DIGITALISERINGSSTYRELSEN

August 2023

Version: 1.2

Revisionsvejledning til de følgende offentlige certifikatpolitikker

- OCES-medarbejdercertifikater version 7.2,
- OCES-virksomhedscertifikater version 7.2,
- Kvalificerede personcertifikater version 1.2,
- Kvalificerede medarbejdercertifikater version 1.2 og
- Kvalificerede virksomhedscertifikater version 1.2

1. Indledning

I forbindelse med Digitaliseringsstyrelsens tilsyn af tillidstjenesteudbydere, der udsteder henholdsvis kvalificerede certifikater og OCES-certifikater, skal der vedlægges en overensstemmelsesvurderingsrapport fra et overensstemmelsesvurderingsorgan (jf. eIDAS artikel 20, stk. 1 og OCES certifikatpolitikker afsnit 8).

Formålet med dette dokument er:

- at beskrive omfanget af overensstemmelsesvurderingen for tillidstjenesteudbydere, der anvender en eller flere af de offentlige certifikatpolitikker for
    - OCES-medarbejdercertifikater version 7.2,
    - OCES-virksomhedscertifikater version 7.2,
    - Kvalificerede personcertifikater version 1.2,
    - Kvalificerede medarbejdercertifikater version 1.2 og
    - Kvalificerede virksomhedscertifikater version 1.2,
- at give eksempler og vejledning på vurderingsudformning, samt
- at beskrive kravene til den endelige overensstemmelsesvurderingsrapport, hvilket kan benyttes af tillidstjenesteudbyderen og overensstemmelsesvurderingsorganet.

Dette dokument er målrettet tillidstjenesteudbydere, der benytter en eller flere af de nævnte certifikatpolitikker, samt overensstemmelsesvurderingsorganer, der vurderer disse tillidstjenesteudbydere.

Læsere af dette dokument forventes at have indsigt i eIDAS-forordningen og ovenstående certifikatpolitikker.

2. Vejledning

2.1 Skema til vurderingen

Som supplement til dette dokument er der udarbejdet et skema (se bilag A), der kan udfyldes og vedlægges til overensstemmelsesvurderingsrapporten. Skemaet indeholder kravene i certifikatpolitikkerne og tilhørende felter, som udfyldes af henholdsvis tillidstjenesteudbyderen og overensstemmelsesvurderingsorganet.

De første kolonner i skemaet indeholder samtlige krav i certifikatpolitikkerne opsat på struktureret form og udgør den primære dokumentation for efterlevelsen af kravene. For hvert enkelt krav er det angivet, om kravet er relevant for en given certifikatpolitik og dermed udfyldes, hvis denne politik understøttes af tillidstjenesteudbyderen.

I tilknytning til de respektive krav indeholder skemaet to kolonner, som udfyldes af tillidstjenesteudbyderen, og to kolonner, som efterfølgende udfyldes af overensstemmelsesvurderingsorganet:

Hensigten med de enkelte kolonner gennemgås nedenfor:

- **Tillidstjenesteudbyderens beskrivelse af opfyldelse (certifikatpraksis)**
  Her beskriver tillidstjenesteudbyderen, hvorledes de tilhørende krav er opfyldt. Redegørelsen indeholder en beskrivelse af implementerede tekniske-, processuelle- eller organisatoriske- tiltag som beskrevet i CPS – Certification Practice Statement (jf. certifikatpolitikkernes afsnit 1.5.4).
- **Tillidstjenesteudbydernes beskrivelse af kontrolmål (SMART)**
  Her beskriver tillidstjenesteudbyderen i form af kontrolmål, hvordan man konkret kan kontrollere, om den beskrevne praksis er opfyldt / implementeret. Punktet bør formuleres som et SMART[1] krav, så det sikres, at det er entydigt og målbart.
- **Revisionshandlinger ved udført vurdering**
  Her angiver overensstemmelsesvurderingsorganet, hvilke typer handlinger som benyttes ved vurderingen af det konkrete krav.
- **Resultat af udført revision**
  Her udtrykker overensstemmelsesvurderingsorganet en konklusion vedrørende den udførte vurdering for det pågældende krav.

