Certification decision
Dealing with major / minor non-conformities

ACAB'c position paper
APP 001

Version 1.0 as of August, 12 2020

Important notice

The present document can be downloaded from:
https://www.acab-c.com/position-papers/

The present document may be made available in electronic versions and/or in print. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ACAB'c secretary.

If you wish to make any comment to the present document, please contact ACAB'c secretary:
secretary@acab-c.com

Introduction

The present document is aiming to explain the certification decision process the ACAB'c member Bodies (CAB) are going to follow in order to close an audit of an eIDAS conformant Trust Service Provider (TSP) in case the audit was not closed or was closed with findings of a specific type.

Audit process and certification decision

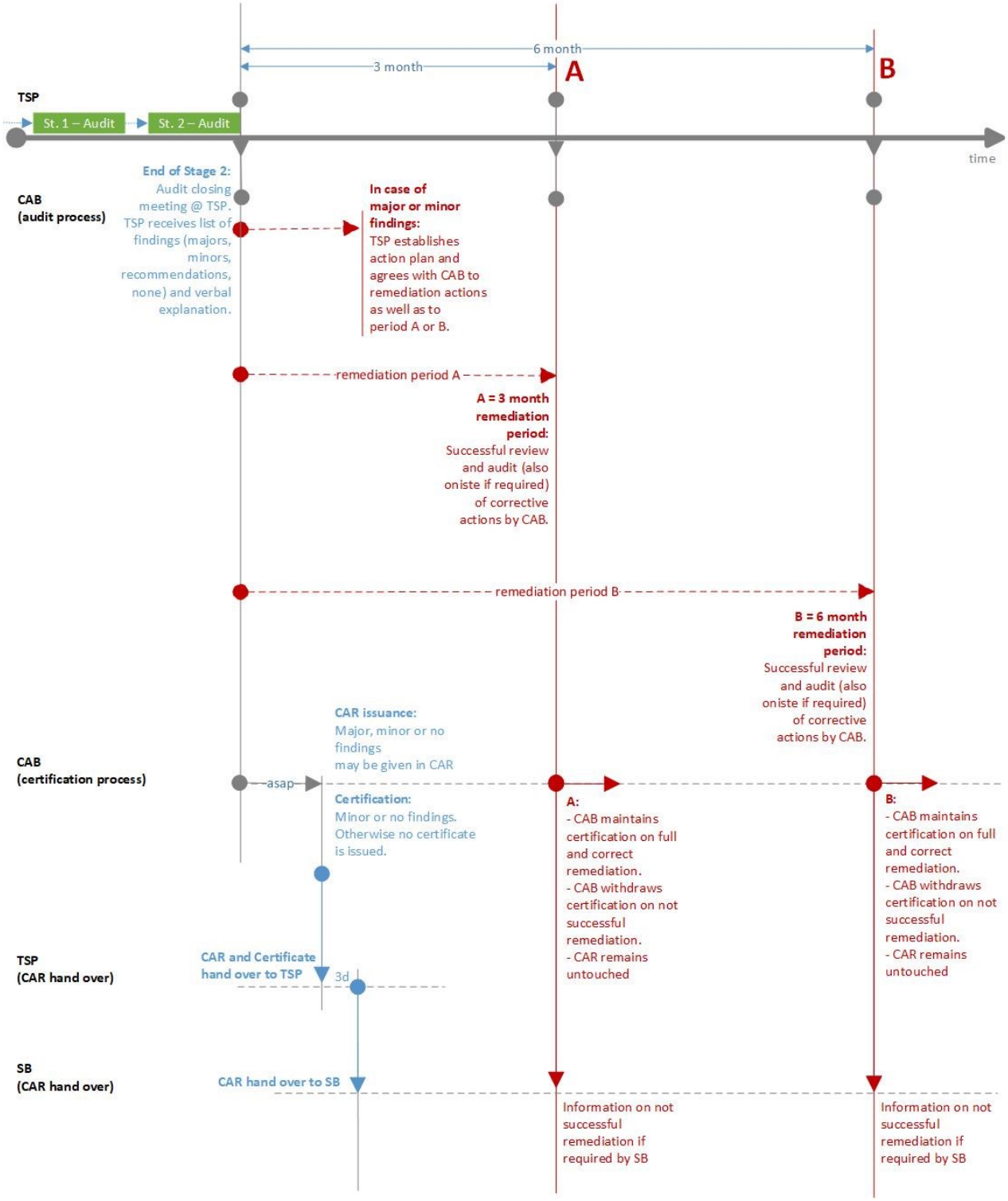
ETSI EN 319 403-1 V2.3.1 (2020-06)[1] introduce in section 7.4.4. the audit process to be followed and in section 7.6 the rules for taking the certification decision.

For audit conclusion and taking the certification decision, ACAB'c members follow the schematic as provided below (Schematic 1) which is regarded to be in line with ETSI EN 319 403-1 V2.3.1 (2020-06)[1].

Note: All member CABs are accredited by National Accreditation Bodies pursuant to the requirements of ISO 17065. The fulfillment of the requirements related to the certification decision as defined in ISO 17065, section 7.6 is required by ETSI EN 319 403-1 V2.3.1, section 7.6 and obviously fulfilled by CAB's accreditation.

