DIGITALISERINGSSTYRELSEN

NemLog-in

Bilag 3 Regler og vilkår for Tjenesteudbyderes brug af NemLog-in Services

Version 1.1

Indholdsfortegnelse

1 Indledning

Dette bilag indeholder de vilkår, som Tjenesteudbydere skal opfylde for at anvende Services fra NemLog-in.

I bilaget benyttes Leverandør som betegnelse for den leverandør, som Tjenesteudbyder på baggrund af egen aftale modtager Autentifikationer fra. En Leverandør kan således både være Broker, Tredjepartsbroker eller Multi-tenant leverandør.

Leverandøren skal indarbejde det i bilaget anførte i sine aftaler med Tjenesteudbydere, således at Tjenesteudbyderne bliver forpligtet heraf.

Vilkårene kan ændres og opdateres løbende, jf. Brokeraftalens punkt 17. Broker skal sikre, at ændringerne videreføres i Brokers aftaler med Aktører.

Punkt 11 skal alene indarbejdes i aftaler, der indgås mellem Tjenesteudbydere og en Multi-tenant leverandør i rollen som Leverandør.

2 Sikkerhedskrav

Tjenesteudbyder skal opfylde de sikkerhedskrav, der er anført på NemLog-in's Tjenesteudbydersite (https://tu.nemlog-in.dk/). Tjenesteudbydere må desuden ikke i anden sammenhæng udsætte NemLog-in og tilknyttede løsninger, herunder MitID-løsningen for sikkerhedsrisiko med hensyn til ægthed, integritet og fortrolighed.

Tjenesteudbyder er forpligtet til at underrette Slutbrugere og Leverandøren om eventuelle sikkerhedsbrud relateret til anvendelsen af NemLog-in.

3 Tekniske krav

Tjenesteudbyder er forpligtet til at opfylde de tekniske krav anført på NemLog-in's tjenesteudbydersite (https://tu.nemlog-in.dk/), der retter sig mod Tjenesteudbydere.

4 Anvendelse af NemLog-in Autentifikation

4.1 Afledte identiteter

Hvis Tjenesteudbyder benytter en Autentifikation fra NemLog-in til at etablere en afledt identitet (fx en alternativ login-mekanisme til egen Selvbetjeningsløsning baseret på den oprindelige NemLog-in Autentifikation), må en sådan Autentifikation ikke fremstilles, omtales eller på anden måde gengives som en Autentifikation fra NemLog-in eller en Autentifikation fra af identifikationsordninger, som NemLog-in formidler, herunder MitID.

Digitaliseringsstyrelsen kan på ingen måde gøres ansvarlig for sikkerhed eller andre forhold relateret til en sådan lokal Autentifikation i en Selvbetjeningsløsning. Dette indebærer bl.a., at oplysninger om evt. spærring, suspendering af en Slutbrugers identifikationsmiddel eller yderligere forhold om identiteten knyttet hertil ikke længere har effekt over for Tjenesteudbyderen.

Tjenesteudbyderen skal være opmærksom på sikkerhedsaspekterne vedrørende sådanne autentifikationer, herunder at Tjenesteudbyderen selv er ansvarlig og bærer risikoen for sådanne autentifikationers validitet og sikkerhedsmæssig kvalitet.

4.2 Maksimal sessionslængde

Den samlede sessionslængde for en NemLog-in Autentifikation hos en Tjenesteudbyder må maksimalt have en udstrækning på 8 timer, hvorefter Slutbrugeren skal re-autentificeres via NemLog-in.

Tjenesteudbyder kan dog forlænge sessionen ud over de 8 timer, hvis følgende krav er opfyldt:

1. Slutbrugeren er aktiv under hele sessionen, jf. krav om sessionsafslutning ved inaktivitet
2. Der er et konkret sagligt forretningsbehov for at den pågældende session skal have en sessionslængde på mere end 8 timer, herunder at formålet med Slutbrugerens Autentifikation og anvendelse af den Digitale Selvbetjeningsløsning fortabes, hvis sessionen ikke kan opretholdes
3. Det er ikke muligt med rimelige midler at indrette den Digitale Selvbetjeningsløsning, således at forretningsbehovet fortsat kan opfyldes inden for en maksimale sessionslængde på 8 timer.

