Certification program eIDAS of the Certification Body (CAB) (accredited area) of SRC Security Research & Consulting GmbH

Version 2.0 / 11.11.2022

Contents

1	Purpose	3
2	Scope of application and products covered	4
3	Certification process	11
4	Complaints and appeals	19
5	Norms	20
6	Annexes	22
7	Glossary	22

1 Purpose

The certification body of SRC Security Research & Consulting GmbH – short SRC – offers other companies certification of products, systems, services and processes in the field of information technology. In the following, the simplified term certification of products is used. Certification is carried out on the basis of normative documents such as legal regulations, standards or technical specifications, which define requirements for products. With certification by an independent third party, the commissioning companies (customers) have the opportunity to document that their products meet the specified requirements.

The certification body of SRC is accredited on the basis of DIN EN ISO/IEC 17065 for the certification of products in the areas of IT security and security technology. This document describes the certification scheme for the award of SRC certificates to qualified trust service providers and the qualified trust services they provide within the scope 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 Regulation).

The eIDAS certification program contains the following sub-programs for the certification of qualified trust services and trust service components:

1) Qualified service for the creation of qualified certificates for electronic signatures - without the need for the electronic signature creation data to reside in a qualified electronic signature creation device (QSCD) - in accordance with Art. 28 of the eIDAS Regulation,

    1a. Qualified service for the creation of qualified certificates for electronic signatures - without the need for the electronic signature creation data to reside in a qualified electronic signature creation device (QSCD) - with the option to manage the signature creation data on behalf of the signatory (remote signature),

2) Qualified service for the creation of qualified certificates for electronic signatures - with the requirement that the electronic signature creation data reside in a qualified electronic signature creation device (QSCD) - in accordance with Art. 28 and 29 of the eIDAS Regulation,

    2a. Qualified service for the creation of qualified certificates for electronic signatures - with the requirement that the electronic signature creation data reside in in a qualified electronic signature creation device (QSCD) - with the option to manage the signature creation data on behalf of the signatory (remote signature),

3) Qualified service for the creation of qualified certificates for electronic seals - without the need for the electronic seal creation data to reside in a qualified electronic seal creation device (QSCD) - in accordance with Art. 38 of the eIDAS Regulation,

    3a. Qualified service for the creation of qualified certificates for electronic seals - without the need for electronic seal creation data to reside in a qualified electronic seal creation device (QSCD) - with the option to manage seal creation data on behalf of the signatory (remote seal),

4) Qualified service for the creation of qualified certificates for electronic seals - with the requirement for the electronic seal creation data to reside in a qualified electronic seal creation device (QSCD) - in accordance with Art. 38 and 39 of the eIDAS Regulation,

   4a. Qualified service for the creation of qualified certificates for electronic seals - with the requirement for the electronic seal creation data to reside in a qualified electronic seal creation device (QSCD) - with the option to manage seal creation data on behalf of the signatory (remote seal),

5) Qualified service for the creation of qualified certificates for website authentication, in accordance with Art. 45 of the eIDAS Regulation,

6) Qualified service for the creation of qualified electronic time stamps in accordance with Art. 42 of the eIDAS Regulation,

7) Qualified validation service for qualified electronic signatures in accordance with Art. 33 of the eIDAS Regulation and / or qualified electronic seals in accordance with Art. 40 of the eIDAS Regulation,

8) Qualified preservation service for qualified electronic signatures in accordance with Art. 34 of the eIDAS Regulation and / or qualified electronic seals in accordance with Art. 40 of the eIDAS Regulation,

9) Qualified service for the delivery of electronic registered mail in accordance with Art. 44 of the eIDAS Regulation,

10) Trust service component for verifying the identity of natural persons and/or legal entities in accordance with Art. 24, Para. 1 of the eIDAS Regulation.

All statements in this certification program apply equally to all sub-programs, unless explicitly stated otherwise.

The eIDAS certification program with its sub-programs 1) - 10) is intended to provide companies that wish to have a certification carried out by SRC with an overview of the procedure. The certification program will be made available to customers and other parties with a legitimate interest upon request and will also be published on the website of the certification body (https://src-zert.de) in the currently valid version. If there are any further questions regarding the certification procedure, the certification body can be contacted as follows:

SRC Security Research & Consulting GmbH

Certification Body (CAB)

Emil-Nolde-Str. 7
53113 Bonn

Email: info@src-gmbh.de
Phone: +49(0)228 2806-0

2 Scope of application and products covered

The certification body of SRC offers qualified trust service providers or previously non-qualified trust service providers seeking the status of a qualified trust service provider within the meaning of the eIDAS Regulation the evaluation and certification of the

aforementioned (qualified) trust services or trust service components in accordance with sub-programs 1) - 10) (where relevant, including sub-programmes a.).