I udvælgelsesprocessen af revionshandlingerne ved vurderingen anbefales det at anvende følgende principper:

Princip	Beskrivelse
Forespørgsel	Interview, møde, forespørgsel med ansvarligt personale hos tillidstjenesteudbyderen
Observation	Observation af gennemførelsen af kontrol
Inspektion	Gennemgang og evaluering af politikker, procedurer og dokumentation vedrørende kontrollens resultater. Dette omfatter gennemlæsning og evaluering af rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet og implementeret. Desuden vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller
Genudførsel af kontrol	Gentagelse af de relevante kontrolelementer for at verificere udførslen af kontrolfunktionerne

[1] **S**pecific (Specifik), **M**easurable (Målbare), **A**chievable (Opnåelige), **R**elevant (Relevante) og **T**ime-bound (Tidsbestemte)

Bemærk at tillidstjenestens udfyldelse af skemaet (Bilag A) bør være dækkende og selvindeholdt. Det er dog tilladt at referere til vedlagte dokumenter i Bilag A for yderligere detaljer (fx teknisk dokumentation, certifikater inden for IT-sikkerhed og / eller beskyttelse af person data - f.eks. ISO 2700x certifikat, diverse ISAE-erklæringer). Vær venligst opmærksom på, at beskrivelsen i skemaet bør være tilstrækkelig dækkende til, at den i sig selv giver en sammenhængende redegørelse for, hvordan kravet er opfyldt.

2.2 Eksempel på udfyldelse af skema

I det følgende gennemgås kort et eksempel på udfyldelse af skemaet. Fokus er på at illustrere logikken i skemaet og ikke at give et udtømmende og realistisk eksempel.

Der tages udgangspunkt i **[KRAV 5.3.2-02]** Kontrol af personale:

KRAV 5.3.2-02
CA skal kontrollere, at ledere og medarbejdere, der udfører betroede opgaver i eller for CA, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv. Dette er ligeledes gældende for RA medarbejdere.

Tillidstjenesteudbyderens beskrivelse af opfyldelse (certifikatpraksis)
Alle medarbejdere, der udfører arbejde for CA skal ved ansættelsen fremvise en straffeattest. Straffeattesten må ikke indeholde forhold, der gør medarbejderen uegnet til at bestride den jobfunktion ansættelsen vedrører. Det er CISO, der beslutter om et forhold er diskvalificerende. Der laves en årlig stikprøve, hvor minimum 5% af ansatte, der udfører arbejde for CA, skal fremvise en ny straffeattest.

Årlig revisionserklæring fra eksterne RA skal omfatte en vurdering af, om den eksterne RA opfylder kravet til kontrol af relevante medarbejdere.

Tillidstjenesteudbydernes beskrivelse af kontrolmål (SMART)
HR-medarbejder kvitterer for, at der er foretaget kontrol af straffeattest i manuel papirbaseret log i forbindelse med ansættelse. Loggen skal indeholde identifikation af medarbejder (medarbejdernummer og navn), dato på straffeattest samt HR-medarbejders navn og underskrift.

HR registrerer årligt, hvem der er udtaget i stikprøve for fremvisning af ny straffeattest med en log svarende til loggen for nyansættelser.

Revisionserklæringer fra eksterne RA'er indsamles og kontrolleres for forbehold i forhold til kontrol af medarbejdere. Det sikres, at der foreligger revisionserklæringer fra alle eksterne RA'er.

Revisionshandlinger ved udført vurdering
Det er kontrolleret, at der findes en log for nyansættelser og en log for medarbejdere, der er udtaget til genfremvisning af straffeattest.

Der er udtaget en population på 10% af nyansættelser, der udfører arbejde for CA, og det er kontrolleret, at disse er registreret med de angivne informationer i den papirbaserede log.

Det er kontrolleret, at loggen for medarbejdere, der er udtaget til genfremvisning af straffeattest, indeholder mindst 5% af medarbejdere, der arbejder for CA, og at der for hver medarbejder er udfyldt de angivne informationer

Det er kontrolleret, at der foreligger revisionserklæringer fra alle eksterne RA'er, og at disse ikke indeholder forbehold i forhold til kontrol af medarbejdere.

Resultat af udført vurdering
Revisionen har ikke givet anledning til bemærkninger, og det konkluderes, at de beskrevne procedurer og kontroller er implementeret og effektive.

