DIGITALISERINGSSTYRELSEN

NemLog-in

Integrationsvejledning til NemLog-in Signering - Legacy

Indholdsfortegnelse

Ændringslog

Dato	Version	Ændringsbeskrivelse	Initialer
2013	1.0		TG
23.11.2021	2.0	Opdatering af vejledningen samt formatering	TG/LEASA

1 Om denne guide

Denne guide indeholder en kort beskrivelse af, hvorledes man som tjenesteudbyder (eller it-leverandør til en tjenesteudbyder) kan integrere en it-løsning til NemLog-in's Signeringstjeneste (herefter blot benævnt *signeringstjenesten*).

Bemærk: guiden omhandler NemLog-in's legacy signeringstjeneste, hvor slutbrugere kan underskrive med NemID. Ønsker man at lade slutbrugere signere med MitID skal NemLog-in's nye signeringstjeneste anvendes.

Guiden er henvendt til teknisk-orienterede personer, der skal planlægge eller udføre integrationen, og den beskriver processen for tilslutning samt de snitflader, som anvendes. Læseren antages at være bekendt med basal terminologi inden for føderationer og brugerstyring.

2 Formålet med signeringstjenesten

Formålet med signeringstjenesten er at tilbyde tjenesteudbydere en fælles, digital løsning, hvormed man med NemID kan indhente en digital signatur fra en bruger på en aftaletekst eller indberetning, hvor der efterfølgende er en høj grad af sporbarhed og teknisk dokumentation for underskriften. Situationen er velkendt fra netbanker, hvor brugeren typisk skal underskrive kontooverførsler og betalinger, inden de effektueres af banken.

Ved at anvende signeringstjenesten slipper tjenesteudbydere for selv at etablere en brugergrænseflade til signering samt for at validere signaturen og etablere en sikker logning af signaturbeviset. Signeringstjenesten gør det således nemmere og billigere at digitalisere områder, hvor man normalt ville bede borgere og virksomheder om papirbaseret underskrift, og hvor der er behov for høj troværdighed og dokumentation omkring, hvad der blev underskrevet af hvem og hvornår.

3 Løsningens komponenter

NemLog-in's signeringstjeneste består af to komponenter, som frit kan anvendes af tjenesteudbydere:

a) Der tilbydes en web-applikation, som står for alt arbejde med at få indhentet en underskrift via brugerens browser. Denne løsning er henvendt til browser-baserede applikationer og fungerer ved at disse foretager et redirect af browseren til signeringstjenesten, som gennemfører et signeringsflow, og herefter foretager et redirect tilbage til applikationen (til et URL valgt af denne).

b) Der tilbydes en web service, som kan bruges til at validere en indhentet signatur fra en bruger (på XML dSig format) samt logge et signaturbevis. Web servicen er beregnet til applikationer, som selv står for brugerinteraktionen i forbindelse med indhentning af brugerens signatur (f.eks. rige klienter), og som blot vil anvende signeringstjenesten til validering og logning.

Bemærk: Det er i signeringstjenesten muligt både at underskrive med privat NemID samt med en NemID medarbejdersignatur.

4 Tilslutning til Signeringstjenesten

Før man som tjenesteudbyder (eller it-leverandør på vegne af en tjenesteudbyder) kan anvende signeringstjenesten, skal man være tilsluttet denne. Tilslutning foregår konkret via NemLog-in's tilslutningssystem, der er en selvbetjeningsportal. Se evt. mere om tilslutningsprocessen på NemLog-in's supportsite: https://tu.nemlog-in.dk/tilslutning/

Ved tilslutning til signeringstjenesten skal man dels underskrive vilkår for anvendelse af løsningen – og dels skal man uploade det OCES funktions- eller virksomhedscertifikat, man vil identificere sig med overfor NemLog-in. Begge snitflader kræver således autentifiktion af tjenesteudbyderen via en digital signatur, hvor det tilhørende certifikat på forhånd skal være registreret i NemLog-in. Hvis it-løsningen i forvejen har uploadet SAML metadata ved tilslutning til NemLog-in's log-in-løsningen, kan man i tilslutningssystemet angive, at signeringscertifikatet fra SAML metadata genanvendes – alternativt kan man angive et nyt certifikat.

5 Miljøer

Signeringstjenesten er tilgængelig i NemLog-in's integrationstestmiljø og i produktionsmiljøet. Integrationstestmiljøet bruges til at teste, at it-systemet har implementeret snitfladen mod signeringstjenesten korrekt inden idriftsættelse.

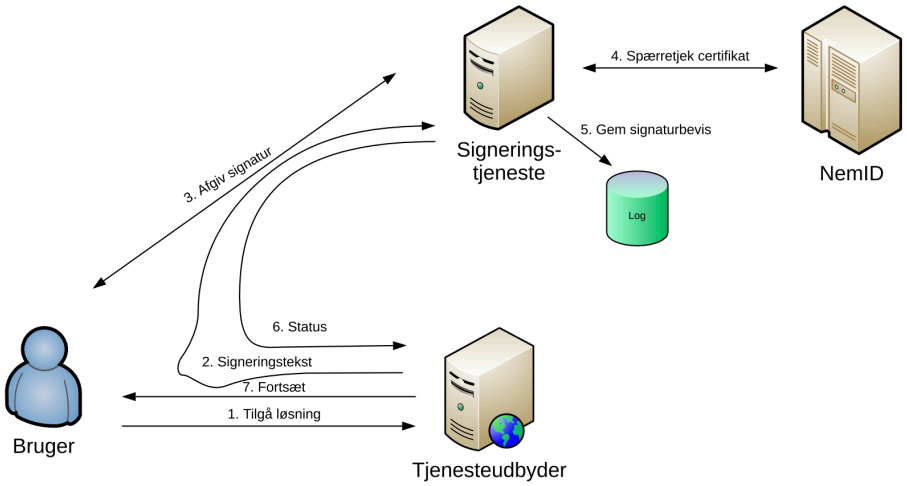
Adresserne på signeringstjenestens end-points er vist i nedenstående tabel:

INTEGRATIONSTEST	
Web applikation	`https://signering.test-nemlog-in.dk/signer.aspx`
Web Service	`https://signingservice.signering.test-nemlog-in.dk/SigningService.svc`
PRODUKTION	
Web applikation	`https://signering.nemlog-in.dk/signer.aspx`
Web Service	`https://signingservice.signering.nemlog-in.dk/SigningService.svc`

Digitaliseringsstyrelsen stiller krav om, at tjenesteudbydere tester integrationen inden idriftsættelse via nogle foruddefinerede test cases. Disse test cases kan findes på www.tu.nemlog-in.dk.

6 Snitflader og flows

De tekniske snitflader, der skal integreres mod, findes beskrevet på NemLog-in's supportsite for tjenesteudbydere[1].

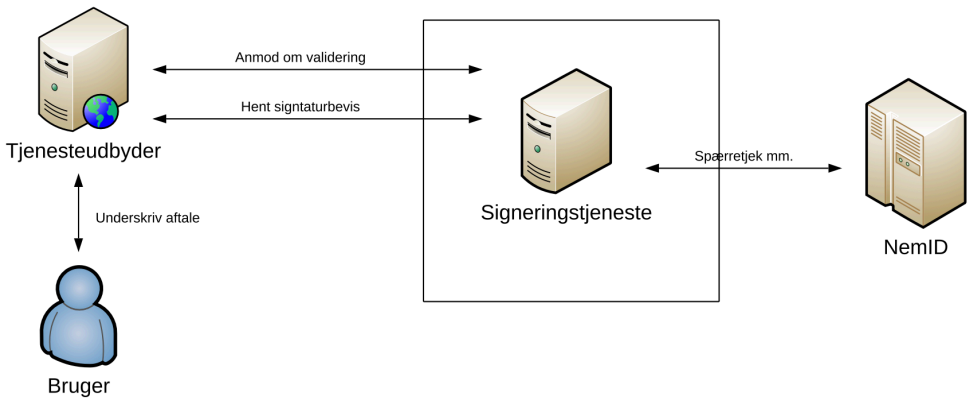


1) Brugeren tilgår en side hos tjenesteudbyderen, der kræver underskrift på en tekst (f.eks. i forbindelse med bekræftelse af en indberetning).
2) Browseren re-dirigeres til signeringstjenesten med information om den tekst, der skal underskrives, samt en række øvrige parametre.
3) Brugeren præsenteres af signeringstjenesten for den tekst, der ønskes underskrevet, og afgiver en digital signatur (via Nets DanID's signeringsklient).
4) Signeringstjenesten validerer brugeren signatur.
5) Signeringstjenesten etablerer og logger bevis for den afgivne signatur og validering (i dedikeret hardwareløsning, der forhindrer manipulation af loggen).
6) Signeringstjenesten foretager re-direct af browseren tilbage til tjenesteudbyderens løsning med information om status. Svaret fra signeringstjenesten er digitalt underskrevet.
7) Tjenesteudbyderen validerer svaret fra signeringstjenesten[2], foretager egen logning, og kan fortsætte interaktionen med brugeren.

[1] https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/signering/hjaelp-og-vejledning/

[2] Se dokumentation for snitfladerne for detaljerede krav til validering og logning.

Nedenstående figur viser det typiske forløb ved anvendelse af web-servicegrænsefladen:



6.1 Dobbeltsigneringer mv.

NemLog-in's signeringstjeneste holder ikke styr på tilstande og arbejdsgange for tjenesteudbydere. I de tilfælde, hvor en tjenesteudbyder ønsker flere brugeres underskrift på samme dokument, skal tjenesteudbyderen derfor selv etablere et workflow, som sender begge brugere over til NemLog-in's signeringstjeneste med samme signeringstekst. Når begge brugere (uafhængigt af hinanden) har underskrevet samme tekst, og et succesfuldt svar fra NemLog-in er modtaget på begge, kan applikationen fortsætte med transaktionen.

7 Yderligere informationer

NemLog-in3 på Digitaliseringsstyrelsens hjemmeside:

https://digst.dk/it-loesninger/nemlog-in/om-loesningen/aendring-i-funktionaliteter/implementeringssite/infrastrukturbeskrivelse/nemlog-in3-projektet/

NemLog-in's supportsite for tjenesteudbydere: https://tu.nemlog-in.dk

8 Referencer

[OIO-SAML] ”OIO Web SSO Profile V3”, Digitaliseringsstyrelsen.

https://digst.dk/it-loesninger/nemlog-in/anvendelse/oiosaml-302/

[OIO-BPP] ”OIO Basic Privilege Profile”, Digitaliseringsstyrelsen.
https://digst.dk/it-loesninger/nemlog-in/anvendelse/oiosaml-302/