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

Version 1.1 / 28.07.2021

Contents

1 Objective

SRC Research & Consulting GmbH's Certification Body – short: SRC - offers other companies the certification of products, systems, services and processes in the area of information technology. In the following, we talk simplified about the certification of products in all these cases. The certification is performed on the basis of normative documents such as legal provisions, standards or technical specifications that define requirements for products. With the certification by an independent certification body, the commissioning companies (customers) have the possibility to provide evidence that their products fulfil the defined requirements.

The SRC Certification Body 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 program for issuing SRC certificates for qualified trust service providers and the qualified trust services they provide that can be assigned to this accredited area. The certification program is designed to provide an overview of the procedure for companies wishing to obtain a certification from SRC. If there are further questions about the certification procedure, the Certification Body can be contacted as follows:

SRC Security Research & Consulting GmbH
Zertifizierungsstelle (KBS)
Emil-Nolde-Str. 7
53113 Bonn

E-Mail: info@src-gmbh.de
Phone: +49(0)228 2806-155

2 Certification program

2.1 Quotation request and certification agreement

The customer who wishes for certification submits his request for the certification process to the Certification Body. The Certification Body informs the interested party about the certification procedure and the customer receives a certification offer that includes the certification agreement with the certification conditions. On the basis of the Certification Body's offer, the customer places an order for certification and, by signing it, accepts the certification agreement including the certification conditions.

2.2 Certification with evaluation and surveillance

After receiving an order for certification, the Certification Body assigns a registration number for the certification and communicates a contact person responsible for the procedure to the customer.

The evaluation is carried out by an audit team under the responsibility of the audit team leader in accordance with the requirements and specifications of the Certification Body. The responsible contact person plans the time schedule of the evaluation and certification process with the customer and the audit team and, if necessary, solves any remaining uncertainties regarding the evaluation and certification process in preliminary discussions.

The evaluation covers all activities to obtain complete information on the fulfilment of the specified requirements by the certified object. This includes planning and preparatory activities as well as document verifications, determination of product characteristics according to defined procedures, tests, inspections and audits.

After the evaluation, the auditors prepare an evaluation report (conformity assessment report according to Article 20 (1) eIDAS) which is the basis for the certification decision. The Certification Body assesses the evaluation on the basis of the evaluation report prepared and monitors the compliance with the procedural specifications on the basis of DIN EN ISO/IEC 17065. The certification decision is documented. The customer is informed about the certification decision.

In the event of a positive certification decision, the certificate will be issued which reflects the scope of the certification and a validity of two years as well as the trust mark. A valid certificate authorises the public use of the trust mark in connection with the certified qualified trusted service in accordance with the requirements of the eIDAS Regulation.

The work of the Certification Body is mainly carried out at the offices of SRC in Bonn and/or Wiesbaden. In addition, tests, audits and inspections are carried out at the customer's premises.

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

The Certification Body of SRC Security Research & Consulting GmbH offers to qualified trust service providers[1], in the sense of the EU Regulation No. 910/2014 dated 23.07.2014 (eIDAS), the assessment and certification of the following qualified trust services:

A. Generation of:

1. qualified certificates for electronic signatures

1a. qualified certificates for electronic signatures with the option to administrate signature creation data on behalf of the signatory (remote signature)

2. qualified certificates for electronic seals

2a. qualified certificates for electronic seals with the option to administrate the seal creation data on behalf of the signatory (remote seal)

3. qualified certificates for website authentication

[1] In the following shortly denoted as TSP (Trust Service Provider).

4. qualified electronic time stamps

B. Verification and validation of:

1. qualified electronic signatures, seals and related qualified certificates

C. Preservation of:

1. qualified electronic signatures, seals or related qualified certificates

D. Delivery of:

1. electronic registered mail.

The assessment and certification is based on relevant ETSI and CEN standards:

ETSI EN 319 401 defines general requirements for TSPs offering one or more of the above qualified trust services (A - D).

