DIGITALISERINGSSTYRELSEN

NemLog-in

Tekniske krav til tjenesteudbyderes anvendelse af NemLog-in3

Version 1.1

Indholdsfortegnelse

1 Dokumenthistorik 4
2 Tekniske krav og politikker 5
2.1 Definitioner 5
2.2 Ændringer til krav og politikker 7
2.3 Opsætning i NemLog-in's Administrationsportal 7
2.3.1 Tilslutning, vedligehold og frakobling 7
2.3.2 Entydigt ansvar for it-systemer 7
2.3.3 Konfiguration af attributter 8
2.4 Ansvar i relation til sikkerhed 8
2.4.1 Generelt om Tjenesteudbyderes egenorganisation 8
2.4.2 Adgangskontrol hos Tjenesteudbydere 8
2.4.3 Certifikater hos Tjenesteudbydere 8
2.5 Forbrugsvarsling 8
2.6 Test af Tjenesteudbyderes integration 9
2.7 Logningspolitik 9
2.8 Drift- og supportpolitik 9
2.9 Beredskabspolitik 10
3 Services i NemLog-in3 11
3.1 Autentifikationsservices 11
3.1.1 Sessionshåndtering og timeout 11
3.1.2 Timeout i NemLog-in 12
3.1.3 Autentifikation til 'native Apps' 12
3.1.4 Afledte identiteter 14
3.2 Opslags- og match tjenester 14
3.3 Rettighedsstyring for erhvervsbrugere 15
3.4 Digitale borgerfuldmagter 15
3.4.1 Håndtering af papirfuldmagter hos offentlige myndigheder og offentligretlige organer 17
3.5 Security Token Service 17
3.6 Integrationskrav 17
3.7 NemID Signeringstjeneste i NemLog-in ('legacy') 18
3.7.1 Type af signatur 18
Slutbrugeren kan afgive signaturer med: 18
- OCES Personcertifikat 19
- OCES Medarbejdercertifikat 19
- OCES Virksomhedscertifikat 19
3.7.2 NemID Signeringstjenestens validering af certifikater 19

3.7.3 Tjenesteudbyders pligt ved anvendelse af NemID Signeringstjenesten 19
3.7.4 Certifikattyper 19
3.8 Signering med kvalificerede signaturer og -segl 19
3.8.1 Den konkrete anvendelse af Signeringstjenesten 20
3.8.2 Signatur og segl 20
3.8.3 Angivelse af UUID 21
3.8.4 Signaturformat 21
3.8.5 Referencetekst 21
3.8.6 Digitaliseringsstyrelsens forpligtelser ved afgivelse af en elektronisk signatur eller segl 21
3.8.7 Tjenesteudbyders forpligtelser ved modtagelse af en elektronisk signatur eller segl 21
3.8.8 Sikring af dokumentation og bevisværdi for signaturer og segl 22
3.9 Validering af elektroniske signaturer og segl 22

1 Dokumenthistorik

Dato	Version	Beskrivelse af ændring	Initialer
17.09.2021	1.0	Første version klar til publicering.	TG
01.10.2021	1.1	Opdateret beskrivelse af NemID signering (underafsnit 3.7.1 til 3.7.4) samt kvalificeret signering i afsnit 3.8 med henvisning til certifikatpolitik.	TG

2 Tekniske krav og politikker

Herunder fremgår tekniske krav og politikker relateret til Tjenesteudbydere tilsluttet NemLog-in, som er underlagt og refereres fra:

- "*Bekendtgørelse om tilrådighedsstillelse og anvendelse af MitID-løsningen og NemLog-in*" for offentlige Tjenesteudbydere og
- "*Vilkår for anvendelse af NemLog-in*" for private Tjenesteudbydere.

Målgruppen for beskrivelsen er teknisk personale hos Tjenesteudbydere eller disses it-leverandører, som skal planlægge, udvikle og teste integrationer til NemLog-in samt herefter håndtere løbende drift. Det forudsættes derfor, at læseren har et vist teknisk kendskab.

