Trust Service Practice Statement (TSPS) of DAkkS

Policy for attribute confirmations in seal certificates entailing the digital accreditation symbol and national authority emblem

Version 1.1

01/09/2023

Susanne Kuch; Prof. Dr Raoul Kirmes ©

1 Policy for DAkkS advanced seals with qualified certificates

1.1 Purpose of the Trust Service Practice Statement - TSPS

The purpose of this *Trust Service Practice Statement - (TSPS*) is to set out the criteria for access, application, revocation and verification of advanced seals with qualified certificates that comply with the DAkkS certificate profile and the determination of the accreditation status through the verification of those seals. The DAkkS-TSPS supplements the profile-specific certificate aspects of the documentation of the trust service provider (TSP) operating the Public Key Infrastructure (PKI). More details on the hierarchy of documents in the PKI are presented in chapter 4.

1.2 Imprint

Publisher	German Accreditation Body © 2023 Am Spittelmarkt 10, 10117 Berlin
Short name	DAkkS

1.3 Document identification

Document type	Trust Service Practice Statement (TSPS)
Name of this document	Trust Service Practice Statement (TSPS) of DAkkS
Subtitle:	Policy for attribute confirmations for the digital accreditation symbol and national authority emblem in advanced seals with qualified certificates
Scope of application	Advanced seals with qualified certificates (X.509 certificates) containing a digital, machine-readable accreditation symbol as national authority emblem that entails information about the accreditation status of a certificate holder. This certificate holder can use the advanced seal on attestations.
Short name of this document	DAkkS-TSPS
Reference for this document	[DAKKS_TSPS]
Version	1.1 from 01.09.2023
Object Identifier (OID)	1.3.6.1.4.1.59749.2.1 {= DAkkS TSPS}

1.4 Structure of the document

The structure of this document is based on the structure of the Internet standard RFC 3647 "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework" in order to ensure easy readability and comparability with other TSPS and CP. Due to the special features of the

DAkkS certificate profile, deviations are necessary. Furthermore, not all aspects of RFC 3647 are addressed. Aspects of RFC 3647 that are not documented in the TSPS-DAkkS are set out in the documentation of the trust service provider that operates the PKI. More details on the hierarchy of documents in the PKI are presented in Chapter 4.

1.5 Version history

Version	Date	Change	Editor
0.1	28.01.2023	Initial version	KIR/SKU
1.0	31.03.2023	Published Version (German)	KIR/SKU
1.1	**01.09.2023**	**Published version (first English translation)** ▪ Editorial Changes ▪ Adjustment of 2.1.4 by adding legal entities	KIR/SKU

The current valid published versions is marked in **bold.**

Content

2 Overview

2.1 Roles and instruments of the accreditation infrastructure

2.1.1 National Accreditation Body (NAB)

The National Accreditation Body (NAB) is an authoritative body in the sense of clause 4.7 of ISO/IEC 17000, which has been mandated by the WTO member state in which it is based to carry out accreditation in the sense of clause 7.7 of ISO/IEC 17000.

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

According to Section 1 of the accreditation body act (AkkStelleG), Section 1 of the accreditation body's regulation on fees (AkkStelleGBV) in conjunction with Regulation (EC) 765/2008, the German Accreditation Body is the competent authority in Germany for the accreditation of conformity assessment bodies.

2.1.3 Conformity assessment body (CAB)

A conformity assessment body is a legal entity as defined in clause 4.6 of ISO/IEC 17000 that performs conformity assessment activities as defined in clauses 4.3 to 4.5 of ISO/IEC 17000, excluding accreditation.

2.1.4 Customer of the conformity assessment body (Customer)

A client of a conformity assessment body is a person or a legal entity that is object of conformity assessment or that provides the object of conformity assessment as defined in clause 4.2 of ISO/IEC 17000 and has an interest in the outcome of the statement.

2.1.5 Attestation

A statement by a conformity assessment body (CAB) as defined in clause 7.3 of ISO/IEC 17000 is that the object of conformity assessment as defined in clause 4.2 of ISO/IEC 17000 fulfills specified requirements or expectations as defined in clause 5.1 of ISO/IEC 17000.

2.1.6 Electronic attestation (eAttestation)

An electronic attestation is an electronically provided statement of a conformity assessment body (CAB) in the sense of clause 7.3 of ISO/IEC 17000 based on an electronic file, e.g. a PDF or a machine-readable format such as XML. If declarations of conformity are provided digitally (eAttestation), the conformity assessment body shall be able to guarantee the integrity and authenticity of the electronic confirmation. This is done by the technical means of an advanced seal with a qualified certificate that complies with the DAkkS certificate profile outlined in this TSPS.

2.1.7 Accreditation symbol and national authority emblem

An accreditation symbol in the sense of clause 3.12 of ISO/IEC 17011 is issued by an accreditation body (NAB) and used by conformity assessment bodies (CAB) on their attestations to indicate that

they are an accredited CAB. If the accreditation body (NAB) operates on a sovereign basis, as do all national accreditation bodies within the meaning of Art. 2 No. 11 of Regulation (EC) 765/2008 in the European Union and the EEA, the symbol may be associated with or represent a national authority emblem.

2.1.8 Digital accreditation symbol and digital national authority emblem

If a digital accreditation symbol with or without a digital national authority emblem as defined in clause 3.12 of ISO/IEC 17011 is provided electronically to the accredited conformity assessment body (CAB), the accreditation body (NAB) shall be able to guarantee the integrity and authenticity of the accreditation symbol with or without a national authority emblem in accordance with clause 4.3.3. lit. a) and c) as well as clause 4.3.5 of ISO/IEC 17011. The accreditation body shall be able to guarantee the integrity and authenticity of the accreditation symbol with or without the authority emblem, because the symbol is associated with the presumption of conformity according to Art. 11 Para. 2 of Regulation (EC) 765/2008. This is done by cryptographic methods to protect the certificates under the responsibility of a qualified trust service such as explained in Chap. 2.3.1.