ETSI EN 319 411-2 defines additional requirements for TSPs that issue qualified certificates. These requirements are relevant for the qualified trust services A.1 - A.3, including the sub-variants. ETSI EN 319 411-2 refers to the requirements of ETSI EN 319 411-1 and distinguishes between the following certification policies:

- QCP-n
  Certification policy for EU qualified certificates for natural persons,
- QCP-n-qscd
  Certification policy for EU qualified certificates for natural persons that requires the use of qualified signature creation devices (QSCD) for the creation of qualified electronic signatures with the associated electronic signature creation data,
- QCP-l
  Certification policy for EU qualified certificates for legal persons,
- QCP-l-qscd
  Certification policy for EU qualified certificates for legal entities that requires the use of qualified seal creation devices (QSCD) for the creation of qualified electronic seals with the associated electronic seal creation data,
- QCP-w
  Certification policy for EU qualified certificates for website authentication.

The ETSI EN 319 412 series of standards (parts 1 to 5) sets requirements for the profiles of issued certificates. These requirements are also relevant for trust services A.1 - A.3 including the sub-variants.

Where qualified certificates are issued for electronic seals or for website authentication in the context of PSD2, the requirements of ETSI TS 119 495 are also taken into account. In this case, these requirements are additionally relevant for trust services A.2, A.2a and A.3.

ETSI EN 319 421 defines requirements for TSPs that issue qualified electronic time stamps. These requirements are relevant for the qualified trust service A.4.

CEN EN 419 241-1 provides requirements for TSPs that generate qualified electronic signatures or qualified electronic seals and perform the creation and administration of electronic signature or seal creation data on behalf of the signatory. These requirements are relevant for the qualified trust services A.1a and A.2a.

ETSI TS 119 441 provides requirements for TSPs offering the verification and validation of qualified electronic signatures or qualified electronic seals. These requirements are relevant for the qualified trust service B.1.

ETSI TS 119 511 provides requirements for TSPs offering the preservation of qualified electronic signatures or qualified electronic seals. These requirements are relevant for the qualified trust service C.1.

The two standards ETSI EN 319 521 and ETSI EN 319 531 set requirements for TSPs offering a qualified electronic registered delivery service. The ETSI EN 319 531 standard only applies to providers whose technical implementation of the service is based on the use of electronic mail. These requirements are relevant for the qualified trust service D.1.

The certification is carried out on the basis of parts 1 to 3 of the standard ETSI EN 319 403. The evaluation shall be carried out by auditors who are employees of the Certification Body or are accredited by the Certification Body.

The auditors shall examine the TSP for conformity to the eIDAS requirements relevant to the qualified trust service, taking into account the requirements of the ETSI standards mentioned above. The audit shall determine whether the organizational and technical measures of the TSP meet the requirements.

The audit of the trust service is divided into two phases:

- The evaluation of the documents provided by the TSP
- On-site assessment.

In the first phase of the TSP audit, the documentation required by the standards is analysed by the auditors and assessed for their conformity. If the assessment of the documents shows that the trust service does not meet the requirements, no on-site audit will be carried out. The customer has the opportunity to adjust the documentation of the TSP to the requirements and to have it assessed by the auditors again.

If, after evaluating the documentation of the TSP, the auditors come to the conclusion that the documentation meets the requirements of the applicable standards, the second phase of the evaluation, the on-site audit, follows. The aim of this audit is to determine whether the trust service is implemented according to the information in the documentation and that it meets the normative requirements. The on-site audit is carried out at the TSP's premises on a date previously agreed on with the customer.

The on-site audit includes checking the organizational, structural and technical implementation of the measures described in the documentation to fulfil the requirements.

During the audit, the auditors collect evidence on a sample basis through interviews of employees, document reviews, observations of activities and conditions, as well as technical tests. Where available, evaluations by other independent bodies on individual parts of the service to be evaluated may also be used. For example, it is not necessary for auditors to perform their own evaluations of technical components. They may use evaluation reports and certificates from other independent bodies for their assessment.

If valid conformity assessments according to the eIDAS Regulation exist for parts of the trust service (e.g. identification) of the TSP in the scope of the certification, they can be reused for the certification of the qualified trust service provider and the qualified trust services provided by it in order to avoid unnecessary redundancy in the tests and thus costs for the TSP. Reuse is basically possible due to the legal requirements pursuant to Art. 20 of the eIDAS Regulation, according to which the TSP must have been evaluated every 24 months by a conformity assessment body.

