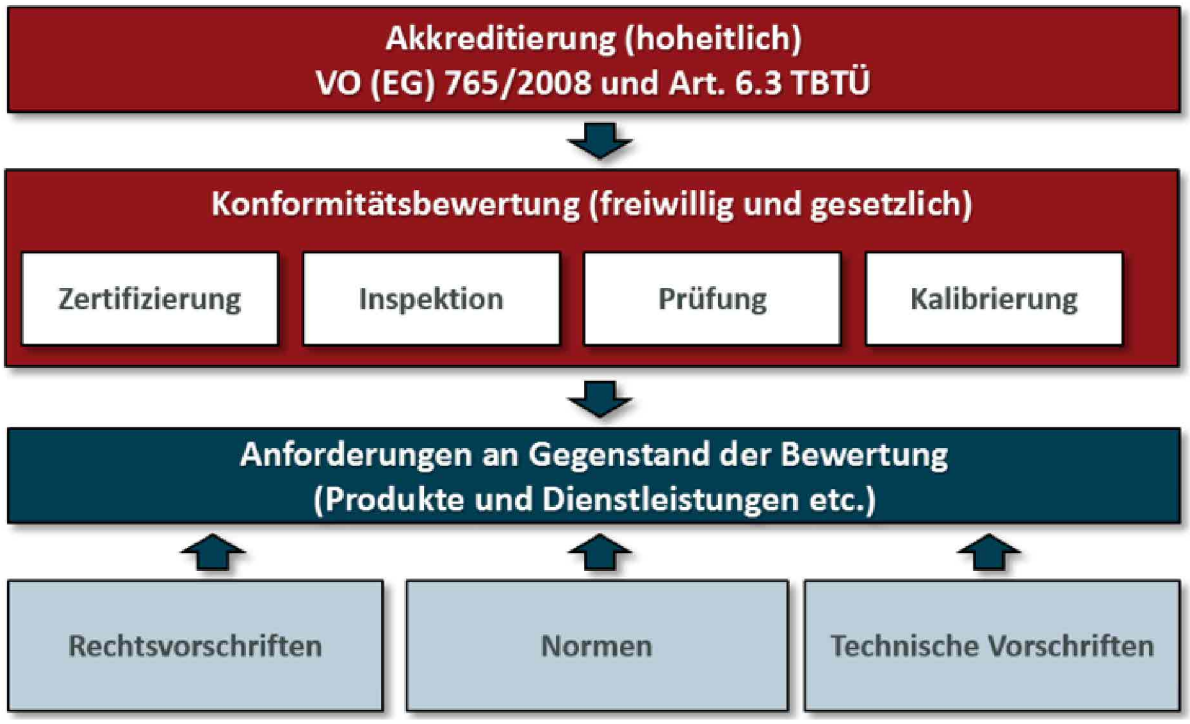


Abbildung 2: Kontext der Akkreditierung - eigene Darstellung DAkkS

Die Digitalisierung der internationalen Qualitätsinfrastruktur erfordert es, dass Konformitätsbewertungsstellen ihre Bestätigungen elektronisch bereitstellen können z.B. als PDF-Dokument oder als maschinenlesbares Format wie z.B. XML. Zur Gewährleistung der oben genannten Anforderungen unterstützt die DAkkS als nationale Akkreditierungsstelle, die Bereitstellung einer Public-Key-Infrastruktur (**PKI**) durch einen qualifizierten Vertrauensdiensteanbieter wie Kap. 2.3.1 dargelegt und betreibt ein speziellen auf die Anforderungen der Akkreditierung angepassten Prozess innerhalb der PKI zur Ausstellung von Zertifikaten mit digitalem Akkreditierungssymbol und Hoheitszeichen der nationalen Behörde.

Eine von der DAkkS akkreditierte Konformitätsbewertungsstelle (CAB) erhält Zugang zu dieser Public-Key-Infrastruktur (PKI). Die Konformitätsbewertungsstelle (CAB) erhält dazu von einem qualifizierten Vertrauensdiensteanbieter fortgeschrittene Siegel auf Basis von qualifizierten Siegelzertifikaten und kryptographisches Schlüsselmaterial, um die akkreditierte Konformitätsbewertungsstelle zu befähigen, ihre Bestätigungen (z.B. Zertifikate, Ergebnisberichte, Laborberichte, Kalibrierscheine, Inspektionsberichte, etc.) digital zu siegeln, um damit die Integrität des Inhaltes dieser Dokumente sowie die Authentizität der akkreditierten Konformitätsbewertungsstelle für die elektronische Übermittlung und Weiterverarbeitung zu gewährleisten. Die an akkreditierten Konformitätsbewertungsstellen ausgegebenen fortgeschrittenen Siegel auf Basis qualifizierter Siegelzertifikate gemäß DAkkS-Zertifikatsprofil enthalten ein digitales Akkreditierungssymbol und Hoheitszeichen, welches den Akkreditierungsstatus der herausgebenden

Konformitätsbewertungsstelle abbildet und das mit dem digitalen Siegel der akkreditierten Konformitätsbewertungsstelle kryptographisch verknüpft ist. Die Siegelzertifikate gemäß dem DAkkS-Zertifikatsprofil können damit hochdigitalisierte und vollautomatische Prozesse mit maschinenlesbaren- und maschineninterpretierbaren Inhalten unterstützen und den elektronischen Austausch von Konformitätsbestätigungen in der globalen Lieferkette und zwischen Akteuren der internationalen Qualitätsinfrastruktur sicherstellen.

2.3 Zuordnung der Rollen und Entitäten in der PKI

2.3.1 Vertrauensdiensteanbieter (VDA)

Ein Vertrauensdiensteanbieter (VDA) im Sinne dieses Dokuments ist ein Qualifizierter Vertrauensdiensteanbieter gemäß Art 3 Nr. 20 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde.

2.3.2 D-Trust GmbH (CA und RA)

Die D-Trust GmbH ist als VDA von der DAkkS damit beauftragt, Siegelzertifikate zu erstellen, die von der DAkkS bestätigte Attribute enthalten. Die D-Trust GmbH nimmt als Vertrauensdiensteanbieter insbesondere die folgenden Rollen war:

- Registrierungsstelle (RA)

  Registrierungsstellen (Registration Authority) sind Einrichtungen der PKI. Die RA erfasst und beurteilt Anträge für Zertifizierungsdienstleistungen auf Siegelzertifikate.

- Zertifizierungsstelle (CA)

  Die Zertifizierungsstelle (Certification Authority – CA) stellen Zertifikate aus und Sperrinformationen (certificate revocation list, CRL) bereit.

Die D-Trust prüft die in den Zertifikatsanträgen enthaltenen Organisationsdaten gegen öffentlich verfügbare Register. Damit übernimmt D-Trust die Organisationsvalidierung. Die Prüfung erfolgt gemäß [ETSI_EN_319_411-1], Abschnitt 6.2.2.