2.2 Overview of the architecture for the eAttestation

The customers of an accredited conformity assessment body (**CAB**) are the users of the statement of conformity **(attestation),** which are marked with the accreditation symbol. This is due to the fact that statements of conformity issued by accredited conformity assessment bodies are mutually recognized in the European internal market as well as in the EEA according to Art. 11 Par. 2, 2nd alternative VO (EC) 765/2008. Mutual recognition can also be used internationally via the accreditation symbol on the basis of existing reciprocity agreements of the TBT Agreement of the WTO.

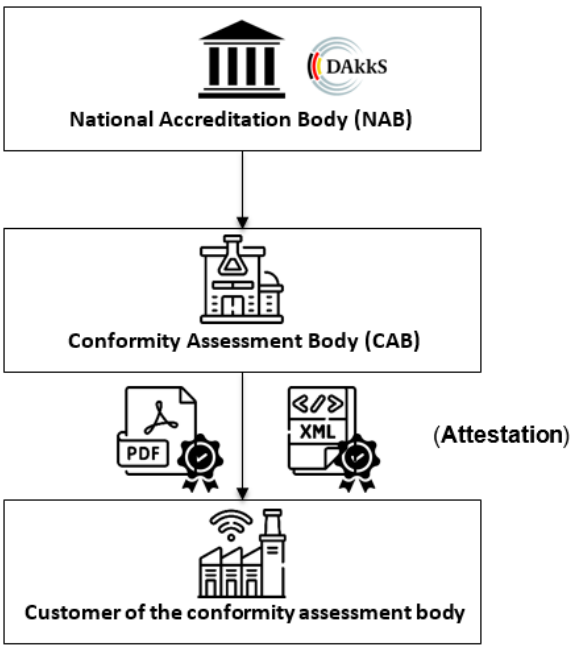

Figure 1: Roles in the field of accreditation - own illustration DAkkS

Accredited conformity assessment bodies carry out conformity assessment activities for which they issue **attestations** with regard to an object of conformity assessment.

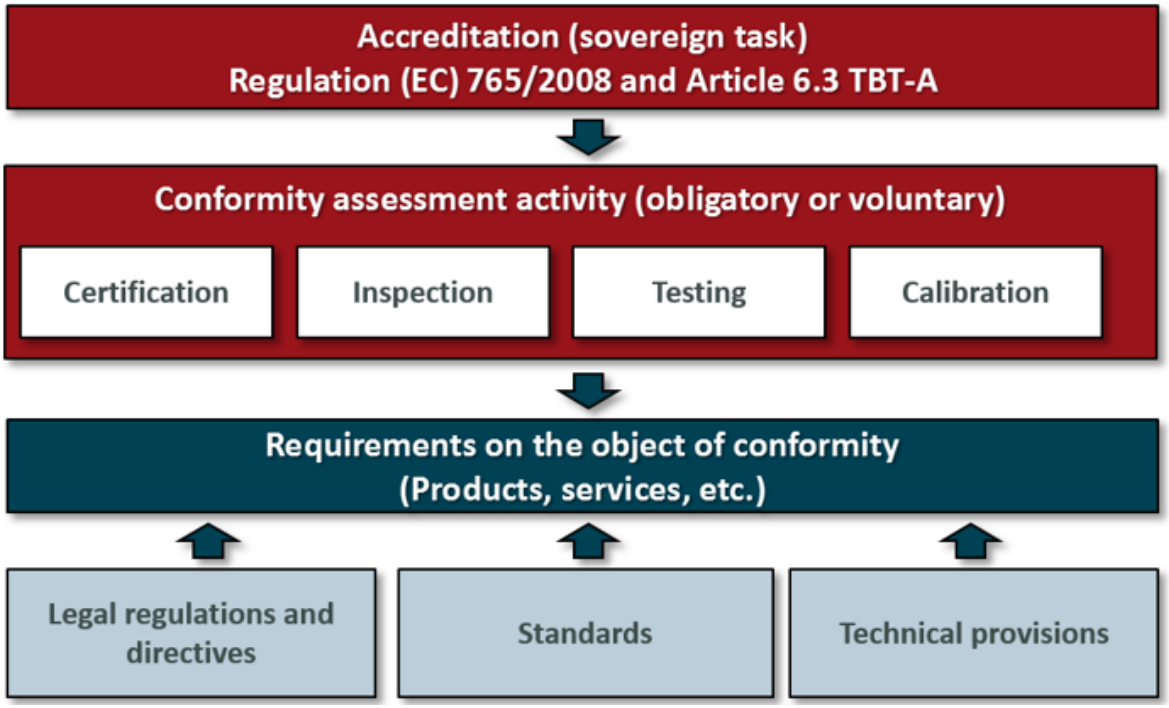

Figure 2: Context of accreditation - own illustration by DAkkS

The digitalization of the international quality infrastructure requires that conformity assessment bodies can provide their attestations electronically, e.g. as PDF document or as machine-readable format such as XML. To ensure the above requirements, DAkkS, as the German national accreditation body, supports the development of a public key infrastructure (**PKI**) by a qualified trust service as described in ch. 2.3.1. In this context, DAkkS operates a special process within this PKI adapted to the requirements of accreditation for issuing certificates with a digital accreditation symbol and a digital national authority emblem.

