Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

Seidlgasse 22 / 9, 1030 Wien
Tel.: +43 1 503 19 63–0
Fax: +43 1 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: +43 316 873-5514
Fax: +43 316 873-5520

https://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

A-SIT Confirmation Body
Tel.: +43 1 503 19 63-0
E-Mail: office@a-sit.at

Checklist: Confirmation Body Certificates under § 7 para 1 SVG in conjunction with article 30 para 3 lit. b eIDAS

Duties carried out by a confirmation body

A-SIT is a confirmation body in terms of § 3 para 1 item 4 SVG[1]. Thus, A-SIT performs security evaluation processes under article 30 of the eIDAS-Regulation[2] and certifies the conformity of qualified electronic signature and seal creation devices (QSCD) with the requirements under eIDAS Annex II. When there are no standards for the security assessment published by the European Commission by means of implementing acts, the assessment is performed under eIDAS article 30 para. 3 lit. b and A-SIT applies equivalent security levels taking into account the state of the art.

Purpose of this checklist

In order to obtain a confirmation body's QSCD-certificate it is necessary to submit technical documents which must fulfil both formal requirements and requirements on the content (see instructions (C)).

The purpose of this checklist is to support the applicants for a QSCD-certificate in preparing the required documents and as a consequence to enable a quick processing of their request. The checklist contains general recommendations; specific requirements depend upon a particular case.

(A) Why are QSCD-certificates necessary?

For the creation of qualified electronic signatures and qualified electronic seals eIDAS requires evaluated and security-certified components and procedures (qualified electronic signature creation devices resp. qualified electronic seal creation devices). According to eIDAS article 30 para 1 the conformity of qualified electronic signature creation devices with the requirements laid down in eIDAS Annex II is certified by appropriate public or private bodies (confirmation bodies) designated by Member States. Moreover, with respect to article 39 para 2 eIDAS, the requirements of article 30 eIDAS apply mutatis mutandis to the certification of qualified electronic seal creation devices (both referred to as "QSCD" or "QSCD-certificate").

[1] Austrian Signature and Trust Services Act. Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG, BGBl. I Nr. 50/2016 vom 08.Juli 2016).

[2] 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

§ 7 para. 1 SVG: The conformity of qualified electronic signature and seal creation devices in conjunction with the requirements of Annex II eIDAS shall be certified by a confirmation body or a notified body in another Member State of the European Union in accordance with Article 30 (1) eIDAS. In the event of a certification pursuant to Art. 30 para. 3 lit. b eIDAS, the equivalency of the security level shall be assessed by the conformity assessment body or by a notified body according to the technical state of the art. […]

Art. 30 para. 3 lit.b eIDAS:(3) The certification referred to in paragraph 1 shall be based on one of the following procedures:

a) […]

b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The conformation body’s QSCD-certificates have to be shown during conformity assessments pursuant to eIDAS article 20 resp. have to be reported to the supervisory authority when qualified trust services are registered or changed, particularly.

(B) Which components and methods should undergo a certification procedure?

Art. 3 point 22 eIDAS: „Electronic signature creation device“ means configured software or hardware used to create an electronic signature“;

Art. 3 point 23 eIDAS: „Qualified electronic signature creation device“ means an electronic signature creation device that meets the requirements laid down in Annex II;

Art. 3 point 31 eIDAS: „Electronic seal creation device“ means configured software or hardware used to create an electronic seal;

Art. 3 point 32 eIDAS: „Qualified electronic seal creation device“ means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;

The fulfilment of the (1) „Requirements for qualified electronic signature creation devices" (cf. Art. 29 eIDAS) and (2) „Requirements for qualified seal creation devices“ (cf. Art. 39 para. 1), in accordance with the standards listed in the Annex of the Commission Implementing Decision (EU) 2016/650[3] must be proven by the confirmation body’s QCSD-certificate. Particularly, this is the case for technical components and procedures for the

a) generation of signature resp. seal creation data,

b) storage of signature resp. seal creation data,

c) processing of signature resp. seal creation data.

Electronic signature or seal creation data can either (1) be held in an entirely but not necessarily exclusively user-managed environment (cf. Implementing Act 2016/650 article 1 para 1) or (2) a qualified trust service provider (qualified TSP) manages the electronic signature or seal creation data on behalf of a signatory or of a creator of a seal (cf. Implementing Act 2016/650 article 1 para 2). In the former case the certification is performed applying the standards listed in the Annex to Implementing Act 2016/650, in the latter the certification is performed under eIDAS article 30 para 3 lit. b and A-SIT applies equivalent security levels taking into account the state of the art.

There are no certification requirements for further technical components and procedures used in the system environment[4] (cf. eIDAS recital 56).

This applies, to components and procedures as follows, for instance:

- to display the data to be signed resp. sealed,
- for authorizing the signatory resp. the creator of a seal against the qualified electronic signature resp. seal creation device,
- to compute the hash value of the data to be signed resp. sealed, as well as for
- smartcard readers and other hardware.