Die ausgestellten Zertifikate sind qualifizierte Siegelzertifikate ohne die Speicherung auf einer Hardware, der sogenannten QES (qualifizierte[1] digitale Signatur-/Siegelerstellungseinheit), im Sinne der eIDAS [Art. 3 Abs. 30 eIDAS VO].

Der beauftragte Vertrauensdiensteanbieter ist verpflichtet, qualifizierte Siegelzertifikate unter Berücksichtigung der Anforderungen der eIDAS VO zu erstellen. Die Anwendung des Zertifikatsprofils mit DAkkS-Attributen und die Aufnahme der entsprechenden OID in die Endnutzerzertifikate setzt

[1] Qualifiziert meint hier, dass die Speicherung des kryptographischen Schlüssels und des Zertifikats auf einer Smartcard (Hardware) erfolgt.

voraus, dass die hier dokumentierte TSPS (Trust Service Practice Statement) zwingend von der DAkkS angewendet wird.

2.3.3 DAkkS-Zertifikatsprofil für elektronische Siegel

Das DAkkS-Zertifikatsprofil, wie in dieser TSPS beschrieben, wird durch eine geschlossene Benutzergruppe der von der DAkkS akkreditierten und überwachten Konformitätsbewertungsstellen genutzt. Die CA des VDA ermöglicht die Bereitstellung von digitalen Siegeln, die auf dem Produkt der D-Trust GmbH „Qualified Seal ID“ basieren. Die in diesem Dokument beschriebenen Siegel sind eine Erweiterung dieses Produkts. Unter Verwendung dieses Produkts werden Siegel erstellt, die als fortgeschrittene Siegel auf Basis eines qualifizierten Siegelzertifikats eingeordnet sind (Art. 3 Abs. 26, 30 eIDAS VO). Sonstige Merkmale der PKI sind im Dokument [DTR_CSM_PKI] und verwiesenen Dokumenten dargelegt.

2.3.4 Zertifikatsnehmer innerhalb der PKI (Subscriber)

Zertifikatsnehmer bzw. Subscriber sind in dem DAkkS-Zertifikatsprofil die zeichnungsberechtigten Personen der Konformitätsbewertungsstelle. Der Subscriber handelt als gesetzlicher oder rechtsgeschäftlicher Vertreter, um das Siegel für die juristische Person zu beantragen. Sie haben als Vertreter der Organisation die Rolle „Zertifikatsnehmer“ im Sinne der [DTR_TSPS] der D-Trust GmbH und verwiesener Dokumente, und damit die folgenden Rechte, die sie innerhalb ihrer Organisation an weitere natürliche Personen delegieren können:

- Beantragung von Siegelzertifikaten mit den spezifischen Attribut-Inhalten
- Beantragung der Sperrung eines ausgestellten Siegelzertifikats

2.3.5 Endanwender innerhalb der PKI

Endanwender des Siegelzertifikats gemäß dem DAkkS-Zertifikatsprofils sind stets juristische Personen und ist stets Mitglied der Benutzergruppe, wie in 2.3.3 genannt. Die Informationen in den ausgestellten Siegelzertifikaten beziehen sich immer auf die Konformitätsbewertungsstelle als juristische Person. Endanwender erhalten Zertifikate der Zertifizierungsstelle (CA). Die Beantragung ist beschränkt auf zulässige Endanwender, die juristische Personen sind und die in der amtlichen Datenbank der akkreditierten Stellen, als akkreditierte Konformitätsbewertungsstellen gelistet sind oder Anspruch auf Listung haben. Akkreditierte Konformitätsbewertungsstellen haben im Sinne der [DTR_TSPS], Abschnitt 1.3.3 der D-Trust GmbH und verwiesener Dokumente die folgenden Rechte:

- Anwendung des bereitgestellten Siegelzertifikats mit Schlüsselmaterial zur Siegelung von Dokumenten gemäß der DAkkS-TSPS

2.3.6 DAkkS als fachlicher Vertreter der Konformitätsbewertungsstelle

Der Zertifikatsnehmer autorisiert die DAkkS für den Antragsprozess und für den Sperrprozess im Namen des Zertifikatsnehmers Erklärungen und Handlungen gegenüber dem VDA in seinem Namen abzugeben. Die Autorisierung garantiert die Validität der akkreditierungsspezifischen Attributsinhalte, da die nationale Akkreditierungsbehörde vor der Herausgabe des elektronischen Siegels an den Zertifikatsnehmer diese Inhalte kontrolliert und freigibt. Ebenfalls hat die nationale

Akkreditierungsbehörde die Möglichkeit ausgegebene Siegelzertifikate unmittelbar zu sperren, wenn die akkreditierungsspezifischen Attribute nicht mehr dem Zertifikatsprofil gemäß dieser TSPS [DAkkS_TSPS] entsprechen.

2.3.7 Zertifikatsnutzer der PKI

Zertifikatsnutzer (englisch relying parties) sind natürliche oder juristische Personen, die Zertifikate gemäß dem DAkkS-Zertifikatsprofil zum Zweck der Verifikation von Authentizität und Integrität von gesiegelten Dokumenten nutzen ohne Zertifikatsnehmer zu sein. Typische Zertifikatsnutzer sind Kunden der akkreditierten Konformitätsbewertungsstellen, die Interesse an der Verifikation der Siegelzertifikate gemäß dem DAkkS-Zertifikatsprofil haben.

2.3.8 Andere PKI-Nutzer der PKI

Andere PKI-Nutzer die gegenüber dem VDA keine vertraglichen Verbindlichkeiten haben und auch nicht in den Schutzbereich als Kunde des Zertifikatsnehmers zu Verifikationszwecken einbezogen sind, werden in dieser TSPS nicht näher berücksichtigt.

3 Zielsetzung der DAkkS-TSPS

Zertifikate die dem DAkkS-Zertifikatsprofil entsprechen, werden von der ausstellenden CA mit der Bezeichnung: „D-TRUST CA 5-22-2 2022“, vom VDA ausgegeben. Die zugehörige Root-CA lautet „D-TRUST Root CA 5 2022“.

Diese DAkkS-TSPS ergänzt lediglich die Vorgaben, die der Vertrauensdiensteanbieter (VDA) bei der Erbringung seiner Dienstleistungen anwendet. Neben diesem Dokument gilt insbesondere die Zertifikatsrichtlinie (CP) der D-Trust, die den Zertifizierungsprozess während der gesamten Lebensdauer der ausgestellten Zertifikate, beginnend mit der Authentifizierung und Registrierung von PKI-Teilnehmern, über die Ausstellung, Anwendung von Zertifikaten bis hin zur Verlängerung, Sperrung oder Ablauf von Zertifikaten, regeln. Die DAkkS-TSPS und die CP der D-Trust sind rechtsverbindlich. Sie enthalten Aussagen über Pflichten, Gewährleistung und Haftung für die Teilnehmer der PKI, die dem DAkkS-Zertifikatsprofil entsprechen. Soweit nicht ausdrücklich genannt, erfolgen auf Basis der DAkkS-TSPS und der CP derD-Trust keine vertraglichen Zusicherungen oder Garantien im Rechtssinne. Die Kenntnis der in diesem TSPS beschriebenen Zertifizierungsverfahren und -regeln sowie der rechtlichen Rahmenbedingungen erlaubt es Benutzern, Vertrauen in die PKI aufzubauen und Entscheidungen zu treffen, inwieweit das durch die PKI gewährte Vertrauens- und Sicherheitsniveau für Anwendungen geeignet ist.