The assessment is based on relevant standards or technical specifications of the standardisation bodies ETSI and CEN. The product requirements to be considered for the sub-programmes are listed below:

2.1 Qualified services for the creation of qualified certificates for electronic signatures without QSCD according to Art. 28 eIDAS, pursuant to sub-program 1):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI EN 319 411-2 V2.3.1 (2021-05), policy QCP-n, including the referenced requirements from
    - ETSI EN 319 411-1 V1.3.1 (2021-05), policy NCP and
    - ETSI EN 319 401 V2.3.1 (2021-05)

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and
- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienstverordnung" - VDV)

If the provider manages the signature creation data on behalf of the signatory (sub-program a.) additionally:

- CEN EN 419 241:2018 (2018-09)

If the provider identifies applicants (natural persons) via video-based procedures or (partially) automated video-based procedures that it operates in its own area of responsibility (no integration of a trust service component), the product requirements for sub-program 10) must also be met.

2.2 Qualified services for the creation of qualified certificates for electronic signatures with QSCD according to Art. 28 and 29 eIDAS, pursuant to sub-program 2):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI EN 319 411-2 V2.3.1 (2021-05), policy QCP-n-qscd, including the referenced requirements from
    - ETSI EN 319 411-1 V1.3.1 (2021-05), policy NCP+ and
    - ETSI EN 319 401 V2.3.1 (2021-05)

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and

- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienstever-ordnung" - VDV)

If the provider manages the signature creation data on behalf of the signatory (sub-program a.) additionally:

- CEN EN 419 241:2018 (2018-09)

If the provider identifies applicants (natural persons) via video-based procedures or (partially) automated video-based procedures that it operates in its own area of responsibility (no integration of a trust service component), the product requirements for sub-program 10) must also be met.

2.3 Qualified services for the creation of qualified certificates for electronic seals without QSCD according to Art. 38 eIDAS, pursuant to sub-program 3):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI EN 319 411-2 V2.3.1 (2021-05), policy QCP-l including the referenced requirements from
    - ETSI EN 319 411-1 V1.3.1 (2021-05), policy NCP and
    - ETSI EN 319 401 V2.3.1 (2021-05)

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and
- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienste-ver-ordnung" - VDV)

If the provider manages the seal creation data on behalf of the signatory (sub-program a.) additionally:

- CEN EN 419 241:2018 (2018-09)

For providers issuing qualified certificates for electronic seals used by payment service providers as defined in Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, additionally:

- ETSI TS 119 495 V1.5.1 (2021-04)

If the provider identifies applicants (legal representatives of legal entities) via video-based procedures or (partially) automated video-based procedures that it operates in its own area of responsibility (no integration of a trust services component), the product requirements for sub-program 10) must also be met.

2.4 Qualified services for the creation of qualified certificates for electronic seals with QSCD according to Art. 38 and 39 eIDAS, pursuant to sub-program 4):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI EN 319 411-2 V2.3.1 (2021-05), policy QCP-l-qscd, including the referenced requirements from
    - ETSI EN 319 411-1 V1.3.1 (2021-05), policy NCP+ and
    - ETSI EN 319 401 V2.3.1 (2021-05)

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and
- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienste-ver-ordnung" - VDV)

If the provider manages the seal creation data on behalf of the signatory (sub-pro-gram a.) additionally:

- CEN EN 419 241:2018 (2018-09)

For providers issuing qualified certificates for electronic seals used by payment service providers as defined in Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, additionally:

- ETSI TS 119 495 V1.5.1 (2021-04)

If the provider identifies applicants (legal representatives of legal entities) via vid-eo-based procedures or (partially) automated video-based procedures that it op-erates in its own area of responsibility (no integration of a trust services compo-nent), the product requirements for sub-program 10) must also be met.

2.5 Qualified services for the creation of qualified certificates for website authentication according to Art. 45 eIDAS, pursuant to sub-program 5):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI EN 319 411-2 V2.3.1 (2021-05), policy QCP-w, including the referenced requirements from
    - ETSI EN 319 411-1 V1.3.1 (2021-05), policy NCP+ and
    - ETSI EN 319 401 V2.3.1 (2021-05)

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and
- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienste-ver-ordnung" - VDV)

For providers issuing qualified certificates for website authentication used by payment service providers as defined in Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, additionally:

- ETSI TS 119 495 V1.5.1 (2021-04)

If the provider identifies applicants (natural persons or legal representatives of legal persons) via video-based procedures or (partially) automated video-based procedures that it operates in its own area of responsibility (no integration of a trust service component), the product requirements for sub-program 10) must also be met.