[1] and later versions if not otherwise stated.

ACAB'c PP1 - eIDAS Audit flow



Schematic 1

Audit process and certification decision details

The process flow shown in Schematic 1 is understood by ACAB'c members as follows:

Audit Stage 2 is the on-site audit where all audit results shall be summarized and at least be verbally explained and discussed with the TSP during the closing session at the latest. Please keep in mind that there may be more than one Stage 2 on site audit events, e.g. in case multiple sites have to be considered. In that case the concluding audit result explanation shall happen during the closing session of the final on site audit event.
Goal in any case is, to leave the TSP behind with sufficient detailed feedback after the audit has been closed in order to allow the TSP to prepare possibly required follow-up actions like remediation measures and action plans.

Option 1: Audit process flow **without** major or minor findings

In case the audit ends with no major or minor findings, the process steps as indicated in **blue color** are going to be performed by the involved parties. The CAB will finalize the audit report documentation and will issue the eIDAS Conformity Assessment Report (CAR) as well as corresponding certificates. As described in ETSI EN 319 403-1 V2.3.1 (2020-06)[1], section 7.6:

certification decision taken in this case is a) certified.

In case of an initial/re-certification, the TSP shall hand out the CAR to the responsible Supervisory Body (SB) for consideration and decision taking no later than three days after reception as it is required by the eIDAS Regulation.

Option 2: Audit process flow **with minor** findings

In case the audit ends with no major but minor findings the process steps as indicated in **blue and red color** are going to be performed by the involved parties. The CAB will finalize the audit report and prepare the certification. In the meanwhile the TSP sets up an action plan defining specific remediation measures as well as clear due dates to take those measures into operation. The action plan must furthermore define evidences to be delivered to the CAB by the TSP in order to demonstrate that certain defined implementation milestones have been reached. The defined measures must cover all detected minor non-conformities in sufficient detail to be understood and evaluated by the CAB. Part of the action plan suggested by the TSP shall be a detailed rationale in case remediation measures are regarded to require more than 3 month implementation time. Based on the action plan the two parties CAB and TSP consider and discuss the defined remediation measures to be implemented at what milestone and what evidences are expected to be provided by the TSP to prove the milestone was met. Following this discussion the CAB decides on the A=3 or B=6 month period for the implementation of remediation measures (see below for guidance on CAB decision taking for A = 3 or B = 6 month remediation period).
As soon as the action plan is successfully agreed between the CAB and the TSP, the CAB will finalize the audit report documentation and will issue the eIDAS conformant Conformity Assessment Report (CAR) as well as the corresponding certificates. Whereas the CAR as well as the certification documentation will clearly list all minor non-conformities.

As all minor non-conformities are now covered by the profound action plan, the certification decision shall be taken as described in ETSI EN 319 403-1 V2.3.1 (2020-06)[1], section 7.6:

certification decision taken in this case is a) certified.

Remediation plan follow-up: All relevant evidences must be provided by the TSP in sufficient time before the A=3 or B=6 month period ends. That is necessary in order to allow the CAB to check the evidences and take the final decision that the minor findings were successfully addressed. In order to do so, the CAB may review the provided evidences either based upon a provided documentation or through an additional onsite audit as it deems that necessary.

In case the CAB decision on the performed TSP remediation measures is **positive** = minor findings successfully remediated, the CAB will keep the CAR as well as the certification upright. The positive decision will be documented and the documentation is submitted to the TSP and/or SB.
In case the CAB decision on the performed TSP remediation measures is **negative** = minor findings not successfully remediated, the CAB will withdraw the certification. It will furthermore inform the SB that the minor nonconformities were not or not fully remediated.

Option 3: Audit process flow **with major** findings

In case the audit ends with major (and with or without minor) findings the audit failed. The details of the further treatment of the situation is to be discussed between the CAB and the TSP. A possible way would be to follow the process steps as already indicated and described above under Option 2, however ending with a (negative) CAR containing statements on the major non-conformities detected. That option may be taken in order to allow the local Supervisory Body (SB) to take further steps and decisions.
In any case no certificate shall be issued in case of an audit closure with major non-conformities as described in ETSI EN 319 403-1 V2.3.1 (2020-06)[1], section 7.6:

certification decision taken in this case is b) not certified.

Guidance on decision taking within remediation period A/B

The decision on the 3 or 6 month remediation period to be taken by the CAB needs to be based upon the rationale provided by the TSP. In case remediation measures are judged to require more than 3 month time to take them into operation, reasons given by the TSP must be based upon robust evidences which can be supported by the CAB. Evidencing for that is on the TSP.

Examples:

a.) In case only TSP documentation needs to be corrected, the typical implementation time to be expected is far shorter than A=3 month. For such changes A can be assumed.
b.) In case the TSP needs to change its implementation in the way that his infrastructure must be changed (e.g. technical devices like HSM need to be bought or enforcement of building security measures like doors, windows, alarm, etc. is required), the typical implementation time to be expected is rather B=6 month. For such changes B can be assumed.