4 Hierarchie der Dokumente in der PKI

Diese DAkkS-TSPS nimmt Bezug auf die geltenden Dokumente der D-Trust GmbH als VDA. In nachfolgender Grafik werden die Beziehungen dieses Dokumentes zu den Dokumenten des VDA und alle für dieses Zertifikatsprofil relevanten Dokumente des VDA angegeben. Die Dokumente des VDA sind abrufbar unter https://www.d-trust.net/en/support/repository.

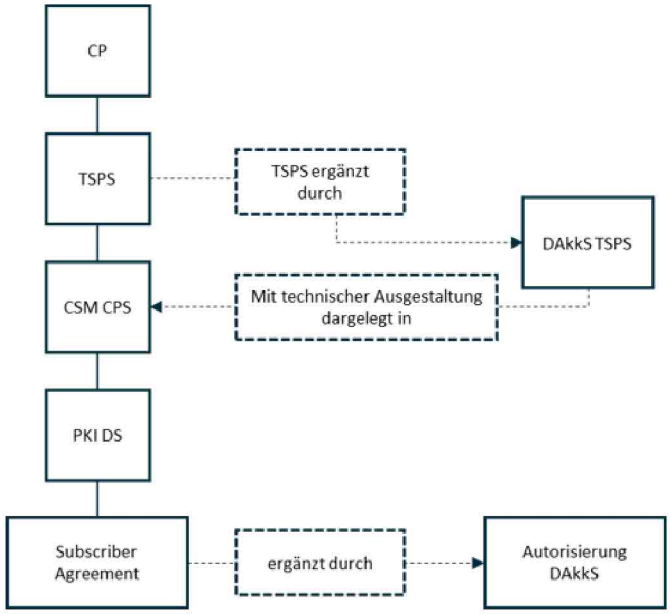


Abbildung 3: Hierarchie der Dokumente in der PKI

Diese DAkkS-TSPS berücksichtigt die Normen:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- 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.

Jedes Siegelzertifikat aus der PKI entspricht dem Standard X.509v3. Im Bereich Erweiterung (**Extensions**) werden im Bereich Policies (2.2.29.32) die relevanten Dokumente dokumentiert, die für das konkrete Zertifikat Geltung beanspruchen:

OID	Wert	Anmerkung
0.4.0.149112.1.1	-	Teil des Basis-Produkts: QCP-l: certificate policy for European Union (EU) qualified certificates issued to legal persons
1.3.6.1.4.1.4788.2.150.5	Policy Qualifier http://www.d-trust.net/internet/files/D-TRUST_CSM_PKI_CPS.pdf	Teil des Basis-Produkts: D-Trust-spezifische Kennzeichnung für qualifizierte Siegelzertifikate ohne qualifizierte Signaturerstellungseinheit, gemäß EN 319 411-2 QCP-l.

1.3.6.1.4.1.59749.2.1	**CPSuri:** https://accreditationauthority.dakks.de/pki/dakks-tsps.pdf	URL zur DAkkS-TSPS
	User Notice Hoheitszeichen (OID: 1.3.6.1.4.1.59749.3.1): https://accreditationauthority.dakks.de/authoritiesemblem.pdf	URL zur **User Notice** mit dem Hoheitszeichen

5 Zertifikatsverwendungen

Die Verwendung aller Siegelzertifikate gemäß dem DAkkS-Zertifikatsprofil ist beschränkt auf die Siegelung von elektronischen Bestätigungen, insbesondere in Ergebnisberichten von akkreditierten Konformitätsbewertungsstellen (eAttestation). Alle Siegelzertifikate der PKI enthalten die Erweiterung („**AdditionalInformation**“, siehe [COMMONPKI], Abschnitt 2.1 und Tabelle 29f) sowie eine spezifische Einschränkung („**Restriction**“, siehe [COMMONPKI], Abschnitt 2.1 und Tabelle 29e).

Diese Erweiterung ist vom Antragsteller mit dem nachfolgenden Wert zu befüllen:

Erweiterung	Wert
Zusätzliche Information (additional information)	Attestation by a conformity assessment body (CAB) as defined in clause 7.3 of ISO/IEC 17000 that the object of a conformity assessment as defined in clause 4.2 of ISO/IEC 17000 meets certain specified requirements or expectations as defined in clause 5.1 of ISO/IEC 17000, in particular the digital sealing of result reports ("statements of conformity").
Einschränkung (restriction)	The application of the sealing key is limited to the sealing of the attestation (statement of conformity).

6 Kryptographische Ausgestaltungen in der PKI

Die qualifizierten Siegelzertifikate gemäß dem DAkkS-Zertifikatsprofil stammen aus einer CA der D-Trust. Die aktuell verwendete CA der D-Trust GmbH ist:

- D-TRUST CA 5-22-2 2022, RSA 4096-Schlüssel, Zertifikatssignatur SHA512 / RSA-PSS

Die dazugehörige Root-CA heißt „D-TRUST Root CA 5 2022“.

Die Siegelschlüssel werden vom CSM der D-Trust erzeugt, derzeit sind dies RSA Schlüssel mit einer Länge von 4096 Bit. Vorgehen nach der Auslieferung der erzeugten Schlüssel finden sich im Dokument [DTR_TSPS], Abschnitt 6.2.10 „Zerstörung privater Schlüssel“.

7 Besonderheiten für das Verfahren in der PKI

Für die Prozesse der Beantragung und Sperrung von Zertifikaten gemäß dem DAkkS-Zertifikatsprofil gelten folgende Bestimmungen, als Konkretisierung der CP und CPS der D-Trust.

7.1 Besonderheiten zur Beantragung

7.1.1 Eingeschränkte Antragsberechtigung

Antragsberechtigt für den Erhalt von qualifizierten Siegelzertifikaten unter Verwendung des DAkkS-Zertifikatsprofils sind nur juristische Personen im Sinne der DAkkS-Regel R 17011. Ausgeschlossen ist die Ausgabe von Zertifikaten an natürliche Personen. Anträge juristischer Personen werden zudem erst angenommen, wenn die juristische Person in der amtlichen Datenbank der akkreditierten Stellen der DAkkS mit mindestens einer Akkreditierung geführt wird oder Anspruch darauf hat und diese Akkreditierung nicht ausgesetzt ist.

7.1.2 Verpflichtung des Antragstellers durch die DAkkS

Der Antragsteller wird vertraglich zur Einhaltung dieser TSPS, unter aller Dokumente des VDA wie in Kapitel 4 dargestellt, im Rahmen des Registrierungsprozesses verpflichtet. Das Akzeptieren der Vertragsbedingungen wird dokumentiert.

