eIDAS Certification of Trust Services

datenschutz cert GmbH
Version 1.0

datenschutz cert

Contents

Document History

Version	Date	Changes	Reason for change	Editor
1.0	10.12.2021		Initialisation	SM

Document Management

Status	Process Document Owner	Version
Final	Dr. Sönke Maseberg	1.0

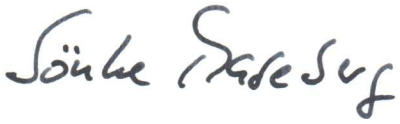
1. Certification of Trust Services

The eIDAS Regulation applies to trust services across the EU. The eIDAS regulates the legal framework for electronic signatures, electronic seals, electronic time stamps as well as electronic registered delivery services and certificate services for website authentication. The qualifies trust services providers must be verified and certified with the qualified trust services.

datenschutz cert GmbH is accredited by DAkkS, and can therefore issue certificates in accordance with eIDAS.

This document describes the procedure for the award of certificates for qualified trust service providers and the qualified trust services they provide which fall within this accredited area. It is intended to provide all necessary information to companies wishing to have certification carried out by datenschutz cert GmbH.

Bremen, 10.12.2021



Dr. Sönke Maseberg
CEO
datenschutz cert GmbH

2. eIDAS

eIDAS stands for "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 regulates electronic identification means for natural and legal persons as well as for trust services. In doing so, the eIDAS provides the legal framework for electronic signatures, electronic seals, electronic time stamps as well as electronic registered delivery services and certificate services for website authentication.

The eIDAS includes the following detailed services:

- Creation
  - Qualified certificates for electronic signatures
  - Qualified certificates for electronic seals
  - Qualified certificates for website authentication
  - Qualified electronic time stamps
  - Qualified electronic signatures
  - Qualified electronic seals
- Verification and Validation
  - Qualified electronic signatures, electronic seals, electronic time stamps and accompanying qualified certificates
  - Qualified certificates for website authentication
- Preservation
  - Qualified electronic signatures, electronic seals or accompanying qualified certificates
- Electronic registered delivery services
  - Electronic services

Website certificates were already called for via the CA/Browser (CAB)-Forum: to date, those who wished to have their certificates pre-installed in the browser and operating systems, had to generate a corresponding certification. These regulations have now also been included in the eIDAS.

3. Criteria

ETSI standards are used for the testing and certification of trust service providers and the trust services they offer:

- 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: Policy requirements for Trust Service Providers issuing EU qualified certificates
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing time-stamps
- ETSI EN 319 521: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI TS 119 511: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- ETSI EN 319 531: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers

4. Conformity Assessment

4.1. Cycles

Each certification procedure consists of the following phases:

- Initial Assessment;
- Surveillance (1 year after initial assessment);
- Re Assessment (2 years after initial assessment).

4.2. Work Items

According to international rules and best practice conformity assessment is carried out as a project in four phases:

- Phase 1: Acceptance of proposal and submission of documentation

  The project starts with acceptance of the proposal by the customer. After the proposal is accepted datenschutz cert GmbH will assign an identification number (ID) to the project. Any further information exchange shall refer to that ID. Once an ID is assigned the customer's duty is to submit complete documentation describing the Trust Service(s) provided by the TSP.

- Phase 2: Stage 1 – check of documentation provided

  After reception of complete documentation describing the Trust Service(s) datenschutz cert GmbH will assess the documentation. In case the documentation submitted reveals major deficiencies or missing information datenschutz cert will prepare a report (Stage 1 Report) describing those findings. If provided, the Stage 1 Report shall contain a management review stating the overall result of the Stage 1 assessment and one or more further sections as required stating the details of the assessment. The Stage 1 Report will be sent to the customer.

- Phase 3: Audit and Stage 2 Report

  After phase 2 is finished (either by a Stage 1 Report or implicitly) datenschutz cert GmbH shall carry out an on-site audit at the premises of the customer where the service(s) is (are) delivered. The audit will check whether the service(s) is (are) operated as described in the documentation. Furthermore, it will assess whether all means applied – technical, personal, organizational, physical – are sufficient to fulfil the requirements of the applicable ETSI standards so that the service(s) is (are) delivered on a qualified level. The outcome of the audit shall be documented in a Stage 2 Report prepared by datenschutz cert GmbH and submitted to the customer.

  In case any major non-conformity is detected during the audit the customer may take appropriate means to overcome that non-conformity prior to finishing the Stage 2 Report.