The extent of reuse is agreed between the responsible contact person of the customer and the auditors. It shall be ensured that the reused results are applicable to the certification of the qualified trust service provider and the qualified trust services it provides under eIDAS.

Following the on-site audit, the auditors shall prepare a conformity assessment report in accordance with Article 20 (1) of the eIDAS Regulation, based on the document assessment and the audit, stating the compliance of the trust service with the relevant eIDAS requirements and standards. This report forms the basis for the certification decision. The decision on certification is taken by the head of the Certification Body or an experienced employee and documented in the minutes of the certification decision. The certificate is issued with a validity period of two years.

A new on-site audit must be carried out within the last six months of the first year after the certificate was issued in order to extend or maintain the validity of the certificate. This surveillance audit shall, as in the initial audit, be carried out in the form of a sample to verify that the conformity of the trust service with the relevant eIDAS requirements is maintained. In the case of surveillance audits, the size of the respective sample shall be at least 50% of the size of the initial audit sample. The sample shall include all changes made since the last audit. The TSP shall immediately inform the Certification Body of any changes affecting the certification and provide a description of the changes. The Certification Body decides, on the basis of the description, whether a new audit is necessary or whether the changes can be reviewed within the scope of the next surveillance or re-certification audit.

During the validity period of a certificate, a maximum of one surveillance audit is performed to maintain the validity of the certificate. No later than 2 years after the certificate has been issued, a full audit is required to renew (or extend) the certificate in accordance with Article 20 (1) of the eIDAS Regulation.

2.3 Certificate publication and use of trust mark

To support the transparency of certifications, the Certification Body maintains a list of certified products that are available to the public. New certificates are published on the website of the certification body (www.src-zert.de) at short notice following a positive certification decision.

The customer is entitled to use the certificate and trust mark in connection with the certified product in publications, catalogues etc. in accordance with the specifications of the eIDAS regulation. In the event of incorrect reference or misleading use of the certificate or trust mark by the customer, the Certification Body is entitled to withdraw the certificate.

Employees of the Certification Body monitor that the customer complies with the certification terms 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 adjust this immediately. Repeated checks regarding the correct use will be conducted by the Certification Body within three months.

2.4 Certification efforts

The costs for

- conducting the certification,
- conducting evaluations,
- handing over certificates at different locations than the premises of the certification body

as well as any other activities of the Certification Body can be found in the price list (Annex 1).

3 Complaints and appeals

In the event of complaints and appeals towards the Certification Body, SRC Security Research & Consulting GmbH provides a three-step objection procedure process for the parties involved:

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 procedure.
2. If this attempt is not successful, the head of the Certification Body shall be consulted in the following step.
3. If no agreement can be reached even after the involvement of the head of the Certification Body, it is possible to lodge an appeal against the decision of the head of the Certification Body and to involve the KBS Advisory Board of the Certification Body as an independent Steering Committee. Such appeals must always be sent in written form to the KBS Advisory Board. The address of the KBS Advisory Board is as follows:

   SRC Security Research & Consulting GmbH
   Zertifizierungsstelle (KBS)
   KBS-Beirat
   Emil-Nolde-Straße 7
   53113 Bonn

   The decision of the KBS Advisory Board shall be made with a simple majority or, in the case of an equal number of votes, by the chairman in accordance with the rules of procedure of the KBS Advisory Board. The

decision is documented in written form and contains the concrete reasons for the decision. This decision shall be communicated in written form to the involved parties and shall be binding for all parties.

4 Guidelines

[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

[6] 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 (July 2018): 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

5 Annex

Annex 1 Price list

6 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
Auditor	Person performing the evaluation
Audit team	Team of auditors
Evaluation	Evaluation includes the activities of auditing, testing, inspection, assessment of services and processes as well as other activities to determine characteristics in the context of the

Term	Explanation
	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 (surveillance audit) to assess if the conformity of the trust service with the relevant eIDAS requirements is maintained.
Certification	Confirmation by an independent body (Certification Body) relating to the product.
Certification program	Certification scheme 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.