2.6 Qualified services for the creation of qualified electronic time stamps according to Art. 42 eIDAS, pursuant to sub-program 6):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI EN 319 421 V1.1.1 (2016-03), including the referenced requirements from
    - ETSI EN 319 401 V2.3.1 (2021-05)

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and
- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienste-verordnung" - VDV)

2.7 Qualified validation services for qualified electronic signatures according to Art. 33 eIDAS and / or qualified electronic seals according to Art. 40 eIDAS, pursuant to sub-program 7):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI TS 119 441 V1.1.1 (2018-08), policy QSVSP, including the referenced requirements from
    - ETSI EN 319 401 V2.3.1 (2021-05)

ETSI TS 119 441 aims to fulfil the generally applicable requirements of Regulation (EU) No 910/2014 for the validation of electronic signatures and seals. The document contains additional requirements for EU Qualified Validation Services (QSVSP) that intend to fulfil the requirements for a qualified validation service for qualified electronic signatures or for qualified electronic seals according to Article 33 of Regulation (EU) No 910/2014.

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and
- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienste-verordnung" - VDV)

2.8 Qualified preservation services for qualified electronic signatures according to Art. 34 eIDAS and / or qualified electronic seals according to Art. 40 eIDAS, pursuant to sub-program 8):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI TS 119 511 V1.1.1 (2019-06), preservation model WST, WTS or WOS, including the referenced requirements from
    - ETSI EN 319 401 V2.3.1 (2021-05)

ETSI TS 119 511 aims to meet the requirements of Articles 34 and 40 of Regulation (EU) No 910/2014 to provide confidence in preservation services that can be used to preserve the validity status of digital signatures or to prove the existence of digital objects using digital signature techniques.

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and
- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienste-verordnung" - VDV)

2.9 Qualified services for the delivery of electronic registered mail according to Art. 44 eIDAS, pursuant to sub-program 9):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI EN 319 521 V1.1.1 (2019-02), policy QERDS, including the referenced requirements from
    - ETSI EN 319 401 V2.3.1 (2021-05)

or

- ETSI EN 319 531 V1.1.1 (2019-01), policy QREMS, including the referenced requirements from
    - ETSI EN 319 401 V2.3.1 (2021-05)
    - ETSI EN 319 521 V1.1.1 (2019-02)

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and
- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienste-verordnung" - VDV)

If the provider identifies senders or recipients (natural persons or legal representatives of legal persons) via video-based procedures or (partially) automated video-based

procedures that it operates in its own area of responsibility (no integration of a trust service component), the product requirements for sub-program 10) must also be met.

2.10 Trust service components for verifying the identity of natural persons and/or legal entities according to Art. 24 (1) eIDAS, pursuant to sub-program 10):

For all providers:

- Regulation (EU) No. 910/2014 of 23.07.2014 (eIDAS)

as well as

- ETSI EN 319 411-2 V2.3.1 (2021-05), requirements for registration authorities of the policies QCP-n and / or QCP-l, including the referenced requirements from
    - ETSI EN 319 411-1 V1.3.1 (2021-05), policy NCP and
    - ETSI EN 319 401 V2.3.1 (2021-05)

For providers from the Federal Republic of Germany additionally:

- Trust Services Act of 18 July 2017 (German "Vertrauensdienstegesetz" - VDG) and
- Trust Services Regulation of 15 February 2019 (German "Vertrauensdienste-verordnung" - VDV) and
- For video-based identification methods: Ordinance No. 118/2021 of the Federal Network Agency "Extension of the temporary recognition of the video identification method as "other identification method" pursuant to § 11 (1) VDG (German "Verfügung Nr. 118/2021 der Bundesnetzagentur "Verlängerung der befristeten Anerkennung der Methode der Videoidentifizierung als „sonstige Identifizierungsmethode" gemäß § 11 Absatz 1 VDG"") (Videoident Ordinance)
- For automated video-based identification methods: Notice No. 340/2021 of the Federal Network Agency "Extension of the provisional recognition of an innovative identification method pursuant to § 11 (3) VDG" (German "Mitteilung Nr. 340/2021 der Bundesnetzagentur „Verlängerung der vorläufigen Anerkennung einer innovativen Identifizierungsmethode gemäß § 11 Absatz 3 VDG") (Autoident Ordinance)
- For Smart-eID methods: Notice No. 341/2021 of the Federal Network Agency "Provisional recognition of an innovative identification method pursuant to § 11 (3) VDG" (German "Mitteilung Nr. 341/2021 der Bundesnetzagentur „Vorläufige Anerkennung einer innovativen Identifizierungsmethode gemäß § 11 Absatz 3 VDG"") (Smart-eID Ordinance)

For providers offering identification services via notified electronic identification means (pursuant to eIDAS Regulation, Article 24 (1) b)) or identification by means of a certificate of a qualified electronic signature or a qualified electronic seal (pursuant to eIDAS Regulation, Article 24 (1) c)) or for providers from other Member States of the European Union offering a video-based identification procedure or a partially or fully automated video-based identification procedure and not voluntarily seeking verification in accordance with the requirements of the Order of the Federal Network Agency (see above), additionally:

- ETSI TS 119 461, matching use case of the policy Baseline LoIP.

