Signaturgruppen

Servicebeskrivelse

Signaturgruppen IdP

Maj 2024

Servicebeskrivelse

Stamdata for ID-tjenesten

ID-tjenestens kaldenavn: "Signaturgruppen IdP"

ID-tjenestens ansvarlige ejer: Signaturgruppen A/S, CVR: 29915938

ID-tjenestens hjemmeside (Servicebeskrivelse, privatlivspolitik, teknisk dokumentation, driftstid og driftskontakt): https://signaturgruppen.dk

ID-tjenestens kontaktinformation:

Telefon:	70256425
Kontakt navn:	Niels Frimodt Sørensen
Kontakt e-mail:	Support@signaturgruppen.dk

Betingelser

Ansvar hos Relying Party (Tjenesteudbyder)

En tjenesteudbyder må kun forlade sig på ID-tjenestens autentifikation af brugere på NSIS Sikringsniveau Betydelig når følgende er opfyldt:

- Tjenesteudbyder har gennemført en gensidig teknisk registrering imod ID-tjenesten i dialog med ID-tjenestens forretningsorganisation.
- Tjenesteudbyder har forsikret sig om, at det tilbudte sikringsniveau fra ID-tjenesten opfylder Tjenesteudbyderens sikringsbehov.
- Tjenesteudbyder har aftalt eventuel anvendelse af eventuelle autorisations-data indeholdt i ID-tjenestens security tokens med henblik på autorisation af rettigheder i tjenesteudbyderens tjeneste.
- Tjenesteudbyder har valideret ID-tjenestens security token ved hver enkelt autentifikation inkl. verifikation af digital signatur, herunder gyldighed af ID-tjenestens certifikat som angivet fra certifikatudsteder.
- Tjenesteudbyder har valideret, at tjenesteudbyder eksplicit fremgår som modtager i det modtagne security token.
- Tjenesteudbyder har uddraget og kontrolleret det aktuelle sikringsniveau, der fremgår af ID-tjenestens security token. Bemærk, at det aktuelle sikringsniveau i det modtagne security token godt kan være lavere end det af tjenesteudbyder efterspurgte sikringsniveau, eller mangle helt, hvilket indikerer overfor tjenesteudbyder, at brugerens identitet ikke er autentificeret på det efterspurgte sikringsniveau.

ID-tjenesten understøtter lokal sessionsbevarelse i henhold til mulighederne herfor i NSIS. Tjenesteudbyder er selv ansvarlig for sikkerhedsforhold omkring eventuelle egne sessionsmekanismer samt vurdering af behovet for at gennemtvinge en ny autentifikation med aktiv brugerinvolvering (dvs. fravælge SSO) jf. NSIS-kapitel 6 krav 8.

Eventuelle persondata eller personhenførbare data som modtages fra ID-tjenesten, skal af tjenesteudbyderen behandles i henhold til den enhver tid gældende lovgivning.

Ansvar hos bruger

En bruger, der benytter ID-tjenesten, registrerer sig i systemet, og bekræfter i den forbindelse eksplicit ID-tjenestens brugervilkår.

Brugeren bekræfter herunder at vedkommende:

- Alene anvender det elektroniske identifikationsmiddel i overensstemmelse med ID-tjenestens politikker (herunder politikker for brug og evt. længde af kodeord).
- Ikke overdrager sit elektroniske identifikationsmiddel til andre.
- Giver fyldestgørende og korrekte svar på alle anmodninger om information i ansøgningsprocessen.
- Tager rimelige forholdsregler for at beskytte sit elektroniske identifikationsmiddel (herunder ved evt. sikkerhedskopiering)
- Omgående anmoder om spærring af sit elektroniske identifikationsmiddel i tilfælde af kompromittering eller mistanke om kompromittering af dette.
- Omgående anmoder om fornyelse af sit elektroniske identifikationsmiddel, hvis indholdet af dette ikke længere er i overensstemmelse med de faktiske forhold (herunder oplysninger afgivet under registreringsprocessen, som indgår i elektroniske identifikationsmidler).

Ansvar hos brugerorganisation

En brugerorganisation forpligter sig ved aftale med ID-tjenesten til at:

- Have indsamlet korrekt information om sine brugere før de registreres i systemet.
- Fjerne forbindelsen hurtigst muligt imellem bruger og brugerorganisation, hvis brugeren ikke længe kan associeres til brugerorganisationen.
- Orientere ID-tjenesten eller fjerne forbindelsen mellem bruger og brugerorganisation, hvis det mistænkes at brugeren er blevet kompromitteret.
- Orientere ID-tjenesten i tilfælde af, at brugerorganisationen går konkurs.

Begrænsninger

Security tokens fra ID-tjenesten må alene anvendes til at autentificere brugere på det i det enkelte security token oplyste NSIS sikringsniveau, når tjenesteudbyder opfylder sit ansvar som beskrevet ovenfor.

Security tokens fra ID-tjenesten må ikke uden tilladelse fra ID-tjenesten anvendes til at udstede andre security tokens, men må kun anvendes direkte af tjenesteudbyder i forbindelse med tjenesteudbyders forretningsfunktionalitet. En sådan tilladelse er dog givet til NemLog-in, til anvendelse i forbindelse med NemLog-in erhvervsidentiteter overfor NemLog-ins tilsluttede brokere og tjenesteudbydere.

ID-tjenesten og ID-tjenestens udbyder ifalder ikke yderligere ansvar end hvad der måtte følge af NSIS.

Betaling

Betaling er beskrevet i standardaftalerne for brugerorganisationer.

Privatlivspolitik

ID-tjenestens til enhver tid gældende privatlivspolitik kan hentes på ID-tjenestens hjemmeside som angivet under ID-tjenestens stamdata.