For supplerende information henvises til NemLog-in's tjenesteudbydersite: http://tu.nemlog-in.dk

2.1 Definitioner

Begreb	**Beskrivelse**
Autentifikation	En elektronisk proces, som genkender og verificerer identiteten af en Slutbruger.
Administrationsportal	En selvbetjeningsløsning i NemLog-in, hvor Tjenesteudbydere kan administrere tilslutningen af deres Digitale Selvbetjeningsløsninger (it-systemer) til NemLog-in, herunder hvilke attributter, der skal leveres til Tjenesteudbyder i autentifikationssvaret samt certifikater og øvrige tekniske oplysninger relevant for integrationen.
Broker	En Juridisk enhed der videreformidler Autentifikation af digitale identiteter til tredjeparter på baggrund af en Autentifikation verificeret af brokeren selv eller evt. af en tredjepart (brokere i flere led). NemLog-in's login-tjeneste i serviceområdet login og autentifikation opererer på baggrund af en aftale med MitID Leverandøren som en MitID Broker ved at formidle MitID-autentifikationer.
Digital selvbetjeningsløsning	Et it-system, hvor privatpersoner eller erhvervsbrugere med digitale identiteter kan tilgå digital selvbetjening efter at være blevet autentificeret. Benævnes også Selvbetjeningsløsning, it-system eller tjeneste (i eIDAS forordningen).
Erhvervsbruger	En fysisk person, der er associeret med en Juridisk enhed, og som er oprettet med en erhvervsidentitet i NemID Erhverv eller MitID Erhverv (benævnt NemLog-in Erhvervsadministration i lov om MitID og NemLog-in).
Identifikationsmiddel	Et identifikationsmiddel kendetegnes som en materiel enhed, en immateriel enhed eller en kombination af disse, der anvendes til online Autentifikation. Identifikationsmidlet skal være under kontrol af den fysiske eller juridiske entitet, der har fået det udstedt. Identifikationsmidler, der kan

	autentificeres via NemLog-in vil enten være baseret på et NemID, MitID eller NSIS anmeldt identifikationsmiddel fra en Lokal IdP.
It-system	Anvendes som synonym for Digital Selvbetjeningsløsning leveret af en Tjenesteudbyder.
Kvalificeret elektronisk signatur	En kvalificeret elektronisk signatur afgivet i Signaturtjenesten på baggrund af et kvalificeret certifikat. Medmindre andet specifikt er anført omfattet betegnelsen også kvalificeret elektronisk segl, der ligeledes kan afgives i Signaturtjenesten. Kvalificerede elektroniske signaturer svarer til underskrifter afgivet af fysiske personer, hvorimod kvalificerede elektroniske segl afgives af virksomheder og tjener som bevis for at de forseglede data hidrører fra virksomheden.
Lokal IdP	Lokal autentifikationstjeneste, hvorigennem en brugerorganisation kan udstille autentifikation af egne erhvervsbrugere, der gennem NemLog-in kan videreformidles til NemLog-in's bagvedliggende tjenesteudbydere (og brokere).
MitID	Den nationale identitetsløsning, som afløser NemID. I NSIS standardens terminologi er MitID en 'elektronisk identifikationsordning'.
MitID Broker	En Broker i MitID infrastrukturen, der leverer autentifikation på baggrund af MitID evt. suppleret af yderligere ydelser. NemLog-in's login-tjeneste i serviceområdet login og autentifikation opererer som en MitID Broker.
MitID Erhverv	Serviceområdet Erhvervsadministration til brugerorganisationer i NemLog-in, der bl.a. muliggør oprettelse og administration af digitale erhvervsidentiteter og (persistente) medarbejder- og virksomhedscertifikater.
NemLog-in	Den fællesoffentlige digitale infrastrukturløsning, som sætter privatpersoner og erhvervsbrugere med digitale identiteter i stand til at interagere med digitale selvbetjeningsløsninger. NemLog-in er endvidere den nationale identitetsgarant for erhvervsidentiteter og indeholder MitID Erhverv-løsningen.
NSIS	National Standard for Identiteters Sikringsniveauer.
Sikringsniveau	Graden af tillid til en autentificeret Identitet (på engelsk "Level of Assurance") og ofte benævnt autenticitetssikringsniveau. Der opereres med tre sikringsniveauer: Lav, Betydelig og Høj.
Slutbruger	En fysisk person i form af en privatperson eller Erhvervsbruger, som kan anvende et identifikationsmiddel som grundlag for Autentifikation over for en Tjenesteudbyder.
Tjenesteudbyder	En juridisk enhed, der stiller én eller flere Digitale Selvbetjeningsløsninger til rådighed for Slutbrugere og som autentificerer disse via en Broker.