A mapping of the legal requirements from the eIDAS Regulation, the Trust Services Act and the Trust Services Regulation to the product requirements from the relevant standards and technical specifications can be found in Annex 2 of the certification program.

The applicable evaluation methods and procedures for the product requirements from the relevant standards and technical specifications can be found in the corresponding annexes 3.* of the certification program.

3 Certification process

The conformity assessment of products is carried out on the basis of relevant standards or technical specifications of the standardisation bodies ETSI and CEN (see chapter 2). It comprises the evaluation of the product by means of all information and results related to the evaluation as well as the certification decision. The execution of the conformity assessment is based on DIN EN ISO/IEC 17065 in conjunction with ETSI EN 319 403-1.

3.1 Request for Proposal and Certification Agreement

The customer for certification sends his request for the certification process to the certification body. For the preparation of the offer, the customer provides a description of the certification object (scope). On the basis of this, the cost of the certification is calculated and an individual offer is prepared. The customer must provide at least the following information for this:

- The type of trust service to be certified (1) - 10)) and the associated product requirements under which the customer wishes to be certified,
- relevant details about the applying trust service provider, in particular the name, address and indication of responsible contact persons,
- the nature and addresses of all sites relevant to the provision of the trust service to be certified, and
- if applicable, the service certificates relevant for the trust service to be certified (if already available).

An assessment of the certification application is carried out by the management of the certification body or an experienced evaluator. In particular, it will be assessed whether the available information is sufficient to carry out the certification process and whether any ambiguities have been clarified, whether the scope has been defined, whether all the resources required for the evaluation activities are available and whether the certification body has the necessary skills and competencies.

After a positive valuation of the application, the certification body informs the interested party about the further certification procedure and, if desired, the customer receives a certification offer containing the Certification Agreement with the certification conditions.

The customer places the order for certification on the basis of the offer of the certification body and accepts the certification conditions by signing the Certification Agreement.

After receipt of the order for certification, the certification body assigns a registration number for the certification and names the customer a contact person responsible for the procedure.

The evaluation is carried out by an evaluation team under the responsibility of the team leader according to the requirements and specifications of the certification body. The responsible contact person (team leader) plans the time schedule of the evaluation process with the customer and the evaluation team and, if necessary, clears up any final uncertainties regarding the evaluation and certification process in preliminary discussions.

3.2 Evaluation

Evaluation comprises all activities to obtain complete information on the fulfilment of the specified requirements by the certification object. This includes planning and preparatory activities as well as documentation reviews, identification of product characteristics according to defined procedures, tests, inspections and audits.

The evaluation is carried out by evaluators who are employees of the certification body or who are approved by the certification body. The certification body ensures that only evaluators with the necessary competence and impartiality are used. The evaluators examine the trust service provider with regard to conformity with the requirements of the eIDAS Regulation relevant for the qualified trust service, taking into account the relevant product requirements.

In order to ensure that the evaluation is carried out, the customer must provide the required documentation, allow the evaluators access to all sites relevant for the provision of the trust services to be certified, and name a responsible contact person.

The evaluation determines whether the organisational and technical measures of the trust service provider meet the requirements. The evaluation of the trust service is divided into two phases:

- the documentation review and the subsequent
- evaluation on site[1].

In the first phase of the evaluation of the trust service provider, the documentation required in the product requirements is analysed by the evaluators and checked for conformity. The documentation must include at least the following documents for all trust services:

- the Trust Service Policy,
- the Trust Service Practice Statement,
- the Security Concept,
- Risk Management documents, including a documented Risk Analysis,

[1] In specific situations that do not allow an on-site evaluation for essential reasons (e.g. protective measures due to the Covid-19 pandemic), the evaluation can be carried out in the form of a remote audit.

- process descriptions as well as relevant working instructions and technical documentation,
- the terms and conditions applicable to the use of the trust service,
- documents for training of the employees,
- service contracts (in case of outsourcing of activities) and
- the Termination Plan for the trust service.

If the documentation review shows that the trust service does not meet the product requirements, no on-site evaluation will be performed. The customer has the opportunity to adapt the documentation of the trust service to the requirements and to have it checked again by the evaluators.