7.2 Besonderheiten zur Autorisierung durch die nationale Akkreditierungsstelle (NAB)

Für jeden Antrag auf Ausgabe eines qualifizierten Siegelzertifikates, welches im Zertifikat ein digitales Hoheitszeichen für den Status der Akkreditierung der Konformitätsbewertungsstelle enthält, ist es erforderlich, der DAkkS als national zuständige Akkreditierungsbehörde, die Rechte als fachlicher Vertreter einzuräumen. Die DAkkS delegiert diese Rolle an ihre Bedienstete und kann in dieser Rolle z.B. qualifizierte Siegelzertifikate für akkreditierte Stellen freigeben oder deren unverzüglichen Widerruf gegenüber der D-Trust GmbH verlangen, wenn die Akkreditierung ausgesetzt oder zurückgezogen wird.

Davon unberührt bleibt das Recht der Konformitätsbewertungsstelle, dass die Konformitätsbewertungsstelle selbst jederzeit den Widerruf ihrer Zertifikate verlangen kann.

7.3 Besonderheiten zur Identifizierung und Authentifizierung

Der Ablauf während der Registrierung des Antragstellers enthält mindestens folgende Schritte:

1. Akkreditierungsverfahren:
   Ablauf und Bescheid einer Akkreditierung, Überprüfung der Antragsdaten auf Nutzung eines „digitalen Akkreditierungssymbols“ im Rahmen der Akkreditierung einer KBS
2. Versand der Vertragsunterlagen, Unterrichtungen und Autorisierung für Siegelzertifikatsnutzung in PKI,
3. Eingangskontrolle der Autorisierung, Identifizierung des Antragstellers als juristische Person und der zeichnungsberechtigten Person

4. Befähigung der Zertifikatsnehmer durch DAkkS Operatoren innerhalb der PKI
5. Bestätigung der Akkreditierung (Berufsgruppenattribut) bei Beantragung Siegelzertifikat durch Zertifikatsnehmer in PKI

1. Akkreditierungsverfahren

Die DAkkS überprüft in ihrer Funktion als Akkreditierungsbehörde, dass der Antrag auf Akkreditierung durch eine juristische Person gestellt wird, die von sich behauptet Konformitätsbewertungsstelle zu sein. Die DAkkS ist gemäß § 1 AkkStelleG i.V.m VO (EG) 765/2008 die in Deutschland zuständige Behörde für Akkreditierungen von Konformitätsbewertungsstellen und erteilt den Status als akkreditierte Konformitätsbewertungsstelle durch hoheitlichen Verwaltungsakt nach dem VwVfG. Die Akkreditierung wird per amtlichen Bescheid bestätigt. Diesem geht eine Überprüfung der Identität und der Kompetenz der Konformitätsbewertungsstelle zu den beantragten Konformitätsbewertungsaktivitäten gemäß ISO/IEC 17011 voraus und zieht eine stetige staatliche Überwachung der akkreditierten Stelle und ihrer Kompetenzen nach sich.

Für die Nutzung eines „digitalen Akkreditierungssymbols“ welches die spätere Ausstellung eines fortgeschrittenen Siegels auf Basis eines qualifizierten Siegelzertifikates beinhaltet ist ebenfalls von Seiten einer Konformitätsbewertungsstelle ein Antrag bei der DAkkS zu stellen. Die DAkkS prüft an dieser Stelle, ob der Antragsteller in der **amtlichen Datenbank** der DAkkS für akkreditierte Stellen gelistet ist oder Anspruch auf Listung (Akkreditierungsentscheidung ist gefallen) in dieser Datenbank hat. **Nur im Erfolgsfall wird die Nutzung eines „digitalen Akkreditierungssymbols“ durch die DAkkS gestattet,** andernfalls abgelehnt.

2. Versand der Vertragsunterlagen

Es werden auf dem Postweg an die physische Adresse des Sitzes der Konformitätsbewertungsstelle die für die Ausstellung eines Siegelzertifikates notwendigen Vertragsunterlagen sowie das Autorisierungsdokument versendet. Damit wird die Erreichbarkeit und die Korrektheit der Angaben zur juristischen Person erneut überprüft.

3. Eingangskontrolle der Autorisierung

Nach erfolgter Rücksendung des Autorisierungsdokuments durch die Konformitätsbewertungsstelle per Mail oder Post an die DAkkS, prüfen die dem VDA benannten Operatoren der DAkkS zunächst, ob das Dokument in Schriftform (§ 126 BGB/ § 126a BGB) mit dem Firmenstempel vorliegt. Ebenso wird geprüft, ob das Dokument von einer **zeichnungsberechtigten Person** der juristischen Person (**Konformitätsbewertungsstelle**), unterzeichnet wurde. Die Identität der zeichnungsberechtigten Person wurde bereits im Verwaltungsverfahren mittels Handelsregisterauszug geprüft und wird an dieser Stelle nochmals geprüft. Dem Handelsregister liegt jeweils eine notarielle Beglaubigung der Anmeldung zugrunde, die eine physische Identifizierung mit amtlichen Dokumenten vor dem zuständigen Notar vorausgesetzt hat. Bei juristischen Personen, die nicht registerfähig sind, wird die Identität des Zeichnungsberechtigten anhand der im Verwaltungsverfahren vorgelegten

Antragsautorisierungen (Gesellschaftsverträge; Vollmachten; etc.) durch die zuständige Behörde verifiziert und bestätigt und wird im Rahmen des hier notwendigen Autorisierungsverfahrens erneut geprüft. Es wird sichergestellt und ggf. amtlich bescheinigt, dass der Unterzeichnende der Zeichnungsberechtigte (z. B. laut Handelsregister) der autorisierenden Konformitätsbewertungsstelle ist. Über die Echtheit der genannten Dokumente wird keine Nachforschung seitens des VDA veranlasst.

Bei Abweichungen ist der Prozess zu wiederholen oder ein vom VDA zugelassenes Fernidentifizierungsverfahren [DTR_CSM_CPS] anzuwenden, um die Identität der Person, die die Autorisierung unterzeichnet hat, zu prüfen.

4. Befähigung der Zertifikatsnehmer

Nach erfolgreicher Prüfung der Organisation und ihrer zeichnungsberechtigten Person mittels offizieller Registereinträge (Handelsregistereinträge, etc.) sowie der Berechtigung zur Beantragung eines Siegelzertifikates (Datenbank akkreditierter Stellen) legen die Operatoren der DAkkS (DAkkS Bedienstete) in ihrer Rolle als „fachliche Vertreter“ der Konformitätsbewertungsstelle diese innerhalb der PKI als Organisation an. Damit werden die zeichnungsberechtigten Personen – oder weitere natürliche Personen an die die Aufgabe delegiert wurde – befähigt ihre Rolle als „Zertifikatsnehmer“ auszufüllen.