2.2 Ændringer til krav og politikker

Digitaliseringsstyrelsen er berettiget til at opdatere nærværende krav og politikker for tjenester anvendelse af NemLog-in. Ved væsentlige ændringer, der defineres som ændringer af grænseflader, der kræver ændringer i Tjenesteudbyders systemer, gives et varsel på minimum 6 måneder. Hvis ændringer skyldes afhjælpning af et akut sikkerhedsmæssigt problem, kan en kortere frist dog være nødvendig. Tjenesteudbydere afholder i alle tilfælde omkostninger til tilpasning af egne systemer.

Mindre justeringer, eksempelvis fornyelse af NemLog-in-certifikat eller indførsel af nye services eller rettigheder, betragtes ikke som en ændring af snitflader.

Ændringer i krav og politikker offentliggøres på NemLog-in's hjemmeside. Der udsendes herudover særskilt meddelelse til de Tjenesteudbydere, der på varslingstidspunktet er tilsluttet NemLog-in. Meddelelsen sendes til de e-mail-adresser, som Tjenesteudbyderne har opgivet.

2.3 Opsætning i NemLog-in's Administrationsportal

2.3.1 Tilslutning, vedligehold og frakobling

En juridisk enhed, der ønsker at anvende NemLog-in's services rettet mod Tjenesteudbydere i sin Digitale Selvbetjeningsløsning, skal først tilsluttes NemLog-in i rollen som Tjenesteudbyder. Ved tilslutning vil NemLog-in ud fra et opslag i CVR-registret afgøre, hvorvidt der er tale om en offentlig eller privat organisation. På baggrund af denne registrering sikres det, at kun relevante services for den pågældende type af tjenesteudbyder er tilgængelige for Tjenesteudbyderen og dennes it-systemer i NemLog-in's Administrationsportal. En bemyndiget for Tjenesteudbyderen skal udpege en eller flere administratorer til at håndtere opsætning i administrationsportalen.

Tjenesteudbydere er (via deres udpegede administratorer) forpligtet til ved oprettelse af deres it-systemer i NemLog-in's Administrationsportal at anvende sigende og retvisende beskrivelser samt løbende at holde disse oplysninger ajour. Forpligtelsen til ajourføring af oplysninger omfatter såvel tekniske oplysninger som fx certifikater og tekniske metadata, kontaktoplysninger på Tjenesteudbyderen, samt brugervendte beskrivelser, herunder referencetekst og alias som oplyser slutbrugere om, hvad der logges ind på i loginsituationen. Tjenesteudbyderens it-systemer skal slettes i Administrationsportalen, når de ikke længere er aktive.

De brugervendte beskrivelser skal udformes, så de er let-forståelige for den almindelige bruger uden kendskab til Tjenesteudbyderens systemer, og det anbefales at brugerteste dem med henblik på at sikre, at de fungerer i praksis. Digitaliseringsstyrelsen forbeholder sig ret til at kontakte en Tjenesteudbyder med henblik på forbedring af tekster, der ikke sikrer tilstrækkelig klarhed eller transparens for slutbrugere.