If, after assessing the trust service provider's documentation, the evaluators conclude that the documentation meets the requirements of the product requirements, the second phase follows, the on-site evaluation. The aim of this evaluation is to determine whether the trust service is implemented according to the information in the documentation and whether the implementation meets the normative product requirements. The on-site evaluation is carried out at the trust service provider's premises during an appointment previously agreed with the customer.

The on-site evaluation includes checking the organisational, structural and technical implementation of the measures described in the documentation to meet the requirements.

In doing so, the evaluators will collect evidence on a sample basis through interviews with staff, reviews of documentation, observations of activities and conditions, and technical testing. Where available, evaluations by other independent bodies on individual parts of the evaluated service may also be used. For example, it is not necessary for evaluators to conduct their own evaluations of technical components. They can use test reports and certificates from other independent bodies for their assessment. It must be ensured that the results used are applicable for the certification of the qualified trust service provider and the trust services it provides according to eIDAS.

If non-conformances are found during the evaluation, the customer is informed. If the customer decides to continue the certification process, the evaluators agree with the customer on the additional evaluation tasks that are necessary to verify the correction of the non-conformances. For these evaluation tasks, the previously described phases of the evaluation are carried out again.

After the evaluation has been carried out, the auditors create an evaluation report (conformity assessment report in accordance with Article 20(1) eIDAS), which forms the basis for the certification decision.

3.3 Review and Certification Decision

The certification body assesses the evaluation on the basis of the evaluation report and monitors compliance with the procedural requirements on the basis of DIN EN ISO/IEC 17065. The decision on certification is made by the head of the certification body or another experienced employee of the certification body, the certification decision maker, taking into account the certification decision criteria.

The following conditions are required for a positive certification decision:

- The impartiality of the evaluators and the certification decision-maker in the evaluation and certification process was and is given[2],
- the certification decision-maker was not involved in the evaluation process,
- a certification agreement with acceptance of the certification conditions has been concluded with the customer,
- the evaluation and certification procedure has been carried out in accordance with the certification program and the rules of the certification body,
- the evaluation report is available and does not indicate any critical non-conformances,
- the evaluation has been carried out on the basis of the standards, laws and policies laid down for the service and
- the certificate shows a result in line with the evaluation results.

The certification decision is recorded and signed by the certification decision-maker.[3]. The customer is informed about the certification decision.

In case of a positive certification decision, the SRC certificate is issued. The SRC certificate reflects the scope of the certification and a validity of maximum 2 years as well as represents the trust mark. A valid certificate entitles to the public use of the trust mark in connection with the certified qualified trust service according to the terms of use of the SRC certificate and the SRC trust mark.

If non-critical non-conformances were identified during the evaluation, a positive certification decision is also made as long as the criteria for a positive certification decision are fulfilled. In this case, certification is subject to conditions and the trust service provider is granted a period of 3 months, in justified cases a period of 6 months, after announcement in the evaluation report (conformity assessment report) to rectify the non-conformances. The rectification is confirmed by an updated certificate or by an addendum to the conformity assessment. In doing so, the original validity period of the certificate is not extended. If the trust service provider fails to remedy the non-conformances in due time, the conditional certificate will be withdrawn.

In case of a negative certification decision, the customer will be informed in writing, stating the reasons. In this case, the customer can resume the evaluation if desired.

The work of the certification body is mainly carried out at SRC's offices in Bonn and/or Wiesbaden. In addition, examinations, audits and inspections are also carried out at customers' premises.

All documents, records and evidence collected in the course of evaluation and certification shall be kept by the certification body for at least 10 years after the expiry of the validity of the certificate.

---

[2] A project-specific risk analysis is carried out for each certification process and documented in the Impartiality Risk Analysis form.

[3] The certification decision is documented in the Certification Decision form.

The certificate is always handed over at the premises of the certification body. On request, the certificate can also be handed over at other locations or delivered by post or e-mail.

3.4 Surveillance

A surveillance must take place within the validity period of the certificate in order to maintain the certificate's validity. The date of the surveillance should be in the last six months of the first year after issuance of the certificate. During this surveillance, a sample is taken to check whether the conformity of the trust service with the relevant product requirements is still given. The scope of the respective sample amounts to at least 50% of the sample size of the initial evaluation. The sample shall include all changes made since the initial evaluation. After the monitoring has been carried out, the evaluators prepare a corresponding evaluation report, which is made available to the customer.

During the validity period of a certificate, a maximum of one surveillance audit is carried out to maintain the validity of the certificate. At the latest 2 years after the issuance of the certificate, a full re-certification is necessary to renew (or extend) the certificate according to Article 20(1) of the eIDAS Regulation.