5. Bestätigung der Akkreditierung in PKI

Die zeichnungsberechtigten Personen oder weitere natürliche Personen, an die die Aufgabe delegiert wurde, können innerhalb der PKI ihren Siegelzertifikatsantrag stellen. Die von der DAkkS benannten Operatoren (DAkkS Bedienstete) bestätigen dann in ihrer Rolle als attributsbestätigende Stelle den Siegelzertifikatsantrag des Zertifikatsnehmers.

7.4 Besonderheiten zur Sperrung

Das Sperren von Zertifikaten kennzeichnet diese ab dem Zeitpunkt der Sperrung als ungültig. Eine Sperrung kann nicht aufgehoben oder rückgängig gemacht werden. Sie kann auch nicht rückwirkend erfolgen. Es ist nicht notwendig, Zertifikate nach Ablauf ihrer Gültigkeit zu sperren.

Insbesondere gelten folgende Besonderheiten:

Die DAkkS ist verpflichtet sicherzustellen, dass sie jederzeit in der Lage ist, ein elektronisch bereitgestelltes Akkreditierungssymbol mit oder ohne Hoheitszeichen im Sinne von Tz. 3.12 der ISO/IEC 17011 zu sperren (vgl. Art. 11 Abs. 2 VO (EG) 765/2008; § 4 Abs. 4 Satz 2 SymbolVO; Tz. 4.3.3. lit. a und c); Tz. 4.3.5 ISO/IEC 17011).

Die DAkkS kann deshalb gegenüber dem Vertrauensdiensteanbieter ein Zertifikat aus der DAkkS jederzeit nach pflichtgemäßem Ermessen sowie bei Verstoß gegen die Anforderungen dieser TSPS über den CSM sperren lassen.

8 Verifizierung zum Status der Gültigkeit des digitalen Akkreditierungssymbols

Das im Zertifikat enthaltene Akkreditierungssymbol ist nur dann gültig, wenn **(1)** die Signaturprüfung des Zertifikates (kryptographische Integrität) gültig ist, **(2)** die Gültigkeitsdauer des Zertifikates nicht überschritten ist, **(3)** der Widerrufsstatus der Gültigkeitsabfrage für das Zertifikat in Bezug zum Referenzzeitpunkt der Siegelerstellung gemäß Schritt 8.3 dieser TSPS das Ergebnis „gültig“ erbracht hat, **(4)** das Zertifikat von der CA „D-TRUST CA 5-22-2 2022“ ausgestellt wurde und der Zertifizierungspfad auf die aktuell im Einsatz befindliche Root-CA „D-TRUST Root CA 5 2022“ (Vertrauensanker) verweist und **(5)** das Zertifikat im Bereich „Admission“ die OID 1.3.6.1.4.1.59749.1 des digitalen Akkreditierungssymbols mit Hoheitszeichen enthält.

8.1 Schritt 1: Signaturprüfung des Zertifikats (kryptographische Integrität)

Das X.509v3 Zertifikat wird mit dem privaten Schlüssel des Ausstellers (CA) des Zertifikats signiert. Mittels des dazugehörigen öffentlichen Schlüssels (public key) kann die Signatur überprüft werden. Es sind die Anforderungen des Standards: „BSI TR-02103 X.509-Zertifikate und Zertifizierungspfadvalidierung“[2] auf Grundlage von RFC 5280 einzuhalten. Wenn die Signaturprüfung fehlschlägt, ist die gesamte Prüfung negativ.

8.2 Schritt 2: Gültigkeitszeitraum

Es muss geprüft werden, ob der aktuelle Zeitpunkt der Zertifikatsprüfung innerhalb der Gültigkeitsdauer eines Zertifikats liegt. Überprüfen Sie den Gültigkeitszeitraum des Zertifikates. Die Gültigkeit eines Zertifikats endet mit dem im Zertifikat vermerkten Ablaufdatum im Feld „Gültig bis“.

8.3 Schritt 3: Widerrufsstatus der Gültigkeitsabfrage über OCSP oder CRL

Der Statusabfragedienst des VDA ist über das Protokoll OCSP verfügbar. Der Dienst ist unter der URL im Zertifikatsfeld „AuthorityInfoAccess“ angegeben. Die Formate und Protokolle der Dienste sind in den Abschnitten 7 der D-Trust-TSPS beschrieben. Die Systemzeit des OCSP-Responder wird täglich mit dem deutschen DCF77-Zeitsignal und verlässlichen Zeitservern (NTP) im Internet synchronisiert. Der VDA gewährleistet, dass der Statusabfragedienst 24 Stunden an 7 Tagen der Woche bereitsteht und eine Verfügbarkeit von 99,95% hat. Der VDA stellt sicher, dass im Falle einer Störung die Ausfalldauer (downtime) maximal vier Stunden beträgt.

Alternativ werden durch den VDA Sperrlisten (CRL) angeboten, die URL des Sperrlistenverteilpunkts befindet sich im Zertifikatsfeld „CRLDistribution Point“. Es gelten die Regelungen der CP, CSM CPS und TSPS der D-Trust.

[2] Originaldokument abrufbar unter: BSI TR-02103 X.509-Zertifikate und Zertifizierungspfadvalidierung (letzter Aufruf 28.08.23)

8.4 Schritt 4: Validierung des Zertifizierungspfad bis zum Vertrauensanker

Die Schritte 1 bis 3 werden im Zertifizierungspfad des Ausstellerzertifikats des zu prüfenden Zertifikats ausgeführt bis zur gültigen Root CA „D-TRUST Root CA 5 2022“. Diese gilt für Zwecke der DAkkS als Vertrauensanker. Wenn eine Signaturprüfung im Zertifizierungspfad fehlschlägt, ist die gesamte Prüfung negativ.

8.5 Schritt 5: Digitales Hoheitszeichen

Parsen Sie in der Erweiterung (**Extensions**) den Bereich "Admission" OID: "1.3.36.8.3" und lesen sie den Bereich "Admission Authority" aus. Dort muss die registered ID „1.3.6.1.4.1.59749.1 {= DAkkS Akkreditierungssymbol}" angegeben sein. Der Wert der OID „1.3.6.1.4.1.59749.1” ist die maschinenlesbare Entsprechung des Akkreditierungssymbols mit Hoheitszeichen der DAkkS und zeigt an, dass die im „Subject“ benannte Stelle (Zertifikatsinhaber) akkreditiert ist.

Die Zertifikate entfalten ihre Bedeutung als Digitale Hoheitszeichen, wenn sich in der **Extension Admission** (siehe [COMMONPKI], Abschnitt 2.1, Tabelle 29b), die folgende Struktur findet:

- Als „Admission Authority“ ist die OID 1.3.6.1.4.1.59749 ausgewiesen.
- Innerhalb der Struktur „ContentsOfAdmission“ ist die DAkkS als Admission Authority durch den DirectoryString „C=DE, O=Deutsche Akkreditierungsstelle GmbH (DAkkS)“ ausgewiesen.
- Innerhalb der Struktur „ProfessionInfos“ als „ProfessionItem“ ist der Text „DAkkS akkreditierte Konformitätsbewertungsstelle“ und als „Profession OID“ die OID „1.3.6.1.4.1.59749.1“ wiederzufinden.