Den praktiske håndtering af it-systemer i Administrationsportalen kan evt. uddelegeres ved at udpege en ekstern it-leverandør som teknisk ansvarlig for it-systemet. En sådan it-leverandør skal ved registrering i NemLog-in acceptere særskilte vilkår.

Tjenesteudbydere er ansvarlige for alle aspekter af deres egne it-systemer (herunder funktionalitet, sikkerhed, brugervenlighed, tilgængelighed og aftestning), uanset om der til integrationen med NemLog-in anvendes en referenceimplementering fra Digitaliseringsstyrelsen eller anden type software. NemLog-in's ansvar er således alene begrænset til de services, der leveres til Tjenesteudbydere.

2.3.2 Entydigt ansvar for it-systemer

Et it-system oprettet i NemLog-in tilhører en entydig Tjenesteudbyder(organisation), der som udgangspunkt er dataansvarlig for it-systemets behandling af personoplysninger, herunder personoplysninger der modtages fra NemLog-in. Såfremt ét fysisk it-system betjener flere dataansvarlige Tjenesteudbydere (fx efter en *multi-tenant* og/eller *Software-as-a-Service* model), er det nødvendigt at oprette ét logisk it-system i NemLog-in for

hver af disse Tjenesteudbydere. Alternativt er der mulighed for at indskyde en NSIS-anmeldt broker, der kan forespørge på vegne af bagvedliggende Tjenesteudbydere samt videreformidle autentifikationen til disse.

Autentifikationsanmodninger til NemLog-in skal entydigt identificere Tjenesteudbyderen i henhold til OIOSAML-standarden. En NSIS-anmeldt broker skal indgås en særskilt aftale med Digitaliseringsstyrelsen.

2.3.3 Konfiguration af attributter

Tjenesteudbydere skal ved opsætning i Administrationsportalen aktivt tage stilling til det sæt af attributter, som deres it-systemer efterspørger fra NemLog-in. Der bør ikke i Administrationsportalen konfigureres flere attributter i it-systemers metadata, end det er nødvendigt, ud fra princippet om dataminimering. Eksempelvis bør der kun efterspørges CPR-nummer og andre globale identifikatorer, hvis der er et sagligt behov for dette. Der er forskelle på hvilke attributter, som offentlige hhv. private Tjenesteudbydere kan efterspørge - eksempelvis kan private tjenester ikke få udleveret CPR-numre fra NemLog-in. For detaljer om tilgængelige attributter henvises til integrationskrav i beskrevet i afsnit 3.6.

2.4 Ansvar i relation til sikkerhed

2.4.1 Generelt om Tjenesteudbyderes egenorganisation

Det er Tjenesteudbyderens ansvar, at sikkerheden i egen organisation og egne systemer er tilstrækkelig, og at de sikkerhedskrav, der er gældende for den pågældende Tjenesteudbyder, efterleves.

2.4.2 Adgangskontrol hos Tjenesteudbydere

Tjenesteudbydere er forpligtet til at varetage adgangskontrol i egne it-systemer, således at Slutbrugere kun opnår den adgang, de er berettiget og autoriseret til. Adgangskontrollen baseres på SAML billet udstedt af NemLog-in med information om identitet, opnået NSIS-sikringsniveau for autentifikationen og tildelte rettigheder samt fuldmagter.

Ansvarsfordelingen mellem Digitaliseringsstyrelsen og Tjenesteudbyderen er i denne situation således, at NemLog-in attesterer hvem slutbrugeren er, sikringsniveauet for Autentifikationen, samt hvilke rettigheder og fuldmagter brugeren evt. er tildelt i NemLog-in, mens Tjenesteudbyderens adgangskontrol i egen løsning på denne baggrund beslutter, hvilke data og hvilke handlinger slutbrugeren kan tilgå/foretage i Tjenesteudbyderens it-system.

