DIGITALISERINGSSTYRELSEN

National eID-gateway

Marts 2022
Version 1.2

Vilkår for tjenesteudbyderes tilslutning til DK eIDAS Connector
Bilag A – Detaljerede sikkerhedskrav

1. Krav til identifikation og sikkerhedsvalideringer

Tjenesteudbyder skal identificere sig overfor DK eIDAS Connector med et virksomhedscertifikat eller et funktionscertifikat. Dette skal også anvendes til at signere den OIOSAML autentifikationsforespørgsel, der sendes til DK eIDAS Connector.

DK eIDAS Connector identificerer sig overfor tjenesteudbyder med et virksomhedscertifikat. Tjenesteudbyder skal validere at det er DK eIDAS Connector, som tjenesteudbyder forespørger inden forespørgslen sker.

Tjenesteudbyder skal validere, at der sendes en korrekt OIOSAML authentication request af sted til DK eIDAS Connector. Tjenesteudbyder skal ved modtagelsen validere at den modtagne SAML assertion, der indeholder svar eller fejlmeddelelser, overholder det aftalte XML skema.

Det er tjenesteudbyders ansvar at sørge for fornyelse af certifikater. Tjenesteudbyderen afholder selv udgifter forbundet med anskaffelse samt fornyelse af tjenesteudbyders virksomhedscertifikat eller funktionscertifikat. Et certifikat skal som regel fornyes hvert andet år. Ved overgang til nyt certifikat skal tjenesteudbyder meddele sine tekniske oplysninger til Digitaliseringsstyrelsen via e-mail til funktionspostkassen eidas@digst.dk. Herunder skal tjenesteudbyder angive dato og tidspunkt for, hvornår det nye certifikat skal tages i anvendelse.

2. Krav til persondata

Brugeren tilgår en dansk tjenesteudbyder. Tjenesteudbyder anmoder gennem DK eIDAS Connector den danske eID-gateway om at autentificere en bruger med et eID fra en anden EU-/EØS-medlemsstat end Danmark. Den danske eID-gateway sender denne forespørgsel videre til den af brugeren udpegede EU-/EØS-medlemsstat, som leverer en positiv eller negativ autentifikation. Digitaliseringsstyrelsen er dataansvarlig og dermed ansvarlig for datas korrekthed og adgang til data, der behandles i den danske eID-gateway.

Hvis autentifikationen er positiv medsendes dataattributter om brugeren, som er fastlagt i eIDAS forordningen. Der medsendes de attributter, som tjenesteudbyderen har specificeret at ville modtage ved tilslutning til den danske eID-gateway. Attributterne er af Digitaliseringsstyrelsen klassificeret som almindelige persondata og CPR-atributten som følsom persondata.

DIGITALISERINGSSTYRELSEN

En bruger kan gøre brug af sine rettigheder over for Digitaliseringsstyrelsen i forbindelse med Digitaliseringsstyrelsens behandling af personoplysninger. En bruger kan ligeledes gøre brug af sine rettigheder over for tjenesteudbyderne i forbindelse med deres behandling af personoplysninger.

2.1 Stillingtagen til attributter

I tilslutningsvejledningens "Vejledning i tilslutning til integrationstestmiljøet for eID-gateway" Bilag I, bedes I tage stilling hvilke attributter I har behov for at få tilsendt af den udenlandske IdP, ved brugerens autentifikation mod jeres løsning.

Det er et krav, at videregivelse af CPR-numre fremgår af lov eller af bestemmelser fastsat i henhold til lov. Er dette ikke tilfældet, kan DIGST ikke lovligt videregive denne personoplysning.

3. Krav til fortrolighed og integritet

Datatransporten fra tjenesteudbyders it-system og til DK eIDAS Connector skal krypteres med mindst AES 256 bit således at data ikke kan kopieres eller ændres. Der skal anvendes tovejs TLS (Transport Level Security). Hvis tjenesteudbyder signerer de metadata, som tjenesteudbyder skal levere til DK eIDAS Connector for at blive tilsluttet den danske eID-gateway, skal tjenesteudbyder anvende SHA 256 som digest algoritme og signatur algoritme.

4. Krav til håndtering af brugersessioner

Tjenesteudbyders forespørgsel til DK eIDAS Connector skal være sikret mod fjendtligt angreb af enhver kendt karakter som fx injections, session-hijacking, overflows etc. Tjenesteudbyder skal sikre, at it-systemet lukker den benyttede session, når der er modtaget et svar fra DK eIDAS Connector.

5. Krav til logning og håndtering af sikkerhedshændelser / incidents

Tjenesteudbyder skal med henblik på fejlsøgning og efterforskning af sikkerhedshændelser logge transportkommunikationen mellem tjenesteudbyder og DK eIDAS Connector. Denne log må ikke indeholde de transporterede persondata, men alene oplysninger om hændelsesforløbet i transporten mellem tjenesteudbyders it-system og DK eIDAS Connectoren. Logningen er specificeret i eID's dokument "eID-gateway Logningspolitik".

Tjenesteudbyder skal omgående underrette Digitaliseringsstyrelsen om sikkerhedshændelser, der opstår i forbindelse med kommunikation til og fra DK eIDAS Connector. Tjenesteudbyder skal underrette Digitaliseringsstyrelsen om sikkerhedshændelser i egne systemer, der har eller kan få betydning for den danske eID-gateway herunder sikkerhedshændelser vedrørende brugere, der logger på it-systemet via den danske eID-gateway.

DIGITALISERINGSSTYRELSEN

6. Beredskab

Det er tjenesteudbyders eget valg, om man ønsker at etablere en nødprocedure eller et nødberedskab til håndtering af eventuelle nedbrud i den danske eID-gateway. Der henvises i øvrigt til dokumentet "Beredskabspolitik".

7. Versionshistorik

Version	Dato	Initialer	Indhold/ændringer
1.0	29.06.2018	OSBUH	Første version til offentliggørelse
1.1	10.02.2021	IDAWI	Indsættelse af afsnit *2.1 Stillingtagen til attributter*
1.2	09.03.2022	IDAWI	Henvisninger er blevet tilpasset og krav til modtagelse af CPR-nummer er blevet tydeliggjort.