A conformity assessment body (CAB) accredited by DAkkS can obtain access to this PKI. As a result, the CAB receives an advanced seal with a qualified certificate and its corresponding cryptographic key from the qualified trust service. This enables the accredited conformity assessment body to digitally seal its attestations (e.g. certificates, result reports, laboratory reports, calibration certificates, inspection reports, etc.) and thereby confirming that the electronic document was issued by an accredited CAB as legal person and ensuring certainty of the document's origin and integrity. The advanced seals that comply with the DAkkS certificate profile are only issued to accredited conformity assessment bodies. Those seals contain a digital accreditation symbol and a national authority emblem which shows the accreditation status of the issuing conformity assessment body. Therefore, those seals can support highly digitized and fully automated processes with machine-readable and machine-interpretable contents and ensure the electronic exchange of trustworthy attestations in the global supply chain and between actors of the international quality infrastructure.

2.3 Assignment of roles and entities in the PKI

2.3.1 Trust service provider (TSP)

For the purposes of this document, a trust service provider (TSP) is a qualified trust service provider as defined in Art. 3 No. 20 of 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 (eIDAS), which provides one or more qualified trust services and which has been granted qualified provider status by the supervisory authority.

2.3.2 D-Trust GmbH (CA and RA)

As a TSP, D-Trust GmbH is commissioned by DAkkS to create an advanced seal with a qualified certificate that contains attributes of accreditation confirmed by DAkkS. As a trust service provider, D-Trust GmbH assumes the following roles in particular:

- Registration Authority (RA)

  Registration Authorities (RAs) are institutions of the PKI. The RA is responsible for verifying the identity and authenticating users of the PKI and verifies and validates certificate requests of users (e.g. requests for advanced seals).

- Certification Authority (CA)

  The certification authority (CA) grants final approval of certificates and issues them. It also provides revocation information (certificate revocation list, CRL).

D-Trust checks the organization data contained in the certificate applications (e.g. for advanced seals) against publicly available registers. In doing so, D-Trust takes over the organization validation. The check is carried out in accordance with [ETSI_EN_319_411-1], chapter 6.2.2.

The issued advanced seals are based on qualified seal certificates without storage on a hardware device, the so called QESCD (qualified[1] electronic signature/seal creation device) in the sense of eIDAS [Art. 3 para. 30 eIDAS Regulation].

The commissioned TSP is obliged to create qualified certificates considering the requirements of the eIDAS regulation. If the DAkkS-specific certificate profile with accreditation attributes and its corresponding OIDs is applied for advanced seals with qualified certificates, it is compulsory for DAkkS to follow the outlined requirements of this document (DAkkS_TSPS).

2.3.3 DAkkS certificate profile for electronic seals

The DAkkS certificate profile, as described in this document (DAkkS_TSPS), can only be used by conformity assessment bodies accredited and supervised by DAkkS as electronic seal end user group. The CA of the TSP enables the provision of electronic seals based on the product of D-Trust GmbH

[1] In this case, <<qualified>> means that the cryptographic key and the certificate are stored on a smartcard (hardware).

"Qualified Seal ID". The seals described in this document with its specific certificate profile are an extension of the product “Qualified Seal ID” and are created as advanced seal with qualified certificate (Art. 3 Para. 26, 30 eIDAS regulation). Other features of the PKI are set out in document [DTR_CSM_PKI] and referenced documents (see ch. 13).

2.3.4 Certificate holder within the PKI (Subscriber)

Within the DAkkS certificate profile, certificate holders or rather subscribers are natural persons as authorized signatories for the conformity assessment body. The subscriber acts as a legal representative to apply for the seal on behalf of the legal entity. As subscriber, they have the role of "certificate holder" as defined in the [DTR_TSPS] of D-Trust GmbH and referred documents (see ch. 13), and thus the following rights, which they can delegate to other natural persons within their organization:

- Application for advanced seals with qualified certificates with the specific accreditation attributes
- Requesting the revocation of an issued seal

2.3.5 End users within the PKI

End users of the electronic seal based on the DAkkS certificate profile are always legal entities and are always members of the user group as mentioned in ch. 2.3.3. The information in the issued electronic seals always refer to the conformity assessment body as the legal entity. End users receive electronic seals with qualified certificates from the certification authority (CA). The application is restricted to authorized end users who are legal entities and who are listed or entitled to be listed in the official database of accredited bodies, as accredited conformity assessment bodies. Accredited conformity assessment bodies have the following rights within the meaning of [DTR_TSPS], chapter 1.3.3 of D-Trust GmbH and referenced documents (see ch. 13):

- Application of the provided advanced seal with qualified certificate as well as the issuance of the cryptographic keys for the sealing of documents with the advanced seal according to the DAkkS-TSPS.

2.3.6 DAkkS as technical representative of the conformity assessment body

The certificate holder authorizes DAkkS for the application as well as revocation process in order to make declarations and take actions towards the TSP on behalf of the certificate holder (= technical representative). The scope is described in more detail in an authorization document. The authorization of the national accreditation authority enables the validity of the accreditation specific attributes. In the application process of an advanced seal the national accreditation authority checks and confirms the accreditation specific attributes prior to the release of the electronic seal to the certificate holder. This also includes the right of the national accreditation authority to immediately revocate the electronic seal based on the DAkkS certificate profile if the requirements of this document (DAkkS_TSPS) doesn’t apply to the certificate holder anymore.

2.3.7 Relying parties of the PKI

Relying parties are natural persons or legal entities that only verify the seals issued according to the DAkkS certificate profile in order to check the authenticity and integrity of sealed documents. They are no certificate holders in the sense of this document. Typical relying parties are customers of accredited conformity assessment bodies (certificate holders) and who are interested in the verification of the seal according to the DAkkS certificate profile issued to the certificate holders.