2.4.3 Certifikater hos Tjenesteudbydere

Tjenesteudbydere er ansvarlige for at anskaffe, forny og registrere egne certifikater - dette gælder både certifikater anvendt i integrationen mod NemLog-in samt øvrige formål, herunder eksempelvis certifikater anvendt på Tjenesteudbyderens hjemmeside. Certifikater skal anvendes i overensstemmelse med de certifikatpolitikker, de er udstedt i medfør af. Bemærk at OIOSAML standarden stiller specifikke krav til tilladte CA'er og nøglelængder for certifikater anvendt til SAML-integrationen, og at disse krav udelukker anvendelse af selvsignerede certifikater.

2.5 Forbrugsvarsling

Tjenesteudbydere skal varsle Digitaliseringsstyrelsen mindst 8 uger forud for tilslutning af it-systemer (til produktion) med spidsbelastning på over 20.000 logins per time eller ved mere end 10.000 signeringer per time, samt hvis der sker signifikante ændringer i forventet spidsbelastning af NemLog-in services for allerede tilsluttede it-systemer.

Ved uvarslet forbrugsstigning i trafikmængden forbeholder Digitaliseringsstyrelsen sig ret til teknisk at begrænse Tjenesteudbyders ressourcetræk på NemLog-in, således at der også er kapacitet til at betjene øvrige Tjenesteudbydere.

Hvis Tjenesteudbydere har en uforudsigelig og høj spidsbelastning, skal Digitaliseringsstyrelsen adviseres for dialog om anvendelse af tekniske foranstaltninger i Tjenesteudbyderens løsning, som kan udjævne trafikken (fx kø-system).

2.6 Test af Tjenesteudbyderes integration

Tjenesteudbydere er inden anvendelse af NemLog-in's produktionsmiljø forpligtet til at gennemføre en integrationstest mod NemLog-in samt uploade en testrapport herfor, der skal godkendes af NemLog-in's forvaltning forud for anvendelse af NemLog-in's produktionsmiljø. Indholdet i integrationstesten fremgår af dokumentet 'Integrationstest ved tilslutning til NemLog-in', der findes publiceret her:

- https://www.nemlog-in.dk/tu/krav/integrationstest/

Formularen som skal uploades efter gennemført test findes her:

- https://tu.nemlog-in.dk/testrapport

Dokumentet indeholder en række obligatoriske test cases, der sikrer at udvalgte aspekter af integrationen mellem NemLog-in og Tjenesteudbydere fungerer, således at den samlede føderation fremstår sammenhængende.

De beskrevne test cases dækker både offentlige og private tjenesteudbyderes anvendelse af NemLog-in services, og det er markeret, hvilke test cases der kun er relevant for offentlige tjenesteudbydere. Endvidere er det markeret, hvilke test cases, der er relevante hvis tjenesten er en 'native app'. Hvis NemLog-in anvendes til eksempelvis indrullering af en 'native app', er der en række test cases, som ikke er relevante, idet NemLog-in's sessionsstyring eksempelvis ikke udstrækker sig til 'native apps'.

2.7 Logningspolitik

Tjenesteudbydere er forpligtet til at overholde NemLog-in's logningspolitik, som er beskrevet her:

- https://www.nemlog-in.dk/tu/krav/logningspolitik

Logningspolitikken har til formål at sikre gennemsigtighed for den enkelte Slutbrugers anvendelse af NemLog-in og er et vigtigt element i sikkerheden af løsningen.

I forbindelse med logning skal Tjenesteudbydere sikre, at logningen sker med præcist tidsstempel. Serverne bør hvis muligt hente deres tid fra en tidsserver, som er Stratum 2 eller højere (se http://en.wikipedia.org/wiki/Network_Time_Protocol), og bør endvidere resynkronisere så ofte, at tiden højst afviger et millisekund.

2.8 Drift- og supportpolitik

Tjenesteudbydere er forpligtet til at overholde NemLog-in's drift- og supportpolitik, som er beskrevet her, samt orientere sig i de politikken beskrevne supportforums på Digitaliser.dk:

- https://www.nemlog-in.dk/tu/krav/drift-og-supportpolitik

Dokumentet beskriver driftsvilkår for den fællesoffentlige log-in-løsning, og beskriver desuden supporten i forbindelse med opkobling og løbende drift af løsning.