[3] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[4] Annotation: However, it may optionally be provided by an expert opinion.

(C) What are the requirements to obtain a QSCD-certificate?

With the documents explained here, it must be demonstrated, both in terms of form and content, that the submitted technical components and procedures meet the provisions of the eIDAS-Regulation and the SVG in the specified environment. If the submitted materials are not suitable, it is not feasible to issue a positive QSCD-certificate. Thus, essential requirements on the type and quality of the materials to be delivered are listed here.

In order to apply for a QSCD-certificate, the applicant should complete the relevant application form and submit it to A-SIT. It is necessary to list the type designations of all HW and SW components as the QSCD-certificate is only valid for the given configuration.

The following **documents** should also be submitted:

(1) Functional **reference sample** (resp. access to a reference installation) and related **user** resp. **installation** and **administrator manuals.**

(2) **Description of production and the lifecycle** from the production to the delivery to the qualified TSP or signatory/creator of a seal (if applicable, personalization and use in operation until disposal). If applicable[5], all applications that are processed on the same devices as the signature and seal creation applications must also be described.

Components are e.g. HW, SW, operating system, functional libraries / APIs. Applications should be presented separately because different manufacturers and life cycles are possible and other documents could be relevant. In the case of different lifecycles, a concept should be provided which completely describes the relationships between components and applications running on them.

Furthermore, it is necessary to clarify under which circumstances security-relevant changes of the certified configuration are possible, e.g: Can executable code be reloaded? Is there a key / other authentication information required? Who has access to authentication information?

(3) **Security targets**, that are recognized as suitable by a confirmation body (§ 3 para. 1 no. 4 SVG).

In particular, security targets according to Common Criteria or ISO / IEC 18045 (see Implementing Decision (EU) 2016/650) can be recognized as suitable.

Providing certification reports of components generating, storing, or processing signature creation data or seal creation data is no condition for QSCD-certification, however speeds up the necessary process of assessing that security levels are comparable to standards listed in accordance with eIDAS article 30 para 3 lit. a. Aligning the security targets with standards listed in accordance with eIDAS article 30 para 3 lit. a also facilitates this process, although with reference to article 30 para 3 lit. b this is not a necessary condition.

(4) Relevant **evidence listed in the Annex** to this checklist

All submitted documents shall be presented briefly but completely in a cover page, including references to the submitted documents or other relevant documents (incl. relevant chapters / sections if appropriate).

Notes: Manufacturers' manuals can only be used if the options/parameters[6] that are actually used in a production environment are clearly shown (e.g. in the cover page with the references to the relevant sections).

Certificates with respect to common evaluation standards for individual technical components are not sufficient by themselves. In particular evidence must be provided that the security-related characteristics are met (e.g. security requirements, certification report, evaluation documents and reports).

Any other circumstances that might affect the technically justified decision on the validity period of the QCSD-certificate shall be explained and substantiated.

[5] i.e. when the applications are known at the time of the certification, otherwise they have to be specified in the TSP's security concept.

[6] Annotation: For instance exact definition (minimum length of cryptographic keys etc.) of used cryptographic mechanisms (in particular according to „SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms, https://www.sogis.org)

(D) What is included in the QSCD-certificate?

In the event of a positive completion of the confirmation process pursuant to § 7 para 1 SVG in conjunction with article 30 para 3 lit. b eIDAS, A-SIT will issue a QSCD-certificate with the following content:

1. Certification of the fulfilment of the requirements pursuant to eIDAS-Regulation and SVG by the examined components and procedures and listing of the certified categories[7] (scope of application).
2. Validity period of the certificate,
   The issued QCSD-certificate will be valid up to revocation by A-SIT. To monitor the validity of the QSCD-certificates an associated surveillance process has been introduced and on assignment A-SIT will conduct an ongoing surveillance concerning the security of the technical components and processes used as well as the suitability of the cryptographic algorithms and parameters. Insofar as circumstances arise from the findings of the technology-assessment-activities, which force an expiry of the QCSD-certificate, the certificate will be revoked by A-SIT. The issuance of the QCSD-certificate includes surveillance for a period of two years. The QSCD-certificate will be revoked if there is no further surveillance assigned.
3. Operating conditions (in production environments),
4. Algorithms as well as associated parameters and
5. Evaluation level and strength of mechanisms.

The result of the confirmation process is the QSCD-certificate and an associated report with the detailed assessment results.

The detailed results covers the bullets above (1. Fulfilment of eIDAS-requirements to 5. Evaluation level and strength). In particular, each requirement of eIDAS Annex II is addressed (cf. Annex on required evidence).

Notes:

A positive QCSD-certificate will be published on A-SIT’s website (unless the applicant prohibits this explicitly).

If an issued QSCD-certificate is revoked during its validity period, it will be published on A-SIT’s website in any case.

In any case, pursuant to eIDAS article 31 para 1, new and revoked QSCD-certificates will be notified to the European Commission that is responsible for establishing, publishing and maintaining a list of certified qualified electronic signature and seal creation devices. The notification is done by the supervisory authority.