2.3.8 Other users of the PKI

Other users of the PKI that do not have any contractual obligations towards the TSP and are also not included in the protective scope as a customer of the certificate holder for verification purposes are not considered in this TSPS.

3 Objective of the DAkkS-TSPS

Advanced seals with qualified certificates that comply with the DAkkS certificate profile are issued by the TSP through the issuing CA with the designation: "D-TRUST CA 5-22-2 2022". The associated root CA is "D-TRUST Root CA 5 2022".

This DAkkS-TSPS supplements the requirements applied by the trust service provider (TSP) in the provision of its services. In addition to this document, the certificate policy (CP) of D-Trust applies in particular, which regulates the certification process throughout the entire life cycle of certificates issued, starting with the authentication and registration of PKI participants, through the issuing and application of certificates to the renewal, revocation or expiry of certificates. The DAkkS-TSPS and the CP of D-Trust are legally binding. They contain statements on obligations, warranty and liability for the participants of the PKI that use advanced seals according to the DAkkS certificate profile. Unless explicitly stated, no contractual assurances or guarantees in the legal sense are made on the basis of the DAkkS-TSPS and the CP of D-Trust. Knowledge of the certification procedures and rules described in this TSPS, as well as of the legal framework, allows users and relying parties in the PKI to build trust in the PKI and to make decisions about the suitability of the level of trust and security provided by the PKI for their applications.

4 Hierarchy of documents in the PKI

This trust service practice statement (TSPS) of DAkkS refers to the applicable documents of D-Trust GmbH as TSP. The following diagram shows the relationship of this document to the documents of the TSP and all documents of the TSP that are relevant for the DAkkS certificate profile. The documents of the TSP are available at https://www.d-trust.net/en/support/repository.

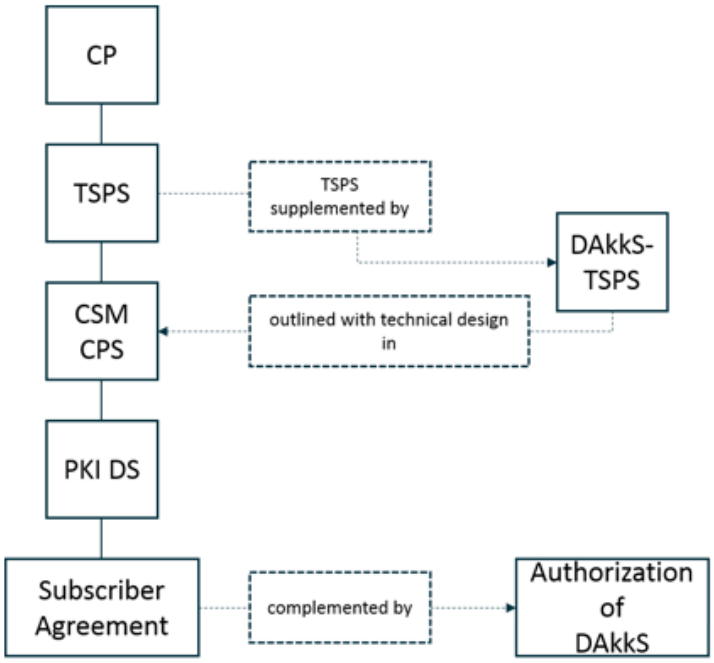

Figure 3: Hierarchy of documents in the PKI

This TSPS takes into account the following standards:

- 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.

Each advanced seal with qualified certificate according to the DAkkS certificate profile issued from the PKI complies with the X.509v3 standard. Regarding the certificate section **extensions**, the section policies (2.2.29.32) mentions the relevant documents that apply to the issued advanced seal with qualified certificate that complies to the DAkkS certificate profile:

OID	Value	Note
0.4.0.149112.1.1	-	Part of the basic product: 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	Part of the basic product: D-Trust-specific marking for seals with qualified certificates without qualified signature

		creation device, according to 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 to DAkkS-TSPS
	User Notice National authority emblem (OID: 1.3.6.1.4.1.59749.3.1): https://accreditationauthority.dakks.de/authoritiesemblem.pdf	URL to **user notice** with the national authority emblem

5 Usage of the electronic seal

The usage of electronic advanced seals with qualified certificates according to the DAkkS certificate profile is restricted to the sealing of statements of conformity, especially to attestations of accredited conformity assessment bodies (eAttestation). All advanced seals with qualified certificates issued according to the DAkkS certificate profile contain the extension ("**AdditionalInformation**", see [COMMONPKI], chapter 2.1 and table 29f as referenced in ch. 13 of this document) and a specific restriction ("**Restriction**", see [COMMONPKI], chapter 2.1 and table 29e as referenced in ch. 13 of this document).

These specific extensions has to be filled in by the certificate holder applicant with the following values:

Extension	Value
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 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").
Restriction	The application of the sealing key is limited to the sealing of the attestation (statement of conformity).

6 Cryptographic design of the PKI

The advanced seals with qualified certificates according to the DAkkS certificate profile originate from a CA of D-Trust. The CA of D-Trust GmbH currently used is:

- D-TRUST CA 5-22-2 2022, RSA 4096 key, certificate signature SHA512 / RSA-PSS

The corresponding root CA is called "D-TRUST Root CA 5 2022".

The cryptographic keys corresponding to each issued seal are generated by the certificate service manager (CSM) of D-Trust; currently these are RSA keys with a length of 4096 bits. Procedures after the delivery of the generated keys can be found in the document [DTR_TSPS], section 6.2.10 "Destruction of private keys".

7 Special features for the procedure in the PKI

The following provisions apply to the processes of applying for and revoking certificates according to the DAkkS certificate profile, as a specification of the CP and CPS of D-Trust.