4.3 Anvendelse af sikringsniveauer

Tjenesteudbyder er ansvarlig for at sikre, at sikringsniveauet i autentifikationssvaret fra NemLog-in er tilstrækkeligt til at dække det konkrete behov i Tjenesteudbyders Digitale Selvbetjeningsløsning.

5 Anvendelse af kendetegn

Den visuelle identitet og de designkomponenter, der stilles til rådighed NemLog-in infrastrukturen, må alene anvendes i forbindelse med Autentifikation via NemLog-in. Det er ikke tilladt for Tjenesteudbyderen at anvende disse til understøttelse af egne eller tredjeparts services.

Tjenesteudbyderen er forpligtiget til at overholde de gældende regler for brug af NemLog-in's og MitID's kendetegn (herefter blot kendetegn), herunder navne, logoer og domænenavne samt øvrigt materiale med tilknytning til Partnerskabet og MitID.

Retningslinjer for UX/UI og kommunikation relateret til NemLog-in og MitID fremgår af Tjenesteudbydersitet.

Tjenesteudbydere har en brugsret til kendetegn og er forpligtet til at anvende disse kendetegn i forbindelse med, at der tilbydes Autentifikation via NemLog-in løsningen og markedsføring heraf.

Retningslinjerne kan ændres, og kendetegn kan ændres helt eller delvist. Tjenesteudbyderne er forpligtet til løbende at holde sig opdateret herom og opfylde de til enhver tid gældende retningslinjer.

Tjenesteudbyderen er ved ophør af aftale om at benytte Autentifikation fra NemLog-in forpligtet til at fjerne enhver henvisning til kendetegn og ophøre med brugen heraf, medmindre anden aftale indgås med en rettighedshaver.

6 Vilkår for Tjenesteudbyders opkrævning af vederlag

Tjenesteudbyderen må ikke opkræve vederlag fra Slutbrugere for Autentifikation eller signering fra NemLog-in.

7 Spærring af adgang til NemLog-in

Tjenesteudbyderes adgang til Autentifikation og øvrige ydelser kan spærres af Leverandøren, hvis Tjenesteudbyderen i væsentligt omfang ikke opfylder de i dette bilag angive krav til Tjenesteudbyderen, eller hvis Tjenesteudbyderens adfærd i øvrigt udgør en sikkerhedsrisiko eller såfremt Tjenesteudbyderen udviser

en adfærd, der i væsentligt omfang påvirker eller er egnet til at påvirke Slutbrugernes opfattelse af NemLog-in og tilknyttede løsninger, herunder MitID-løsningen negativt.

Leverandøren er i øvrigt berettiget til at videreføre en spærring fra Digitaliseringsstyrelsen, herunder spærringer der er begrundet i væsentlige sikkerhedsmæssige grunde.

8 Certifikater og signering

8.1 Anvendelse af NemLog-in Digital Signering

Såfremt Tjenesteudbyder med rimelighed forlader sig på en kvalificeret elektronisk signatur eller et kvalificeret elektronisk segl og tilhørende certifikat fra NemLog-in Digital Signering, er Digitaliseringsstyrelsen erstatningsansvarlig for tab efter dansk rets almindelige regler.

For de i Certifikatpolitikkens krav 9.6.1-04 anførte forhold er Digitaliseringsstyrelsen ansvarlig for tab, medmindre Digitaliseringsstyrelsen kan løfte bevisbyrden for ikke at have handlet forsætligt eller uagtsomt.