9 Prüfung von gesiegelten Bestätigungen von Konformitätsbewertungsstellen

Bei der Prüfung von gesiegelten Bestätigungen gilt der Zeitpunkt der Siegelerstellung als Referenzzeitpunkt für die Zertifikatsprüfung. Weitere Informationen zu der definierten Aussteller-CA in maschinenlesbarem Format (XML) finden sich auf der Trusted-List der EU (https://ec.europa.eu/tools/lotl/eu-lotl.xml).

10 Informationen zum Geltungsbereich der Akkreditierung

10.1 Schritt 1: Auslesen der „Subject-Serialnumber“

Das X.509v3 Zertifikat enthält im Bereich >Subject< das Attribut „SerialNumber“ aus [ITU-T-X.520], indem die eindeutige >Registrierungsnummer der Urkunde< zur Kennzeichnung des Akkreditierungsverfahrens der Konformitätsbewertungsstelle (CAB) angegeben ist.

Der Wert hat mindesten 22 Zeichen, die wie nachfolgend dargestellt strukturiert sein müssen. Der Wert kann maximal 64 Zeichen umfassen.

Die ersten 22 Stellen des Wertes haben folgende Bedeutung:

AAAAAAA-CC-XX-YYYYY-ZZ-NN

AAAAAAA: max. 7 Stellen für Kurzbezeichnung der NAB (z.B. DAkkS00)

CC: zwei Stellen für den ISO-Code des WTO-Staates von dem die NAB autorisiert worden ist und in dem diese ihren Sitz hat (z. B. DE)

XX: zwei Stellen für das Kurzzeichen der Akkreditierungsaktivität

Für die DAkkS sind dies:

BB	Biobanken
IS	Inspektionsstelle
K0	Kalibrierlaboratorium
ML	Medizinisches Laboratorium
PL	Prüflaboratorium
EP	Anbieter von Eignungsprüfungen
RM	Referenzmaterialhersteller
ZE	Zertifizierungsstelle für Produkte
ZM	Zertifizierungsstelle für Managementsysteme
ZP	Zertifizierungsstelle für Personen
VS	Validierungs- bzw. Verifizierungsstelle

YYYYY: fünf Stellen für die fortlaufende Stammnummer (Kundennummer) zur Identifikation der Rechtsperson der Konformitätsbewertungsstelle in der Datenbank der NAB

ZZ: zwei stellen für eine fortlaufende Nummer der Konformitätsbewertungsstelle, die innerhalb einer Akkreditierungsaktivität mehrere eigenständige Akkreditierungsverfahren anzeigt

NN: Weitere Stellen für Festlegungen der zuständigen NAB. Bei der DAkkS ist dies die Registriernummer als eindeutige Kennzeichnung einer Urkunde (Gesamturkunde und Teilurkunde) und deren Anlage zum Akkreditierungsbescheid. Gibt es zu einem Akkreditierungsverfahren keine Teilurkunden sondern nur eine Gesamturkunde, ist „NN“ = „00“.

Ein Beispiel für die Registrierungsnummer der zutreffenden Urkunde ist: DAkkS00-DE-PL-19516-01-00

10.2 Schritt 2: Datenbank der akkreditierten Stellen

Mit der Registrierungsnummer der Urkunde kann der Zertifikatsinhaber über die amtliche Datenbank der akkreditierten Stellen der DAkkS gefunden werden. Diese ist abrufbar unter www.dakks.de.

Dort wird tagesaktuell der aktuelle Geltungsbereich der Akkreditierung dargestellt.