7.1 Special features for the application

7.1.1 Limited eligibility to apply

Only legal entities within the meaning of DAkkS Rule R 17011 are eligible to apply for electronic advanced seals with qualified certificates using the DAkkS certificate profile. The issuance of such seals to natural persons is excluded. Furthermore, applications from legal entities will only be accepted if the legal entity is listed in the official database of accredited bodies of DAkkS with at least one accreditation or is entitled to the listing and the accreditation is not suspended.

7.1.2 Obligation of the applicant by the DAkkS

The applicant is contractually obliged to comply with this TSPS, including all documents of the TSP as presented in chapter 4, as part of the registration process. The acceptance of the terms and conditions is documented.

7.2 Special features of the national accreditation body (NAB) authorization

For each application for the issuance of an electronic seal that contains a digital accreditation symbol as attestation by a national accreditation authority for the accreditation of the conformity assessment body (CAB), it is necessary to grant the national accreditation authority, the rights as technical representative. The NAB delegates this role to its officials and in this role can, for example, release electronic seals to accredited CABs but also demand the immediate revocation of the electronic seal vis-à-vis D-Trust GmbH if the accreditation is suspended or withdrawn.

This shall not affect the right of the conformity assessment body itself to request the revocation of its electronic seal at any time.

7.3 Special features for identification and authentication

The procedure during the registration of the applicant contains at least the following steps:

1. Accreditation procedure:
   Procedure and notification of an accreditation, verification of the application data for the use of a "digital accreditation symbol" by an accredited CAB

2. Dispatch of contract documents, notifications and authorization for the usage of the electronic seal within the PKI,
3. Check of the authorization, identification of the applicant as a legal entity and of the authorized signatory
4. Empowerment of certificate holders by DAkkS operators within the PKI
5. Confirmation of accreditation (occupational attribute) by DAkkS operators when a certificate holder applies for an electronic seal in the PKI

1. Accreditation procedure

In its function as national accreditation authority, DAkkS verifies that the application for accreditation is submitted by a legal entity claiming to be a conformity assessment body. According to Section 1 of the accreditation body act (AkkStelleG) in conjunction with Regulation (EC) 765/2008, DAkkS is the competent authority in Germany for accreditations of conformity assessment bodies and grants the status as accredited conformity assessment body by sovereign administrative act according to the German Administrative Procedure Act (Verwaltungsverfahrensgesetz (VwVfG)). The accreditation is confirmed by official confirmation. This is preceded by a review of the identity and competence of the conformity assessment body for the requested conformity assessment activities in accordance with ISO/IEC 17011 and entails continuous monitoring of the accredited body and its competence by the national accreditation authority.

A conformity assessment body shall submit an application to the national accreditation authority, DAkkS, for the use of a "digital accreditation symbol" that includes the issuance of an advanced seal with a qualified certificate. Subsequently, DAkkS checks whether the applicant is listed in its **official database of accredited bodies** or is entitled to the listing in this database (accreditation decision has been made). **Only in case of a successful check by DAkkS, the use of a "digital accreditation symbol" is permitted,** otherwise it is rejected**.**

2. Dispatch of contract documents

The contractual documents necessary for issuing an electronic seal as well as the authorization document are sent by post to the physical address of the registered office of the conformity assessment body. This verifies again the accessibility and the correctness of the information on the legal entity.

3. Check of the authorization

After the conformity assessment body has returned the authorization document to DAkkS by e-mail or post, DAkkS operators identified towards the TSP first check whether the document is submitted in written form (§ 126 German Civil Code (BGB)/ § 126a German Civil Code (BGB)) including the company stamp. It is also checked by those DAkkS operators whether the document has been signed by an **authorized signatory of** the legal entity (**conformity assessment body**). The identity of the authorized signatory was already checked in the administrative procedure via an extract from the

commercial register and is checked again at this point. The commercial register is based in each case on a notarial certification of the application, which requires physical identification with official documents towards the competent notary. In case of legal entities that are not capable of being registered within the commercial register, the identity of the authorized signatory is verified and confirmed by the national accreditation authority based on the submitted legally valid documents within the administrative procedure (e.g. articles of association; powers of attorney; etc.). Those documents are checked again as part of the authorization procedure required here. It is ensured and, if necessary, officially certified that the signatory is the authorized signatory (e.g. according to the commercial register) of the authorizing conformity assessment body. The TSP will not initiate any investigation into the authenticity of the aforementioned documents.

In case of deviations, the process shall be repeated or a remote identification procedure [DTR_CSM_CPS] approved by the TSP shall be used to verify the identity of the authorized signatory.

4. Empowerment of certificate holders

After the successful verification of the organization and its authorized signatory by means of official register entries (commercial register entries, etc.) as well as the confirmation of the application eligibility for an electronic seal (database of accredited bodies), the operators of the DAkkS (DAkkS officials) in their role as "technical representatives" of the conformity assessment body (CAB) create an organization account for the CAB within the PKI. This enables the authorized signatories - or other natural persons to whom the task has been delegated - to fulfil their role as "certificate holder".

5. Confirmation of accreditation in PKI

The authorized signatory or other natural persons to whom the task has been delegated can then submit their electronic seal application within the PKI. Subsequently, the DAkkS operators confirm the certificate holder's application for an electronic seal in their role as the accreditation attribute-confirming national accreditation authority.

7.4 Special features for revocation

Revoking certificates of electronic seals marks these as invalid from the time of revocation. A revocation can neither be lifted nor reversed. Such certificates cannot be revoked with retroactive effect either. It is not necessary to revoke certificates after their validity has expired.