- Phase 4: Preparation of CAR / surveillance report

  Preparation of the CAR / surveillance report by datenschutz cert GmbH will take place in parallel to preparation of Stage 1 and Stage 2 reports. In case the Stage 1 and Stage 2 Reports do not state any major non-conformity, maybe after every

enhancement necessary, the CAR / surveillance report shall state fulfilment of the requirements of Regulation (EU) 910/2014. Otherwise, it shall state any open issue, i. e. any requirement not fulfilled as well as the reason for that result. It shall be submitted to the customer. This will end the project.

4.3. List of Certificates

list of our awarded certifications can be found at: https://www.datenschutz-cert.de/zertifikatslisten. The list shows the applicant, the scope, the certificate ID and the validity of the certification.

4.4. Revocation, Suspension or Restriction of a Certificate

Conformity assessments and conformity assessment documents shall be withdrawn, suspended, withdrawn or restricted in accordance with the provisions of the respective regulations, standards and approval standards.

Certificates shall be restricted, suspended or withdrawn in particular if the contracting entity

- the requirements of the regulations, standards, approval standards and approval bodies or the generally recognised state of the art on which the conformity assessment is based change,
- the underlying conformity assessment document is no longer suitable to substantiate the conformity assessment,
- no approval was available for the conformity assessment,

The certification body shall inform the applicant of the reasons for the withdrawal of the certificate. In the event of withdrawal, the certificate published online via the certificate list at www.datenschutz-cert.de shall be set to the status as withdrawn and removed from the list after 4 weeks at the latest. The withdrawal of the certificate may also be published elsewhere.

4.5. Costs and Fees

Please contact us for an individual offer.

4.6. Form

If you are interested in certification, please contact us! You can also fill out the enquiry form, which contains the information that is important to us. You will find the form at: http://www.datenschutz-cert.de.

4.7. Terms and Conditions

Any service of datenschutz cert GmbH is delivered solely according to the terms and conditions of datenschutz cert: Allgemeine Geschäftsbedingungen and Konformitätsbewertungsordnung. For further information as well as for certifications lists, please, visit www.datenschutz-cert.de.

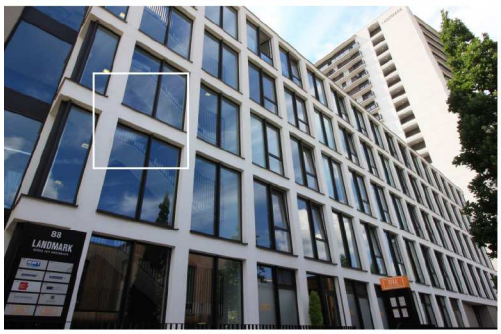
5. datenschutz cert GmbH

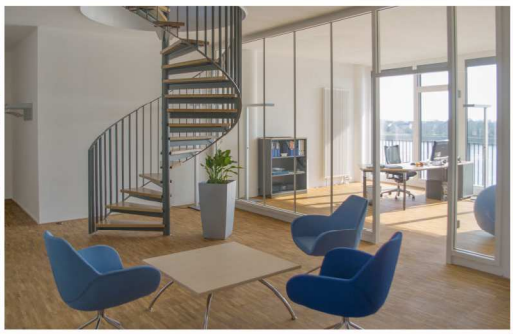
datenschutz cert GmbH provides conformity assessments in the fields of data protection and information security. The conformity assessments include evaluation of IT products and systems, auditing of processes and services as well as certification services according to international standards.

datenschutz cert GmbH is a subsidiary of datenschutz nord group. Legal office address is Konsul-Smidt-Str. 88a, D-28217 Bremen, Germany. CEO is Dr. Sönke Maseberg

datenschutz cert GmbH has proven competences as follows:

- datenschutz cert GmbH is a Deutsche Akkreditierungsstelle GmbH (DAkkS) accredited Confirmation Assessment Body under Regulation (EU) 910/2014 and, therefore, permitted to issue Conformity Asessment Reports according to European Standards as referenced by the European Commission.
- datenschutz cert GmbH is a Deutsche Akkreditierungsstelle GmbH (DAkkS) accredited Certification Body according to ISO/IEC 27006 and, therefore, permitted to issue internationally recognized certificated for ISO/IEC 27001 conformant Information Security Management Systems (ISMS).
- datenschutz cert GmbH is a Bundesnetzagentur (German Supervisory Authority) recognized Evaluation and Confirmation Body under German Law and Directive 1999/93/EC.
- datenschutz cert GmbH is a Bundesamt für Sicherheit in der Informationstechnik (BSI) licensed Evaluation Laboratory for IT Security Evaluations.









datenschutz cert GmbH

Headquarters
Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: (+49) 421 69 66 32 50

Further Site
Mainstraße 143
63065 Offenbach am Main
Tel.: (+49) 69 87 00 783 580

office@datenschutz-cert.de
www.datenschutz-cert.de

datenschutz cert