In addition to surveillance, the trust service provider shall immediately inform the certification body of any changes that may affect certification and provide a description of the changes. The certification body shall decide on the basis of the description whether a new documentation review or a new on-site evaluation is necessary or whether the changes can be reviewed during the next surveillance or re-certification. In the case of a renewed documentation review or on-site evaluation, the evaluators prepare a corresponding evaluation report which is made available to the customer.

If non-conformances are found in the course of the surveillance or the evaluation of changes, a plan to remedy these non-conformances within a set period shall be agreed with the customer. As a rule, this period shall not exceed 3 months after the non-conformance has been announced in the evaluation report. If the complexity of the planned remedial action so requires, the deadline may be extended to up to 6 months after the non-conformance has been disclosed in the evaluation report.

The evaluation report of the surveillance or the evaluation of changes serves as the basis for a certification decision analogous to section 3.3. If the certification decision is positive, an addendum to the conformity assessment report and an updated certificate are issued while retaining the original period of validity. The issuance of an updated certificate or an addendum to the conformity assessment report can be waived if no changes to the certification documentation are necessary.

3.5 Certificate publication and use of trust mark

To support the transparency of certifications, the certification body maintains a list of certified products, which is made available to the public. New certificates are published on the certification body's website (www.src-zert.de) shortly after a positive certification decision, including a brief description of the certified product.

The customer is entitled to use the certificate and the trust mark in connection with the certified product in publications, catalogues etc. in accordance with the specifica-

tions of the terms of use of the SRC certificate and the SRC trust mark. In case of incorrect reference or misleading use of the certificate or the trust mark by the customer, the certification body is entitled to withdraw the certificate.

Employees of the certification body regularly monitor that the customer complies with the certification conditions when using the certificates and trust marks. If incorrect references or misleading use of the certificate or trust mark are detected, the customer is requested to correct this immediately. A repeat check for correct use shall be carried out by the certification body within three months.

3.6 Multi-certification

If a trust service provider operates several trust services, these trust services can be evaluated within the framework of a joint certification procedure. The product requirements of the sub-programs concerned are taken into account.

Requirements that are identical in the sub-programs and are implemented identically for all operated trust services only have to be evaluated once. The results of this evaluation can be used in all certifications concerned.

The certification process for all trust services considered in the multi-certification follows the specifications from chapters 3.1 to 3.4. A separate conformity assessment report and certificate is issued for each trust service.

3.7 Certification efforts

The costs for the efforts for

- the performance of the certification,
- the performance of evaluations,
- the handing over of certificates at locations other than the premises of the certification body

as well as further activities of the certification body, if applicable, can be found in the price list (Annex 1).

3.8 Evaluation methods

In addition to on-site audits and inspections, the following methods are used in the evaluation:

- Documentation Review,
- Recognition of certificates for Hardware Security Modules (HSMs) and Qualified Signature or Seal Creation Devices (QSCDs),
- Recognition of certifications of sub-components, and
- Recognition of independent third party reports.

These are described in more detail below:

3.8.1 Documentation Review

Within the scope of the documentation review, it is checked whether the documentation to be provided by the trust service provider (in particular Trust Service Policy,

Trust Service Practice Statement and Termination Plan) comprehensibly demonstrates the fulfilment of the respective product requirements.

3.8.2 Recognition of certificates for HSMs and QSCDs

Insofar as individual requirements stipulate that components used by the trust service provider, for example HSMs or QSCDs, must have certain certifications, this shall be verified as follows.

Certification according to FIPS PUB 140-2

The certificate of the component used is to be queried via the website of the NIST Cryptographic Module Validation Program[4] and the status ("Validation Status" field) of the certification is to be checked. Certificates should have the status "Active" in order to be accepted. Certificates in "Historical" status may also be accepted if the trust service provider can demonstrate that the circumstance that led to this classification ("Historical Reason" field) is not relevant to the use case under consideration or does not lead to a loss of security. Certificates for which the status "Revoked" is issued may not be accepted.

It must be verified that the firmware used on the component matches that specified in the certificate.

Evaluation and certification according to Common Criteria (ISO/IEC 15408)

Certifications according to Common Criteria (CC) must have been issued by a body accredited for this purpose. The current validity of the CC certificate must be checked. This can be done, for example, by calling up the list of certified products of the respective certification body.

It must be verified that the components used by the trust service provider are operated in accordance with the identification and conditions from the CC certification.

If an evaluation of the technical component according to the specifications of the Common Criteria is sufficient and no certification is required, the successfully completed evaluation must be verified. For this purpose, information from the Common Criteria Portal (https://www.commoncriteriaportal.org/) can be used or evidence of the successful evaluation is available from the Common Criteria evaluation body (e.g. the Evaluation Technical Report (ETR), Evaluation Summary).