In particular, the following special features apply:

DAkkS is obliged to ensure that it is able to revoke an electronically provided accreditation symbol with or without a national authority emblem within the meaning of clause 3.12 of ISO/IEC 17011 at any time (cf. Art. 11 Para. 2 of the Regulation (EC) 765/2008; Section 4 Para. 4 Sentence 2 of the Accreditation Symbol Ordinance - SymbolVO; clause 4.3.3. lit. a) and c) as well as clause 4.3.5 of ISO/IEC 17011).

Therefore, DAkkS at its discretion is able to revoke a certificate based on the DAkkS certificate profile within the CSM of the TSP at any time if the requirements to hold a certificate aren't fulfilled by a certificate holder anymore or if a breach of the requirements of this TSPS occur.

8 Verification on the status of the validity of the digital accreditation symbol

The digital accreditation symbol contained in the advanced seal with a qualified certificate is only valid if **(1)** the signature check of the advanced seal with a qualified certificate (cryptographic integrity) is valid, **(2)** the validity period of this advanced seal with a qualified certificate has not been exceeded, **(3)** the revocation status of the electronic validity query in relation to the reference time of the seal creation according to chapter 8.3 of this document (DAkkS_TSPS) has yielded the result "valid", **(4)** the advanced seal with a qualified certificate was issued by the CA "D-TRUST CA 5-22-2 2022" and the certification path refers to the root CA "D-TRUST Root CA 5 2022" (trust anchor) currently in use and **(5)** the advanced seal with a qualified certificate contains the OID 1.3.6.1.4.1.59749.1 as reference to the digital accreditation symbol with national authority emblem in the "Admission" area.

8.1 Step 1: Signature verification (cryptographic integrity)

The X.509v3 certificate on which the advanced seal is based is signed with the private key of the issuer (CA) of the certificate within the PKI. The signature can be verified by means of the associated public key. The requirements of the standard: "BSI TR-02103 X.509 certificates and certification path validation" based on RFC 5280 must be complied with for certificates fulfilling the DAkkS certification profile. If the signature check fails, the entire check is negative.

8.2 Step 2: Validity period

It must be checked whether the current time of the signature check is within the validity period of a certificate. Therefore, the check of the validity period of the certificate is necessary. The validity of a certificate ends with the expiry date noted in the certificate in the field "valid until".

8.3 Step 3: Revocation status of the validity query via OCSP or CRL

The status request service of the TSP is available via the OCSP protocol. The service is specified under the URL in the certificate field "AuthorityInfoAccess". The formats and protocols of the services are described in section 7 of the D-Trust-TSPS [DTR_TSPS]. The system time of the OCSP responder is synchronized daily with the German DCF77[2] time signal and reliable time servers (NTP) on the Internet. The TSP ensures that the status request service is available 24 hours a day, 7 days a week

[2] In other regions, other well-known official time services are for example MSF in Great Britain (60 kHz), France Inter in France (162 kHz), as well as the station groups RWM in Russia (4,996 MHz, 9,996 MHz und 14,996 MHz), WWV, WWVB, WWVH in the US (60 kHz; 2,5, 5, 10, 15 und 20 MHz) and until 2011 HBG in Switzerland (75 kHz).

and has an availability of 99.95%. The TSP ensures that in the event of a malfunction, the downtime is a maximum of four hours.

Alternatively, revocation lists (CRL) are offered by the TSP; the URL of the revocation list distribution point is located in the certificate field "CRLDistribution Point". The regulations of the TSP that are referenced in its PKI documents ([DTR_CP], [DTR_CSM_CPS], [DTR_TSPS]) apply.

8.4 Step 4: Validation of the certification path to the trust anchor

Steps 1 to 3 are carried out in the certification path of the issuer certificate of the certificate to be verified until the valid root CA "D-TRUST Root CA 5 2022". This is considered a trust anchor for DAkkS purposes. If a signature check fails in the certification path, the entire check is negative.

8.5 Step 5: Digital national authority emblem

In the section **extension**, parse the area "Admission" OID: "1.3.36.8.3" and read out the area "Admission Authority". The registered ID "1.3.6.1.4.1.59749.1 {= DAkkS accreditation symbol}" must be mentioned there. The value of the OID "1.3.6.1.4.1.59749.1" is the machine-readable equivalent of the accreditation symbol with the DAkkS national authority emblem and indicates that the body named in the "Subject" (certificate holder) is accredited.

The certificates unfold their meaning as digital national authority emblem if the following structure is found in the section **extension admission** (see [COMMONPKI], section 2.1, table 29b as referenced in ch. 13 of this document):

- The OID 1.3.6.1.4.1.59749 is the reference to the "Admission Authority"
- Within the structure "ContentsOfAdmission", DAkkS is identified as Admission Authority by the DirectoryString "C=DE, O=Deutsche Akkreditierungsstelle GmbH (DAkkS)"
- Within the structure "ProfessionInfos" as "ProfessionItem" the text "DAkkS accredited conformity assessment body" can be found as well as for "Profession OID" the OID "1.3.6.1.4.1.59749.1" representing the DAkkS accreditation symbol.

9 Verification of sealed attestations (eAttestations) from conformity assessment bodies

When checking sealed attestations (eAttestations), the time of the seal creation (application of the seal on the document) is considered the reference time for the signature certificate check. Further information on the defined issuer CA can be found in a machine readable format (XML) on the EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).

10 Information on the scope of accreditation

10.1 Step 1: Read out the "Subject-Serialnumber"

The X.509v3 certificate contains in the section >Subject< the attribute "SerialNumber" from [ITU-T-X.520]. This attribute “SerialNumber” contains the unique >registration number of the accreditation certificate< to identify the accreditation procedure of the conformity assessment body (CAB).

The value has at least 22 characters, which shall be structured as shown below. The value can have a maximum of 64 characters.