11 Graphische Übersicht zum Zertifikatsprofil

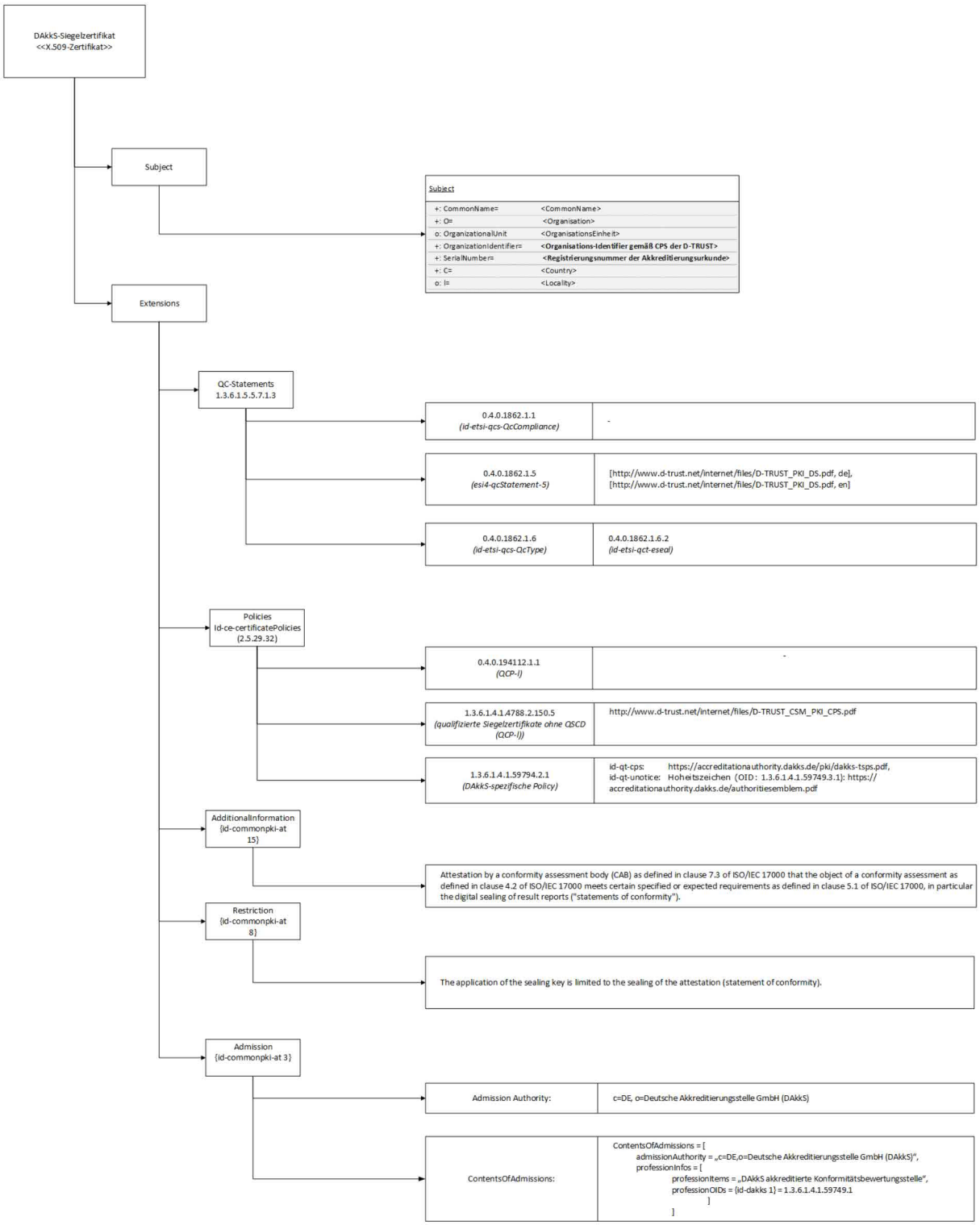
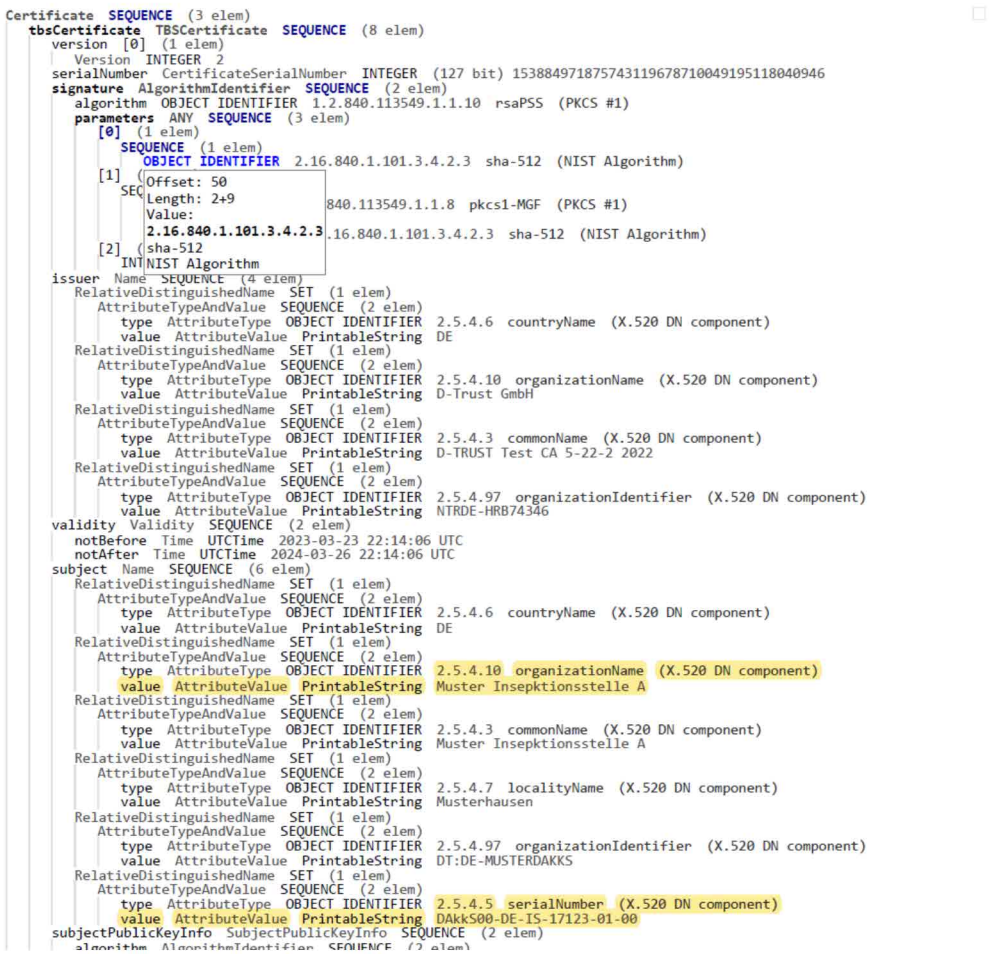


Abbildung 4: Zertifikatsprofil auf Basis Spezifikationsdokument der D-Trust für DAkkS-spezifisches Siegelzertifikat