(E) Non-Disclosure-Statement

A-SIT obeys a strict policy of confidentiality. A-SIT’s Non-Disclosure-Statement (NDS) is publicly available on the A-SIT Website (https://www.a-sit.at/pdfs/nds_asit.pdf).

In order to meet requirements of applicants, A-SIT will issue a signed version of the NDS upon request. A-SIT will not enter into other Non-Disclosure Agreements (NDAs). Confidentiality declarations or NDAs provided by the applicant or its suppliers are therefore not necessary.

Vienna, October 2017

A-SIT Secure Information Technology Center – Austria

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2017-10-24T23:47:02+02:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at
Note	This document is signed with a qualified electronic signature. According to Art. 25 para. 2 of the Regulation (EU) No 910/2014 of 23. July 2014 ("eIDAS-Regulation") it shall have the equivalent legal effect of a handwritten signature.	

[7] see (B) lit. a - c

Annex: Required evidence pursuant to eIDAS

for components and procedures to generate, store and process signature or seal creation data (if applicable:

(A1) Evidence that the technical components and procedures have been successfully evaluated against the security target.

This can be done by appropriate expert opinions, certification reports, security certificates, evaluation technical reports and when appropriate additional evaluation documents. Relevant operating conditions listed in these documents will be included into the QCSD-certificate if appropriate. There is no specific requirement, who has to conduct the evaluation of the components and procedures. By request of the applicant necessary evaluations can be commissioned by the confirmation body resp. they can be performed by the confirmation body itself. In the latter case the required evidence will be provided during the confirmation process. Security requirements that have to be completely implemented by technical means in the case of electronic signatures resp. seals that are created in an entirely user-managed environment can be implemented by organizational or technical-organizational measures in a controlled environment of a qualified TSP in the case of remote electronic signature services (cf. eIDAS recital 52). The existence of such requirements has to be reasonably documented. The fulfilment of these requirements will be evaluated by the confirmation body; required evidence will be announced in the individual case.

(A2) Evidence that for qualified electronic signatures resp. qualified electronic seals only algorithms and parameters are used that are in line with the standards for security assessments pursuant to eIDAS article 30 para 3 lit. a and also comply with the state of the art.

This includes sufficient details of the cryptographic algorithms and used parameters (minimum length of cryptographic keys etc.) as well as the padding where applicable. The state of the art will be interpreted on the basis of recognized crypto-catalogues (in particular „SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms, https://www.sogis.org).

.

(A3) Evidence that the confidentiality of the signature resp. seal creation data is assured (cf. eIDAS Annex II para 1 lit. a).

This includes evidence that security relevant changes in technical components must be apparent for the signatory resp. the creator of a seal (i.e. modifications that would lower the required level of security).

(A4) Evidence that signature resp. seal creation data can practically occur only once (cf. eIDAS Annex II para 1 lit. b).

This includes a detailed and comprehensible presentation of the methods and algorithms used for key generation as well as an exact documentation of the random-quality and safeguarding against age-related modifications.

(A5) Evidence that signature resp. seal creation data cannot, with reasonable assurance, be derived (cf. eIDAS Annex II para 1 lit. c).

This includes a detailed specification of the key management.

(A6) Evidence that the electronic signature resp. the electronic seal is reliably protected against forgery using currently available technology (cf. eIDAS Annex II para 1 lit. c).

This includes evidence that forgery of signatures resp. seals can reliably be identified and security relevant changes in technical components must be apparent for the signatory resp. the creator of a seal (i.e. modifications that would lower the required level of security).

(A7) Evidence that the unauthorised use of signature resp. seal creation data is reliably prevented (cf. eIDAS Annex II para 1 lit. d).

This includes any existing safeguarding for protecting the signature resp. seal creation data against use by others.

(A8) Evidence that the data to be signed is not altered by the qualified signature resp. seal creation device (cf. eIDAS Annex II para 2).

This includes evidence that tampering of signed or sealed data is reliably identified. Security relevant changes in technical components must be apparent for the signatory resp. the creator of a seal (i.e. modifications that would lower the required level of security).

(A9) Evidence that the qualified signature resp. seal creation device does not prevent that the data to be signed resp. sealed is presented to the signatory resp. creator of a seal prior to signing resp. seal creation (cf. eIDAS Annex II para 2).

This includes documentation of the application of the signature resp. seal creation device (comprehensible presentation of the signature resp. seal-process).

In the case of remote electronic signature services:

(A10) Evidence that generating or managing electronic signature resp. seal creation data on behalf of the signatory resp. creator of a seal is done only by a qualified trust service provider (cf. eIDAS Annex II para 3).

This includes detailed documentation of the designated operational environment of the signature resp. seal creation device.

(A11) Evidence that electronic signature resp. seal creation data is duplicated only for back-up purposes and that this is done under the conditions laid down in eIDAS Annex II para 4 lit a and b (cf. eIDAS Annex II para 4).

This includes detailed documentation of the provided back-up and redundancy mechanisms.