DIGITALISERINGSSTYRELSEN

August 2023

Version: 1.2

Audit guide for the following public certificate policies

- OCES employee certificates version 7.2,
- OCES business certificates version 7.2,
- Qualified person certificates version 1.2,
- Qualified employee certificates version 1.2 and
- Qualified business certificates version 1.2

1. Introduction

In connection with the Danish Agency for Digital Government's supervision of trust service providers issuing qualified certificates and OCES certificates, a conformity assessment report from a conformity assessment body shall be enclosed (cf. eIDAS article 20(1) and OCES certificate policies clause 8).

The purpose of this document is:

- to describe the scope of the conformity assessment for trust service providers that use one or more of the public certificate policies for
    - OCES employee certificates version 7.2,
    - OCES business certificates version 7.2,
    - Qualified person certificates version 1.2,
    - Qualified employee certificates version 1.2 and
    - Qualified business certificates version 1.2
- to provide examples and guidance on the preparation of audits and assessments, and
- to describe the requirements for the final conformity assessment report which can be used by the trust service provider and the conformity assessment body.

This document is aimed at trust service providers that use one or more of the certificate policies mentioned, and at conformity assessment bodies that assess such trust service providers.

Readers of this document are expected to be familiar with the eIDAS Regulation and the above certificate policies.

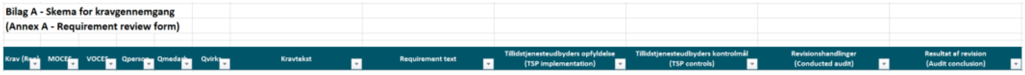
2. Guide

2.1 Assessment form

As a supplement to this document, a form has been prepared (see Annex A) which is to be completed and attached to the conformity assessment report. The form contains the requirements from the certificate policies and related fields to be filled in by the trust service provider and the conformity assessment body, respectively.

The first columns contain all requirements from the certificate policies presented in a structured format and constitute the primary documentation for compliance with the requirements. For each individual requirement, it is specified whether the requirement is relevant for a given certificate policy and thus should be filled in if this policy is supported by the trust service provider.

Next to the respective requirements, the form has two columns to be filled in by the trust service provider and two columns to be filled in afterwards by the conformity assessment body:



Bilag A - Skema for kravgennemgang
(Annex A - Requirement review form)

Krav (Req	MOCES	VOCES	Qperso	Qmedarb	Qvirks	Kravtekst	Requirement text	Tillidstjenesteudbyders opfyldelse (TSP implementation)	Tillidstjenesteudbyders kontrolmål (TSP controls)	Revisionshandlinger (Conducted audit)	Resultat af revision (Audit conclusion)

The purpose of the individual columns is described below:

- **"Tillidstjenesteudbyderens beskrivelse af opfyldelse" - Trust service provider's description of compliance (certificate practice)**
  Here, the trust service provider describes how the related requirements are met. This account contains a description of any implemented technical, procedural or organizational measures as described in the CPS – Certification Practice Statement (see clause 1.5.4 of certificate policies).
- **"Tillidstjenesteudbydernes beskrivelse af kontrolmål" - Trust service provider's description of SMART goals**
  Here, the trust service provider uses SMART-goals to describe how to check whether the described practice has been observed/implemented. This item should be formulated as a SMART[1] requirement to make sure that it is clear and measurable.
- **"Revisionshandlinger ved udført vurdering" - Audit actions for completed assessments**
  Here, the conformity assessment body specifies the types of actions used in the assessment of the specific requirement
- **"Resultat af udført revision" - Outcome of completed audit**
  Here, the conformity assessment body gives a conclusion regarding the completed assessment of the relevant requirement.

It is recommended to use the following principles in the selection of audit actions:

Principle	Description
Inquiry	Interview, meeting, inquiry with responsible staff at the trust service provider
Observation	Observation of the completion of control
Inspection	Review and evaluation of policies, procedures and documentation regarding the outcome of the control. That includes review and evaluation of reports and other documentation to assess whether controls have been prepared and implemented. Moreover, it is assessed whether controls are monitored and checked at appropriate intervals
Repetition of control	Repetition of the relevant control elements to verify the execution of the control functions

[1] **S**pecific, **M**easurable, **A**chievable, **R**elevant and **T**ime-bound

Please note that the completion by the trust service provider of the form (Annex A) should be comprehensive and self-contained. However, it is permitted to refer to documents appended in Annex A for further details (e.g. technical documentation, IT security certificates and/or protection of personal data - e.g. ISO 2700x certificate, various ISAE declarations). Please note that the description in the form should be sufficient to provide a coherent account of how the requirements has been observed.

2.2 Example of how to fill in the form

The following gives a short example of how to fill in the form. Focus is on illustrating the logic of the form and not on providing an exhaustive and realistic example.