12 Zertifikatsprofil

Ausschnitt aus einem Musterzertifikatsbaum



```
Extension  SEQUENCE  (2 elem)
   extnID  OBJECT IDENTIFIER  1.3.36.8.3.3  admission  (Teletrust attribute)
   extnValue  OCTET STRING  (162 byte) 30819F88082B0601040183D26530819230818FA047A44530433134303206035504 0A1…
      SEQUENCE  (2 elem)
         [8]  (8 byte) 2B0601040183D265
         SEQUENCE  (1 elem)
            SEQUENCE  (2 elem)
               [0]  (1 elem)
                  [4]  (1 elem)
                     SEQUENCE  (2 elem)
                        SET  (1 elem)
                           SEQUENCE  (2 elem)
                              OBJECT IDENTIFIER  2.5.4.10  organizationName  (X.520 DN component)
                              PrintableString  Deutsche Akkreditierungsstelle GmbH (DAkkS)
                        SET  (1 elem)
                           SEQUENCE  (2 elem)
                              OBJECT IDENTIFIER  2.5.4.6  countryName  (X.520 DN component)
                              PrintableString  DE
               SEQUENCE  (1 elem)
                  SEQUENCE  (2 elem)
                     SEQUENCE  (1 elem)
                        UTF8String  DAkkS akkreditierte Konformitätsbewertungsstelle
                     SEQUENCE  (1 elem)
                        OBJECT IDENTIFIER  1.3.6.1.4.1.59749.1
   Extension  SEQUENCE  (2 elem)
      extnID  OBJECT IDENTIFIER  1.3.6.1.5.5.7.1.1  authorityInfoAccess  (PKIX private extension)
      extnValue  OCTET STRING  (123 byte) 3079302B06082B06010505073001861F687474703A2F2F73746167696E672E6F63737…
         SEQUENCE  (2 elem)
            SEQUENCE  (2 elem)
               OBJECT IDENTIFIER  1.3.6.1.5.5.7.48.1  ocsp  (PKIX OCSP)
               [6]  (31 byte) http://staging.ocsp.d-trust.net
            SEQUENCE  (2 elem)
               OBJECT IDENTIFIER  1.3.6.1.5.5.7.48.2  caIssuers  (PKIX subject/authority info access descriptor)
               [6]  (62 byte) http://www.d-trust.net/cgi-bin/D-TRUST_Test_CA_5-22-2_2022.crt
   Extension  SEQUENCE  (2 elem)
      extnID  OBJECT IDENTIFIER  2.5.29.32  certificatePolicies  (X.509 extension)
      extnValue  OCTET STRING  (229 byte) 3081E2300C060A2B06010401A534020202308 1D1060A2B0601040183D26502013081C…
         SEQUENCE  (2 elem)
            SEQUENCE  (1 elem)
               OBJECT IDENTIFIER  1.3.6.1.4.1.4788.2.2.2
            SEQUENCE  (2 elem)
               OBJECT IDENTIFIER  1.3.6.1.4.1.59749.2.1
               SEQUENCE  (2 elem)
                  SEQUENCE  (2 elem)
                     OBJECT IDENTIFIER  1.3.6.1.5.5.7.2.1  cps  (PKIX policy qualifier)
                     IA5String  https://accreditationauthority.dakks.de/pki/dakks-tsps.pdf
                  SEQUENCE  (2 elem)
                     OBJECT IDENTIFIER  1.3.6.1.5.5.7.2.2  unotice  (PKIX policy qualifier)
                     SEQUENCE  (1 elem)
                        UTF8String  Hoheitszeichen (OID: 1.3.6.1.4.1.59749.3.1): https://accreditationauthority.dak
   Extension  SEQUENCE  (2 elem)
      extnID  OBJECT IDENTIFIER  2.5.29.31  cRLDistributionPoints  (X.509 extension)
      extnValue  OCTET STRING  (68 byte) 30423040A03EA03C863A687474703A2F2F63726C2E642D74727573742E6E65742F6372…
         SEQUENCE  (1 elem)
            SEQUENCE  (1 elem)
               [0]  (1 elem)
                  [0]  (1 elem)
                     [6]  (58 byte) http://crl.d-trust.net/crl/d-trust_test_ca_5-22-2_2022.crl
   Extension  SEQUENCE  (2 elem)
      extnID  OBJECT IDENTIFIER  2.5.29.14  subjectKeyIdentifier  (X.509 extension)
      extnValue  OCTET STRING  (22 byte) 041471DB3EE517D6A9DC6359CEF04F48A2CF4E3D58E0
         OCTET STRING  (20 byte) 71DB3EE517D6A9DC6359CEF04F48A2CF4E3D58E0
   Extension  SEQUENCE  (3 elem)
      extnID  OBJECT IDENTIFIER  2.5.29.15  keyUsage  (X.509 extension)
      critical  BOOLEAN  true
      extnValue  OCTET STRING  (4 byte) 030206C0
         BIT STRING  (2 bit) 11
   Extension  SEQUENCE  (2 elem)
      extnID  OBJECT IDENTIFIER  1.3.36.8.3.8  restriction  (Teletrust attribute)
      extnValue  OCTET STRING  (109 byte) 0C6B546865206170706C69636174696F6E206F662074686520736 5616C696E67206B6…
         UTF8String  The application of the sealing key is limited to the sealing of the attestation …
   Extension  SEQUENCE  (2 elem)
      extnID  OBJECT IDENTIFIER  1.3.36.8.3.15  additionalInformation  (Teletrust attribute)
      extnValue  OCTET STRING  (354 byte) 0C82015E417474657374617469 6F6E206279206120636F6E666F726D6974792061737…
         UTF8String  Attestation by a conformity assessment body (CAB) as defined in clause 7.3 of IS…
signatureAlgorithm  AlgorithmIdentifier  SEQUENCE  (2 elem)
   algorithm  OBJECT IDENTIFIER  1.2.840.113549.1.1.10  rsaPSS  (PKCS #1)
   parameters  ANY  SEQUENCE  (3 elem)
```

```
signatureAlgorithm  AlgorithmIdentifier  SEQUENCE  (2 elem)
   algorithm  OBJECT IDENTIFIER  1.2.840.113549.1.1.10  rsaPSS  (PKCS #1)
   parameters  ANY  SEQUENCE  (3 elem)
      [0]  (1 elem)
         SEQUENCE  (1 elem)
            OBJECT IDENTIFIER  2.16.840.1.101.3.4.2.3  sha-512  (NIST Algorithm)
      [1]  (1 elem)
         SEQUENCE  (2 elem)
            OBJECT IDENTIFIER  1.2.840.113549.1.1.8  pkcs1-MGF  (PKCS #1)
            SEQUENCE  (1 elem)
               OBJECT IDENTIFIER  2.16.840.1.101.3.4.2.3  sha-512  (NIST Algorithm)
      [2]  (1 elem)
         INTEGER  64
signature  BIT STRING  (4096 bit) 1100110010110110100001011001000001110010000011101011110111101001111010…
```

Abbildung 5: Musterzertifikatsauszug

13 Referenzierte Dokumente

13.1 Referenzierte Dokumente für PKI

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente sowie der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Dokumente.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel	Version	Stand (Datum)
[COMMONPKI]	T7 & TeleTrust (2009): Common PKI Specifications for Interoperable Applications	2.0	20.01.2009
[ITU-T-X.520]	ITU (2019): ITU-T X.520 – Information technology – Open Systems Interconnection – The Directory: Selected Attribute types	-	14.10.2019
RFC 3647	The Internet Society (2003): „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework	-	11/2003
[ETSI EN 319 401]	ETSI (2021): Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers	2.3.1	05/2021
[ETSI_EN_319_411-1]	ETSI (2021): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements	1.3.1	05/2021
[ETSI EN 319 411-2]	ETSI (2021): 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.	2.3.1	05/2021
[DTR_CP]	D-Trust (2023): Zertifikatsrichtlinie (CP) der D-Trust GmbH	3.12	14.02.2023
[DTR_TSPS]	D-Trust (2022): D-TRUST Trust Service Practice Statement (TSPS)	1.5	14.11.2022

[DTR_CSM_CPS]	D-Trust (2022): Certification Practice Statement der D-TRUST CSM PKI	3.8	14.11.2022
BSI TR-02103: X.509	BSI (2020): BSI TR-02103 X.509-Zertifikate und Zertifizierungspfadvalidierung	1.0	29.09.2020
eIDAS - Regulation (EU) No. 910/2014	European Parliament and European Council (2014): 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	-	28.08.2014

13.2 Referenzierte Dokumente für Akkreditierung und Konformitätsbewertung

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente mit Bezug auf Akkreditierung und Konformitätsbewertung sowie der mit der vorliegenden Version korrelierenden Entwicklungsstände dieser Dokumente.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel	Version	Stand (Datum)
ISO/IEC 17000	ISO/IEC (2020): Conformity assessment - Vocabulary and general principles	2.0	12/2020
ISO/IEC 17011	ISO/IEC (2017): Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies	2.0	11/2017
Regulation (EC) 765/2008	European Parliament and European Council (2008): REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93	-	13.08.2008
AkkStelleG	Bundesrepublik Deutschland (2009): Gesetz über die Akkreditierungsstelle (Akkreditierungsstellengesetz - AkkStelleG)	-	31.07.2009
AkkStelleGBV	Verordnung über die Beleihung der Akkreditierungsstellenach dem Akkreditierungsstellengesetz (AkkStelleG-Beleihungsverordnung - AkkStelleGBV)	-	19.6.2020
SymbolVO	Verordnung zur Gestaltung und Verwendung des Akkreditierungssymbols der Akkreditierungsstelle (Akkreditierungssymbolverordnung - SymbolVO)	-	15.12.2009

Abbildungsverzeichnis

Bildnachweis zu Abbildung 1

NAB Icon	Quality free icon von Freepik auf www.flaticon.com
CAB Icon	Lab free icon von Freepik auf www.flaticon.com
PDF Icon	PDF free Icon von Freepik auf www.flaticon.com
XML Icon	Xml File free icon von Freepik auf www.flaticon.com
Quality Icon	Quality free Icon von Freepik auf www.flaticon.com
Customer Icon	Factory free icon von Freepik auf www.flaticon.com