DIGITALISERINGSSTYRELSEN

14. november 2013
TG

Guide til integration med NemLog-in / Signering

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

Formålet med signeringstjenesten

Formålet med signeringstjenesten er at tilbyde myndigheder en fælles, digital løsning, hvormed man 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 it-systemudbydere 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.

Løsningens komponenter

NemLog-in's signeringstjeneste består af to komponenter, som frit kan anvendes af myndigheder (og it-leverandører på vegne af myndigheder)[1]:

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).

[1] Løsningen kan som de øvrige NemLog-in komponenter ikke benyttes af private virksomheder til løsninger, med mindre de etableres for en offentlig myndighed.

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.

Tilslutning til Signeringstjenesten

Før man som myndighed (eller it-leverandør på vegne af en myndighed) kan anvende signeringstjenesten, skal man være tilsluttet denne. Tilslutning foregår konkret via NemLog-in's tilslutningssystem, der er en selvbetjeningsportal for bl.a. myndigheder og deres it-leverandører. Den er planlagt til idriftsættelse ultimo august 2013, og indtil dette tidspunkt kan tilslutning ske manuelt ved kontakt til Digitaliseringsstyrelsen på nemlogin@digst.dk.

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 it-systemudbyderen 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.

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`

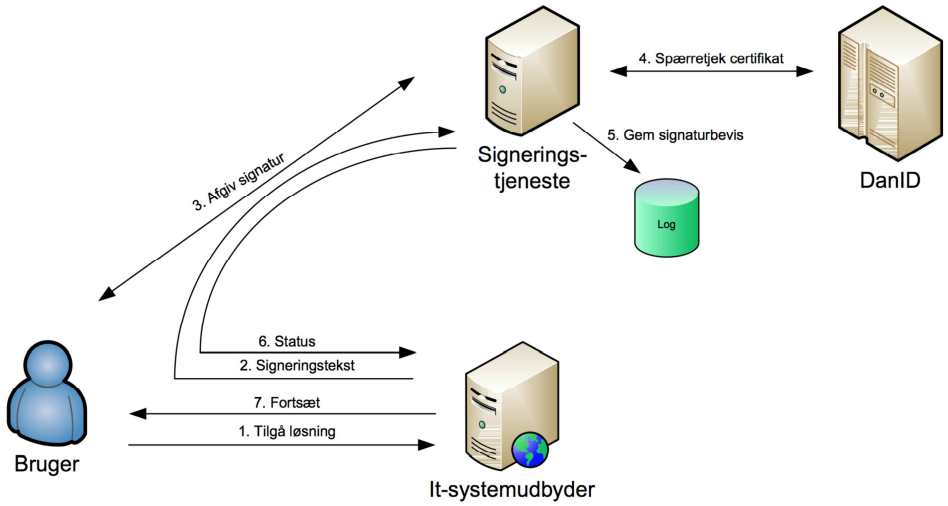
Produktion	
- Web applikation	`https://signering.nemlog-in.dk/signer.aspx`
- Web Service	`https://signingservice.signering.nemlog-in.dk/SigningService.svc`

Digitaliseringsstyrelsen stiller krav om, at it-systemudbydere tester integrationen inden idriftsættelse via nogle foruddefinerede test cases. Disse test cases kan findes på NemLog-in's side på digitalisér.dk[2].

Snitflader og flows

De tekniske snitflader, der skal integreres mod, findes beskrevet på NemLog-in's testportal[3]:

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



Forløbet er flg.:

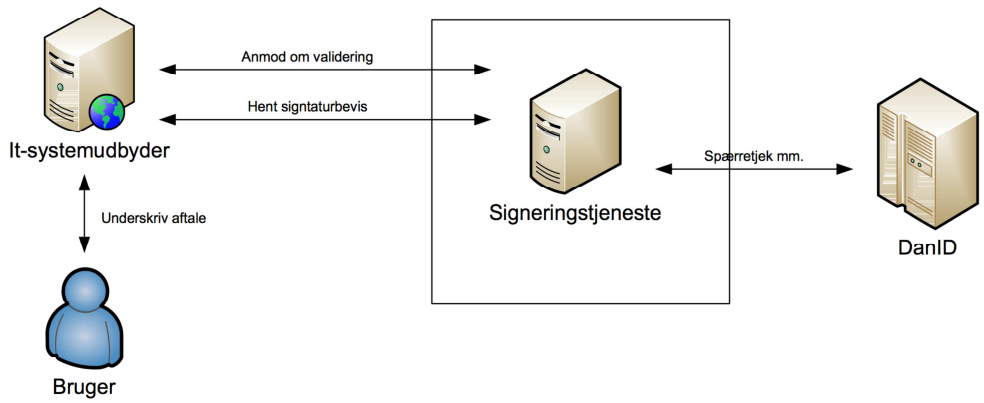
1. Brugeren tilgår en side hos it-systemudbyderen, der kræver underskrift på en tekst (f.eks. i forbindelse med bekræftelse af en indberetning).
2. Browseren re-dirigeres til signeringstjenesten med information om den tekst, der skal underskrives, samt en række øvrige parametre.

[2] https://digitaliser.dk/resource/2553483

[3] https://test-nemlog-in.dk/Testportal/dokumenter/NemLog-in2%20-%20signing%20service.pdf

3. Brugeren præsenteres af signeringstjenesten for den tekst, der ønskes underskrevet, og afgiver en digital signatur (via DanID's signeringsapplets).
4. Signeringstjenesten validerer brugeren signatur bl.a. via dialog med DanID.
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 it-systemudbyderens løsning med information om status. Svaret fra signeringstjenesten er digitalt underskrevet.
7. It-systemudbyderen validerer svaret fra signeringstjenesten[4], foretager egen logning, og kan fortsætte interaktionen med brugeren.

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



Dobbeltsigneringer mv.

NemLog-in's signeringstjeneste holder ikke styr på tilstande og arbejdsgange for myndighedsapplikationer. I de tilfælde, hvor en myndighed ønsker flere brugeres underskrift på samme dokument, skal myndigheden 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.

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

Bagudkompatibilitet til signeringstjenesten på Virk.dk

NemLog-in's signeringstjeneste erstatter den signeringstjeneste, som hidtil har eksisteret på Virk.dk portalen. Ved design af den nye tjeneste er det tilstræbt, at grænsefladen ligner den gamle grænseflade så meget som muligt. Der er dog en række mindre ændringer til grænsefladen, som bl.a. er sikkerhedsmæssigt begrundet, så derfor vil der være behov for tilretning løsninger, der tidligere har anvendt Virk's signeringstjeneste. Der henvises til snitfladebeskrivelsen for yderligere detaljer.

De oplysninger, som Virk.dk historisk har registreret om løsninger, der anvender Virk's signeringstjeneste, bliver migreret til NemLog-in's signeringstjeneste. Det betyder, at disse løsninger ikke behøver at tilslutte sig NemLog-in's signeringstjeneste (og herunder registrere deres certifikat) – de skal dog tilpasses ændringerne i snitfladen til signeringstjenesten.

Yderligere informationer

Digitaliseringsstyrelsens hjemmeside:
http://www.digst.dk/loesninger-og-infrastruktur/NemLogin

Digitaliser.dk:
https://digitaliser.dk/network/2549480

NemLog-in's testportal:
https://test-nemlog-in.dk/testportal/

Referencer

[OIO-SAML] ”OIO Web SSO Profile V2.0.9”, Digitaliseringsstyrelsen.
http://digitaliser.dk/resource/2377872

[OIO-BPP] ”OIO Basic Privilege Profile”, Digitaliseringsstyrelsen.
http://digitaliser.dk/resource/2377872

[VIRK-SYS] ”Systembeskrivelse - Brugerrettighedsstyringssystem VIRK”, Cap Gemini, Version 2.2, 2011-08-05.
http://myndighedsnet.virk.dk

[VIRK-PRO] ”Procesbeskrivelse - Brugerrettighedsstyringssystem VIRK”, Cap Gemini, Version 1.3.1, 4-5-2010.
http://myndighedsnet.virk.dk