Certification as QSCD

Qualified signature/seal creation devices must be certified as QSCDs by a body approved for this purpose. As a rule, these should be listed on the EU QSCD list in accordance with Article 31 No. 2 eIDAS.[5] QSCDs that are not on the EU list may also be accepted, provided that a valid certificate from an approved body pursuant to Article

[4] https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search

[5] Informative EU list of certified QSCDs: https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

30, paragraph 1 eIDAS[6] can be presented. In addition, SSCDs that fall under the transitional rule of Article 51(1) eIDAS are accepted.

It must be verified that the QSCDs used by the trust service provider are handled according to the conditions from the QSCD certification.

3.8.3 Recognition of certifications of sub-components

If valid certifications in accordance with the requirements of the eIDAS Regulation already exist for certain (partial) components (e.g. identification of the applicant) for the trust service considered in the evaluation, these can be reused for the certification of the qualified trust service provider and the qualified trust services provided by it. The reuse is possible in principle due to the legal requirements according to Art. 20 (1) eIDAS Regulation, according to which the trust service provider must be audited by a conformity assessment body every 24 months.

The extent of reuse is agreed between the responsible contact person of the customer and the evaluators. It shall be ensured that the reused results are applicable for the certification of the qualified trust service provider and the qualified trust services provided by it. In particular, it shall be verified that the conformity assessment report and the associated certificate have been issued by a certification body that has been authorised by a national accreditation body to perform corresponding certifications and to issue corresponding certificates. In addition, it shall be verified that the certificate is valid and that the scope of the certification covers the relevant product requirements for the fulfilment of which the results are to be reused.

If the conformity assessment report of the certified component contains information that leads the evaluators to doubt the fulfilment of individual product requirements, the evaluators must themselves verify the fulfilment of the requirements concerned by appropriate evaluation methods.

If the existing certification relates to a trust service component operated by a third party that is to be integrated into the trust service under consideration, the evaluators must verify that the product requirements are also fulfilled by the corresponding interfaces between the trust service and the connected component.

3.8.4 Recognition of reports from independent third parties

In principle, each trust service provider can commission third parties to fulfil individual product requirements on its behalf (outsourcing). If the trust service provider makes use of this possibility, it must be verified that the relevant product requirements are fulfilled by the commissioned third party.

Depending on the scope of the outsourcing and the product requirements involved, this can be done by:

- on-site audits or inspections at the third party or
- the review of reports on activities carried out (e.g. reports of penetration tests or vulnerability tests) or of certifications of certain properties of a product (e.g.

[6] Informative EU list of „Designates Bodies for the certification of QSCDs: https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/BODIES_QSCD_SSCD

information on the false acceptance rate of automated, video-based identification procedures).

If on-site audits or inspections are carried out at third parties, these shall be carried out to the same extent as if compliance with the product requirements were ensured by the trust service provider itself.

If the verification of compliance with the product requirements is performed by reviewing reports or certification documents provided by a third party, the evaluators must check that the methods of investigation underlying the report or certification are appropriate to demonstrate compliance with the product requirement beyond reasonable doubt. In particular, the evaluators must verify that the respective reports or certifications have been issued by a third party that has sufficient independence from the trust service provider and has appropriate qualifications and authorisations to perform the audit or certification. In addition, it must be verified that the scope and validity period of the report or certification are suitable to demonstrate compliance with the respective product requirement. By reviewing the documented results of the test (e.g. a penetration test report) or the certification, the evaluators must be able to consider the fulfilment of the product requirement as given without doubt.

3.9 Termination, restriction or withdrawal of certification

A positive certification decision can be subsequently, i.e. after the certificate has been issued, withdrawn or restricted by the conformity assessment body. This occurs in particular in the following cases:

- The supervisory body withdraws the status of "qualified trust service provider" from the customer completely or for specific services.
- The customer ceases its activities as a "qualified trust service provider" or no longer offers specific services.
- It was found that existing certification requirements are no longer sufficiently fulfilled.

The restriction, termination or withdrawal of certification requires the decision of the management of the certification body with the involvement of the employee of the conformity assessment body who made the certification decision for the customer or for the specific service of the customer. In this case, the customer and the competent supervisory body shall be informed of the termination, restriction or withdrawal of certification.

If existing requirements are changed or new requirements are defined, a new certification procedure must be initiated.

The (temporary) suspension of a certification with a subsequent reinstatement of the certification is not supported. For services whose certification has been terminated or withdrawn, a new certification procedure must always be carried out if the need arises.

