DIGITALISERINGSSTYRELSEN

August 2023

Version: 1.2

Revisionsvejledning til Offentlig politik for kvalificeret signatur- og segl validering

Version 1.2

1. Indledning

I forbindelse med Digitaliseringsstyrelsens tilsyn af tillidstjenesteudbydere, der udbyder kvalificerede signatur- og seglvalidering, skal der vedlægges en overensstemmelsesvurderingsrapport fra et overensstemmelsesvurderingsorgan (jf. eIDAS artikel 20, stk. 1).

Formålet med dette dokument er:

- at beskrive omfanget af overensstemmelsesvurderingen for tillidstjenesteudbydere, der anvender den offentlige politik for kvalificerede signatur- og seglvalidering 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

- Offentlig politik for kvalificeret signatur- og seglvalidering version 1.2,

samt overensstemmelsesvurderingsorganer, der vurderer disse tillidstjenesteudbydere.

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

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 valideringspolitikken og tilhørende felter, som udfyldes af henholdsvis tillidstjenesteudbyderen og overensstemmelsesvurderingsorganet.

De første kolonner i skemaet indeholder samtlige krav i valideringspolitikken opsat på struktureret form og udgør den primære dokumentation for efterlevelsen af kravene.

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

Bilag A - Skema for kravgennemgang (Annex A - Requirement review form)						
Krav (Req)	Kravtekst	Requirement text	Tillidstjenesteudbyders opfyldelse (TSP implementation)	Tillidstjenesteudbyders kontrolmål (TSP controls)	Revisionshandlinger (Conducted audit)	Resultat af revision (Audit conclusion)

Hensigten med de enkelte kolonner gennemgås nedenfor:

- **Tillidstjenesteudbyderens beskrivelse af opfyldelse (VA-praksis)**
  Her beskriver tillidstjenesteudbyderen, hvorledes de tilhørende krav er opfyldt. Redegørelsen indeholder en beskrivelse af implementerede tekniske-, processuelle- eller organisatoriske- tiltag som beskrevet i VA-praksis (jf. valideringspolitikken afsnit 6.2).
- **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

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-erklæ-

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

ringer). 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 6.1-01]** Risikovurdering:

KRAV 6.1-01

VA skal gennemføre risikovurdering for at identificere, analysere og evaluere forretningsmæssige og tekniske risici.

Tillidstjenesteudbyderens beskrivelse af opfyldelse (VA-praksis)
VA gennemfører halvårlige risikovurderinger. Desuden gennemføres risikovurderinger ved større organisatorisk, driftsmæssige eller tekniske ændringer relateret til den udbudte tjeneste. Det er CISO, der beslutter om en ændring har et omfang, der kræver en risikovurdering.

Risikovurderingen forelægges ledelsen.

Tillidstjenesteudbydernes beskrivelse af kontrolmål (SMART)
Alle risikovurderinger underskrives af ledelsen og arkiveres i minimum 7 år. In-tern revision kontrollere løbende og mindst 1 gang årlig, at der foreligger ledel-sesunderskrevne risikovurderinger for at forgangne periode.

Revisionshandlinger ved udført vurdering
Det er kontrolleret, at der forefindes det 3 ledelsesunderskrevne risikovurderinger for den reviderede periode, der dels dække de ordinære vurderinger og dækker en større organisatorisk ændring. Det er ikke konstateret at der har været andre organisatoriske, driftsmæssige eller tekniske ændringer i perioden med et omfang, der kræver en særskilt risikovurdering.

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. Revisionserklæringen udarbejdes efter ISAE 3000 standarden eller

tilsvarende, og der skal opnås en høj grad af sikkerhed efter denne standard. Protokollatet skal 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 valideringspolitikken skal således være opfyldt, før løsningen kan siges at leve op til valideringspolitikken.

Det er tillidstjenesteudbyderens ansvar at udforme alle relevante procedurer og kontroller til sikring af, at kravene i valideringspolitikken 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.

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.