3. Krav til overensstemmelsesvurderingsrapporten

Overensstemmelsesvurderingsorgan skal ud over udfyldelse af ovennævnte skema udarbejde et specifikt protokollat (revisionserklæring) om den tillidstjenesteudbyderens løsning jf. certifikatpolitikkernes afsnit 8.6. Revisionserklæringen kan udarbejdes efter ISAE 3000 standarden eller tilsvarende, og der skal opnås en høj grad af sikkerhed efter denne standard. For kvalificerede politikker skal protokollatet overholde eIDAS krav til en overensstemmelsesvurderingsrapport.

Revisionserklæringen har til formål at konkludere (på baggrund af indholdet i skemaet – Bilag A - for de enkelte krav), hvorvidt tillidstjenesteudbyderen samlet set har etableret alle relevante procedurer samt at udformningen og funktionaliteten af kontroller, der knytter sig til procedurerne, er effektive. Samtlige krav for en relevant certifikatpolitik skal således være opfyldt for den relevante type løsning, før løsningen kan siges at leve op til den pågældende certifikatpolitik.

Det er tillidstjenesteudbyderens ansvar at udforme alle relevante procedurer og kontroller til sikring af, at kravene i en given certifikatpolitik overholdes.

Det er overensstemmelsesvurderingsorganets ansvar at udtrykke en konklusion om, hvorvidt de af ledelsen etablerede procedurer og kontroller var hensigtsmæssigt udformet og implementeret på tidspunktet for overensstemmelsesvurderingen, og hvorvidt disse fungerede hensigtsmæssigt i hele erklæringsperioden (se afsnittet "3.1 Periode for overensstemmelsesvurderingsrapporten" herunder).

I bilag A er der angivet kontrolmål, som er omfattet af revisionserklæringen, samt eksempler på konkrete revisionshandlinger, der kan udføres. Overensstemmelsesvurderingen skal omfatte procedurer og kontroller inden for alle kontrolmål. Det er overensstemmelsesvurderingsorganets ansvar at tilpasse revisionshandlingerne til de konkrete procedurer og kontroller, der er etableret hos tillidstjenesteudbyderen.

3.1 Periode for overensstemmelsesvurderingsrapporten

Hvis der er tale om en ny løsning/tilbudstjeneste fra tillidstjenesteudbyderen, kan der anvendes en ISAE 3000 type 1 erklæring som det første protokollat, og erklæringsperioden kan omfatte én given dato, som ikke er på mere end 90 dage fra rapporteringsdatoen til Digitaliseringsstyrelsen.

Tillidstjenesteudbyderen skal herefter én gang årligt indsende en tilsvarende type 2 erklæring udfærdiget af et overensstemmelsesvurderingsorgan. Erklæringsperioden for disse erklæringer skal dække fra datoen for sidste erklæring. Erklæringen skal være Digitaliseringsstyrelsen i hænde jf. certifikatpolitikkerne afsnit 1.5.3.

Tillidstjenesteudbyderen er i enhver henseende ansvarlig for underleverandører, som varetager kontroller eller leverer relevante ydelser på vegne af tillidstjenesteudbyderen. I det omfang tillidstjenesteudbyderen benytter underleverandører, skal revisionen ligeledes omfatte relevante underleverandører.

Digitaliseringsstyrelsen vil ved gennemgang af overensstemmelsesvurderingsrapporten (revisionserklæringen) fra tillidstjenesteudbydere anvende kontrolmål fra skemaet (Bilag A) til at vurdere, om overensstemmelsesvurderingsorganets revisionserklæring omfatter de nødvendige forhold. Hvis der er områder, som ikke er relevante, skal overensstemmelsesvurderingsorganet begrunde, hvorfor forholdet ikke er relevant. Eksisterer der forhold, som er væsentlige, og som ikke er indeholdt i områderne nedenfor, skal disse områder medtages i den afgivne revisionserklæring.

I det tilfælde, at en revisionserklæring afgives med forbehold, kan dette medføre, at tillidstjenesteudbyderen mister retten til at udbyde den relevante tillidstjeneste. I det tilfælde der fremgår bemærkninger af erklæringen (ofte af mindre væsentlig karakter), skal Digitaliseringsstyrelsen senest 60 kalenderdage fra erklæringsperiodens udløb modtage en skriftlig redegørelse fra tillidstjenesten indeholdende en beskrivelse af forholdene og en detaljeret handlings- og tidsplan for udbedring af forholdet. Overholdes dette ikke, kan dette ligeledes medføre, at tillidstjenesten mister retten til at udbyde den relevante tillidstjeneste.