The first 22 digits of the value have the following meaning:

AAAAAAA-CC-XX-YYYYY-ZZ-NN

AAAAAAA: max. 7 digits for short name of the NAB (e.g. DAkkS00)

CC: two digits for the ISO code of the WTO country from which the NAB has been authorized and in which it has its headquarters (e.g. DE)

XX: two digits for the abbreviation of the accreditation activity

For DAkkS, this would be:

BB	Biobanks
IS	Inspection body
K0	Calibration laboratory
ML	Medical Laboratory
PL	Testing laboratory
EP	Proficiency testing provider
RM	Reference material manufacturer
ZE	Certification body for products, processes and services
ZM	Certification body for management systems
ZP	Certification body for persons
VS	Validation or verification body

YYYYY: five digits for the sequential identification number (customer number) to identify the legal entity of the conformity assessment body in the NAB database

ZZ: two digits for a consecutive number of the conformity assessment body indicating several independent accreditation procedures within one accreditation activity

NN: Further two digits for specifications of the competent NAB. At DAkkS, these digits are used to clarify the registration number of an accreditation certificate as a unique

identification number of an accreditation certificate (overall accreditation certificate and partial accreditation certificate) and its valid annex. If there are no partial accreditation certificates for an accreditation procedure but only one overall accreditation certificate, "NN" = "00".

An example for the registration number of the applicable certificate is: DAkkS00-DE-PL-19516-01-00

10.2 Step 2: Database of accredited bodies

With the registration number of the accreditation certificate included in the X.509v3 certificate as attribute “SerialNumber”, the certificate holder within the PKI can also be found via the official database of accredited bodies provided by the national accreditation body. This can be accessed at https://www.dakks.de/en/accredited-bodies-search.html.

The current valid scope of accreditation of an accredited CAB is displayed there on a daily basis.

11 Graphical overview of the certificate profile

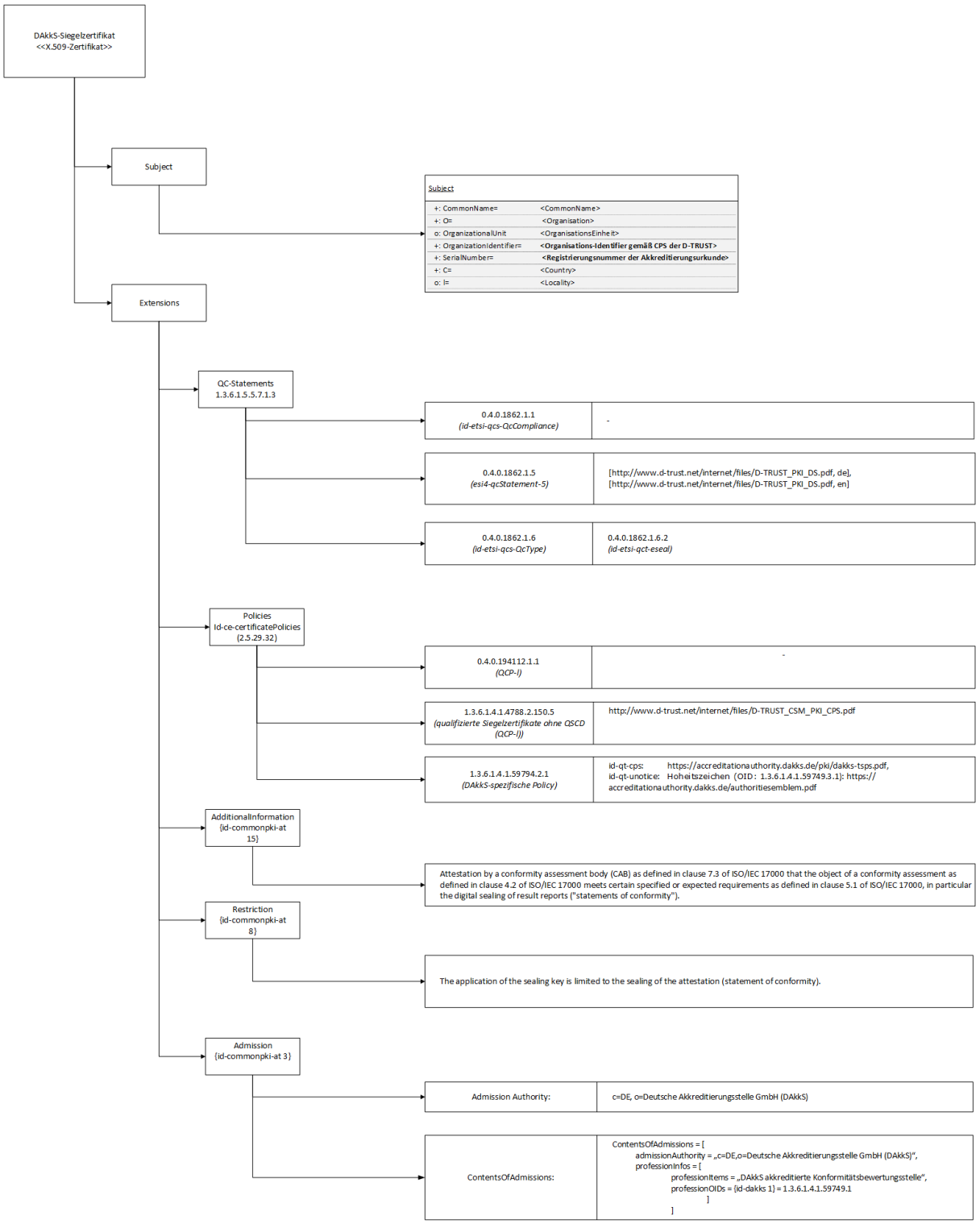

Figure 4: Certificate profile based on TSP specification document for DAkkS-specific advanced seal with a qualified certificate