The example is based on **[REQ 5.3.2-02]** Control of staff:

REQ 5.3.2-02
The CA must check that managers and employees performing trusted tasks at or for the CA have not been convicted of a crime that makes them unsuitable for performing their job. This also applies to RA employees.

Trust service provider's description of compliance (certificate practice)
All employees performing work for the CA shall present a criminal record certificate. The criminal record certificate must not state any matters that disqualify the employee from performing the work required by the position. The CISO will decide whether any matters are disqualifying. Annual spot checks are made where at least 5% of employees performing work for the CA shall present a new criminal record certificate.

Annual audit reports from external RAs shall include an assessment of whether the external RA meets the requirement for control of relevant employees.

Trust service provider's description of SMART goals
HR employees acknowledges that criminal record certificates have been checked in a manual paper-based log in connection with employment. The log shall contain employee identification (employee number and name), date of criminal record certificate and the name and signature of the HR employee.

Every year, HR registers who have been selected for spot checks for presentation of a new criminal record certificate corresponding to the log for new employees.

Audit reports from external RAs are collected and checked for qualifications in relation to the control of employees. It must be ensured that audit reports are available from all external RAs.

Audit actions for completed assessments
It has been checked that a log is available for new employees and that a log is available for employees selected to present a new criminal record certificate.

A population of 10% of new employees performing work for the CA has been selected, and it has been checked that the new employees are registered with the information stated in the paper-based log.

It has been checked that the log for employees selected to present a new criminal record certificate contains at least 5% of the employees working for the CA and that the stated information have been entered.

It has been checked that audit reports are available from all external RAs and that they do not contain qualifications in relation to the control of employees.

Outcome of completed assessment
The audit has not given rise to any comments and it can be concluded that the procedures and controls described have been implemented and are effective.

3. Requirements for the conformity assessment report

In addition to filling in the above form, the conformity assessment body shall prepare a specific auditor's record (audit report) regarding the trust service provider's solution, cf. clause 8.6 of the certificate policies. The audit report can be prepared in accordance with the ISAE 3000 standard or a similar standard, and a high degree of certainty must be achieved under this standard. For the qualified policies, the audit report shall be compliant with a conformity assessment report cf. eIDAS.

The purpose of the audit report is to conclude (based on the content in the form – Annex A – for the individual requirements) whether the trust service provider, overall, has managed to establish all relevant procedures and that the design and functionality of controls related to the procedures are effective. All requirements for a relevant certificate policy shall be met for the relevant type of solution before the solution can be said to comply with the relevant certificate policy.

The trust service provider is responsible for preparing all relevant procedures and controls for ensuring compliance with the requirements of a given certificate policy.

The conformity assessment body is responsible for formulating a conclusion as to whether the procedures and controls defined by management were appropriately designed and implemented at the time of the conformity assessment, and whether they worked appropriately throughout the reporting period (see section 3.1. 'Period of the conformity assessment report' below).

Annex A specifies SMART goals that should be considered by the audit report as well as examples of specific audit actions that can be carried out. The conformity assessment shall comprise procedures and controls within all SMART goals. The conformity assessment body is responsible for adapting the audit actions to the specific procedures and controls established by the trust service provider.

3.1. Period of the conformity assessment report

In the event of a new solution/tender service from the trust service provider, an ISAE 3000 type 1 report may be used as the first record, and the report period may comprise a given date that does not exceed 90 days from the reporting date for the Danish Agency for Digital Government.

The trust service provider shall then submit a corresponding type 2 report annually prepared by a conformity assessment body. The reporting period for such reports shall run from the date of the latest report. The report must be received by the Danish Agency for Digital Government as described in clause 1.5.3 of the certificate policies.

Under any circumstance, the trust service provider is responsible for subcontractors that undertake checks or delivers relevant services on behalf of the trust service provider. To the extent that the trust service provider uses subcontractors, the audit must also include relevant subcontractors.

In connection with the review of the conformity assessment report (the audit report) from trust service providers, the Danish Agency for Digital Government will apply SMART goals from the table (Annex A) to assess whether the conformity assessment body's audit report covers the required matters. In case of areas that are not relevant, the conformity assessment body shall provide reasons for why the particular matter is irrelevant. In case of significant matters that are not included in the areas below, such areas must be included in the audit report provided.

In case of a qualified audit report, the trust service provider may lose the right to provide the trust service in question. If the report includes comments (usually of minor importance), the Danish Agency for Digital Government must receive a written statement from the trust service containing an account of the matters and a detailed action plan and time schedule for the remediation of the matter not later than 60 calendar days from the expiry of the reporting period. If the trust service fails to observe this, it may lose the right to provide the trust service in question.