Digitaliseringsstyrelsens erstatningsansvar efter denne bestemmelse er begrænset til 100.000 kr. for hver tabsgivende begivenhed og er i alle tilfælde maksimeret til 100.000 kr. årligt. Ved en tabsgivende begivenhed anses alle forhold, der udspringer af samme fortsatte eller gentagne ansvarspådragende forhold.

Ovenstående begrænsning er kun gældende, såfremt misligholdelsen ikke kan henføres til grov uagtsomhed eller forsætlige forhold.

8.2 Tjenesteudbyders pligt ved modtagelse af et certifikat

Forud for at have tillid til et certifikat fra den Danske Stat – Tillidstjenester, skal Tjenesteudbyder som modtager af en signatur sikre sig følgende:

- At certifikatet er gyldigt - dvs. ikke opført på Den Danske Stats Tillidstjenesters spærreliste på tidspunktet for signeringen,
- at det formål, certifikatet søges anvendt til, er passende i forhold til evt. anvendelsesbegrænsninger i certifikatet samt
- at anvendelsen af certifikatet i øvrigt er passende i forhold til niveauet af sikkerhed, som er beskrevet i certifikatpolitikken for det pågældende certifikat

Inden et tidsstempel (såfremt et tidsstempel indgår i det signerede dokument) accepteres, skal Tjenesteudbyder som modtager af en signatur sikre sig følgende:

- at tidsstemplet er korrekt signeret, og at den private nøgle, der bruges til at signere tidsstemplet, ikke er blevet markeret som kompromitteret på kontroltidspunktet,
- at anvendelsen sker inden for eventuelle begrænsninger for brugen af tidsstemplet angivet i tidsstempelpolitikken og
- at andre forholdsregler, der er angivet i aftaler eller lignende, er opfyldte.

9 Krav fra Tjenesteudbydere

Ethvert krav fra Tjenesteudbydere, der relaterer sig til NemLog-in Services skal rettes imod Leverandøren. Undtaget herfra er dog krav, der relaterer sig til fejl i signaturer eller segl fra NemLog-in Digital Signering, der skal rettes mod Digitaliseringsstyrelsen.

10 Særlige forhold for Offentlige Tjenesteudbydere

Offentlige Tjenesteudbyderes modtagelse af Autentifikation fra NemLog-in via Leverandøren er reguleret af Lov om MitID og NemLog-in, herunder bekendtgørelse om tilrådighedsstillelse og anvendelse af MitID-løsningen og NemLog-in. De beføjelser, som Digitaliseringsstyrelsen har i medfør af Bekendtgørelsen er gældende uanset, at Autentifikationer modtages via Leverandøren. Beføjelserne kan udmøntes af Digitaliseringsstyrelsen gennem Leverandøren.

11 Behandling af personoplysninger

[Obs! Dette punkt er alene gældende for Tjenesteudbydere, der modtager Autentifikation fra en Multi-tenant leverandør. I det omfang, at én eller flere de i punktet adresserede oplysninger ikke videreformidles fra broker til Multi-tenant leverandøren, kan de undtages fra databehandleraftalen.]

Det skal af Tjenesteudbyders databehandleraftale med Leverandøren fremgå, at Leverandøren som databehandler behandler følgende oplysninger om Slutbruger som led i modtagelsen af autentifikationssvaret fra NemLog-in:

- Navn og CPR-nummer (hvis CPR-nummer er registreret),
- E-mailadresse (erhvervsbrugere)
- Pseudonym (erhvervsbrugere)
- PID og RID
- CVR-nummer (erhvervsbrugere)
- Sikringsniveau
- NemLog-in identifikationsnummer på den elektroniske identitet (UUID)

Nærmere detaljer om de pågældende oplysninger fremgår af seneste version af OIOSAML Web SSO Profile.

Leverandøren må ikke behandle autentifikationssvar på anden måde eller til andre formål end hvad der følger af lov om MitID og NemLog-in, medmindre Tjenesteudbyder har et selvstændigt hjemmelsgrundlag for behandlingen af autentifikationssvar.