12 Certificate profile

Extract from a sample certificate tree

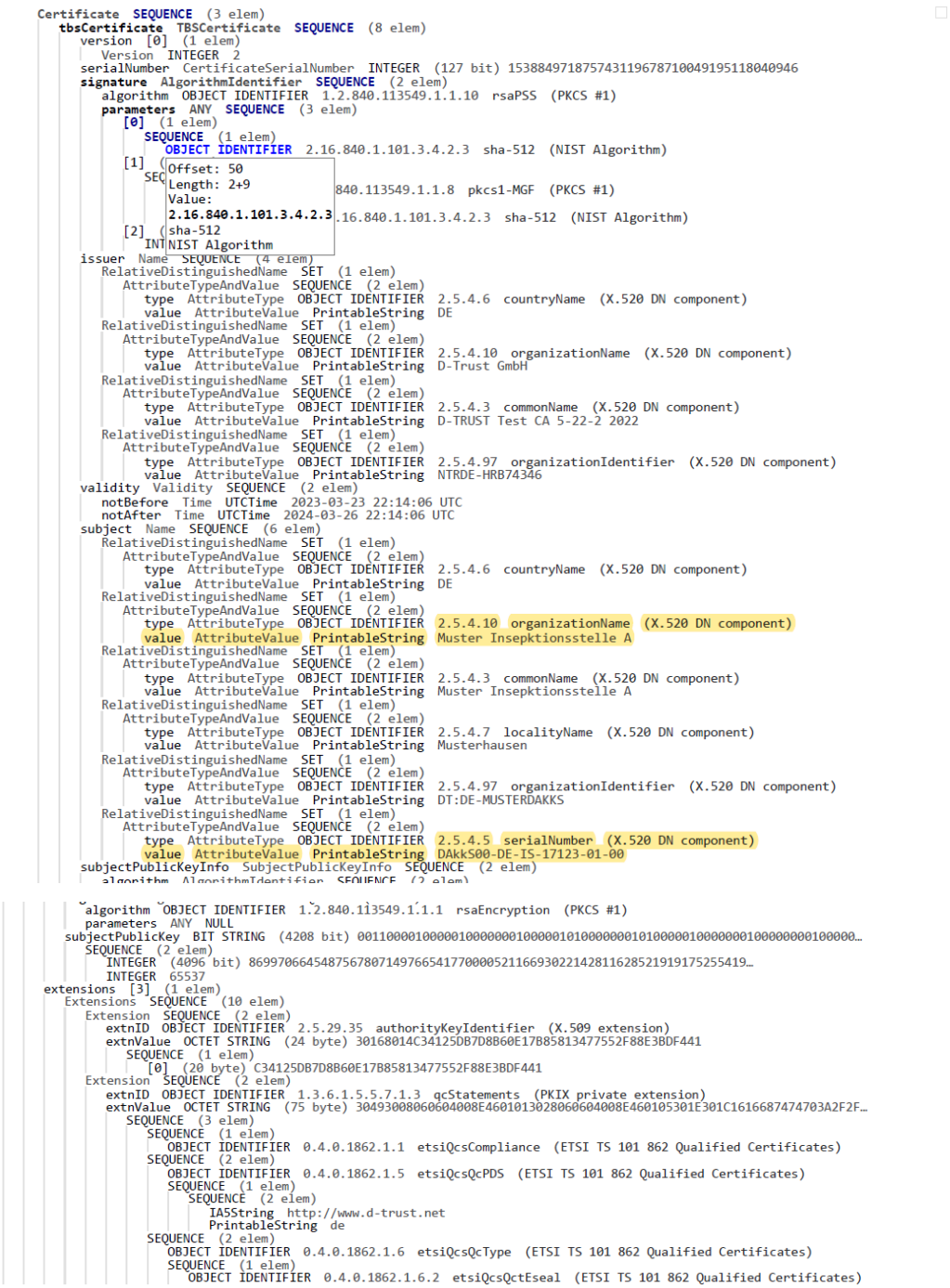

Figure 5: Extract of a sample of an advanced seal with a qualified certificate based on DAkkS certificate profile

13 Referenced documents

13.1 Referenced documents for PKI

The following table contains the names of the documents referenced in this document and the development status of these documents correlating with this version.

[Source]	Publisher (publication date): Title	Version	Status (date)
[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	2.3.1	05/2021

	and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.		
[DTR_CP]	D-Trust (2023): Certificate Policy (CP) of 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 of the D-TRUST CSM PKI	3.8	14.11.2022
BSI TR-02103: X.509	BSI (2020): BSI TR-02103 X.509 certificates and certification path validation	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 Referenced documents for accreditation and conformity assessment

The following table contains the documents referenced in the present document with regard to accreditation and conformity assessment as well as the development status of these documents correlating with the present version of this document.

[Source]	Publisher (publication date): Title	Version	Status (date)
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	Federal Republic of Germany (2009): Law on the Accreditation Body (Accreditation Body Act - AkkStelleG)	-	31.07.2009
AkkStelleGBV	Accreditation body regulation on fees (AkkStelleGBV)	-	19.6.2020

SymbolVO	Ordinance on the Design and Use of the Accreditation Symbol of the Accreditation Body (Accreditation Symbol Ordinance - SymbolVO)	-	15.12.2009

List of figures

Picture credits for Figure 1

NAB Icon	Quality free icon from Freepik at www.flaticon.com
CAB Icon	Lab free icon by Freepik at www.flaticon.com
PDF Icon	PDF free icon from Freepik at www.flaticon.com
XML Icon	Xml File free icon from Freepik at www.flaticon.com
Quality Icon	Quality free icon from Freepik at www.flaticon.com
Customer Icon	Factory free icon from Freepik at www.flaticon.com