4 Complaints and appeals

SRC Security Research & Consulting GmbH provides a three-stage appeals process for the parties involved in the event of complaints and appeals to the certification body:

1. In the first instance, an attempt should be made to solve the problem independently with the contact person of the certification body responsible for the certification procedure.
2. If this attempt is not successful, the next step is to involve the head of the certification body.
3. If no agreement can be reached even after involving the head of the certification body, it is possible to appeal against the decision of the head of the certification body and to involve the CAB Advisory Board of the certification body as an independent steering committee. Such appeals must always be sent in writing to the CAB Advisory Board. The address of the CAB Advisory Board is as follows:

   SRC Security Research & Consulting GmbH

   Certification Body (CAB)
   CAB Advisory Board

   Emil-Nolde-Str. 7
   53113 Bonn

   The decision of the CAB Advisory Board shall be made by a simple majority or, in the case of an equal number of votes, by the chairperson in accordance with the rules of procedure of the CAB Advisory Board. The decision is documented in written form and contains the concrete reasons for the decision. It shall be communicated in writing to the parties involved and shall be binding for all.

5 Standards

[1] DIN EN ISO/IEC 17065:2013-01 „Conformity assessment - Requirements for bodies certifying products, processes and services“

[2] ETSI EN 319 401 V2.3.1 (2021-05): Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[3] ETSI EN 319 403-1 V2.3.1 (2020-06): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers

ETSI TS 119 403-2 V1.2.4 (2020-11): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates

ETSI TS 119 403-3 V1.1.1 (2019-03): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

[4] ETSI EN 319 411-1 V1.3.1 (2021-05): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements

[5] ETSI EN 319 411-2 V2.3.1 (2021-05): 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[6] ETSI EN 319 412-1 V1.4.4 (2021-05): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI EN 319 412-2 V2.2.1 (2020-07): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412-3 V1.2.1 (2020-07): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

ETSI EN 319 412-4 V1.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 V2.3.1 (2020-04): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[7] ETSI TS 119 495 V1.5.1 (2021-04): Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking

[8] ETSI EN 319 421 V1.1.1 (2016-03): Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[9] CEN EN 419 241-1 (2018-09): Trustworthy Systems Supporting Server Signing, Part 1: General System Security Requirements

[10] ETSI TS 119 441 V1.1.1 (2018-08): Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services

[11] ETSI TS 119 511 V1.1.1 (2019-06): 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

[12] ETSI EN 319 521 V1.1.1 (2019-02): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers

[13] ETSI EN 319 531 V1.1.1 (2019-01): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers

[14] ETSI TS 119 461 V1.1.1 (2021-07), Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

6 Annexes

Annex 1 Price list

Annex 2 Mapping of the legal requirements of the eIDAS Regulation, the Trust Services Act and the Trust Services Regulation to the product requirements in the standards and technical specifications of the standardisation bodies ETSI and CEN

Annexes 3 Establishment of criteria and evaluation methods

Annex 3.a, criteria according to ETSI EN 319 401
Annex 3.b, criteria according to ETSI EN 319 411-1
Annex 3.c, criteria according to ETSI EN 319 411-2
Annex 3.d, criteria according to ETSI EN 319 421
Annex 3.e, criteria according to ETSI EN 319 521
Annex 3.f, criteria according to ETSI EN 319 531
Annex 3.g, criteria according to ETSI TS 119 441
Annex 3.h, criteria according to ETSI TS 119 461
Annex 3.i, criteria according to ETSI TS 119 495
Annex 3.j, criteria according to ETSI TS 119 511
Annex 3.k, criteria according to CEN EN 419 241-1
Annex 3.l, criteria of the Ordinance pursuant to § 11 (1) VDG
Annex 3.m, criteria of the Ordinance pursuant to § 11 (3) VDG

Annex 4 Certification Agreement

Annex 5 Terms of Use SRC Certificates and SRC Trust Mark

7 Glossary

Term	Explanation
eIDAS	REGULATION (EU) No 910/2014 of the European Parliament and of the Council as of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
Evaluator	Person performing the evaluation
Evaluation team	Team of evaluators
Evaluation	Evaluation includes the activities of auditing, testing, inspection, assessment of services and processes as well as

Term	Explanation
	other activities to determine characteristics in the context of the conformity assessment of products.
Product	In the context of the certification, the term product includes the terms product, system, service and process.
Verification	Determination of one or more characteristics of a product according to a defined certification procedure (see also Evaluation)
Surveillance	Actions (e.g. surveillance audit) to assess if the conformity of the trust service with the relevant eIDAS requirements is maintained.
Certification decision-maker	Person who makes the certification decision.
Certification	Confirmation by an independent body (certification body) related to products, processes, systems or persons.
Certification program	Certification system relating to specific products to which the same specified requirements, rules and procedures are applied.
Certification system	Rules, procedures and management for the implementation of certifications.