2.9 Beredskabspolitik

Tjenesteudbydere er forpligtet til at orientere sig i samt overholde NemLog-in's beredskabspolitik, som er beskrevet her:

- https://www.nemlog-in.dk/tu/krav/beredskabspolitikhttps://www.digitaliser.dk/resource/3126701

Beredskabspolitikken fastlægger en fælles beredskabsprocedure for varsling og genopretning (recovery) i forbindelse med eventuelt driftsnedbrud af NemLog-in eller i forbindelse med eventuel kompromittering af denne.

3 Services i NemLog-in3

Herunder beskrives de tekniske services i NemLog-in3-løsningen med tilhørende krav til Tjenesteudbydere ved anvendelse af disse. Der henvises til relevant teknisk dokumentation på andre sider, hvor yderligere detaljer fremgår.

3.1 Autentifikationsservices

NemLog-in3 brokeren udstiller to SAML Identity Provider (IdP) endepunkter, der begge kan kaldes af Tjenesteudbydere med henblik på autentifikation af slutbrugere, Single Logout og Attribute Query:

- En IdP baseret på OIOSAML 2.1.x specifikationen, som er forbeholdt offentlige tjenesteudbydere, og som skal udfases.
- En IdP baseret på OIOSAML 3.0.x specifikationen, der kan anvendes af såvel offentlige som private tjenesteudbydere.

Begge IdP'er understøtter autentifikation med NemID, MitID og på sigt lokale IdP'er. Digitaliseringsstyrelsen forbeholder sig ret til at tilføje flere typer identifikationsmidler, der opfylder kravene på de respektive sikringsniveauer i NSIS-standarden.

Anvendelse af NemLog-in's IdP'er kan alene ske fra It-systemer oprettet i NemLog-in's Administrationsportal. Tilsluttede It-systemer skal til enhver tid overholde kravene i de gældende OIOSAML specifikationer hørende til de anvendte IdP'er.

Offentlige Tjenesteudbydere har mulighed for Single Sign-On On til it-systemer, hvorfra der udføres en myndighedsopgave, når slutbruger i forvejen har en session med NemLog-in, mens en slutbruger altid vil skulle autentificere sig aktivt i NemLog-in, når de tilgår en privat Tjenesteudbyders it-systemer eller et offentligt it-system, hvorfra der ikke udføres en myndighedsopgave.

OIOSAML specifikationerne er tilgængelige her:

- https://migrering.nemlog-in.dk/nemlog-in-broker/offentlig-tjenesteudbyder/oiosaml-3-0-2/

3.1.1 Sessionshåndtering og timeout

En SAML Assertion's udløbstidspunkt skal valideres som beskrevet i OIOSAML standarderne (NotOnOrAfter attributten) herunder skal den afvises, hvis den præsenteres efter udløb.

Tjenesteudbydere kan oprette en session på baggrund af en gyldig Autentifikation med NemLog-in. I den forbindelse skal Tjenesteudbydere konfigurere deres it-systemer, så brugersessioner udløber efter at slutbrugeren har været inaktiv i en periode. Det er valgfrit, om timeoutperioden nulstilles, hver gang Slutbrugerens browser tilgår en Tjenesteudbyders it-system (sliding expiration), eller om den er uafhængig af brugeraktivitet (fast timeout periode). Tjenesteudbyderens timeout-periode må maksimalt sættes til 50 min. Digitaliseringsstyrelsen anbefaler dog generelt en timeout-periode på 30 min.

Intræder timeout, skal der sendes en ny autentifikationsanmodning til NemLog-in. Hvis Slutbrugeren fortsat har en session med NemLog-in, da kan denne evt. håndteres uden at Slutbrugeren skal autentificere sig aktivt igen (via Single Sign-On).

Den samlede sessionslængde hos en Tjenesteudbyder må højst være 8 timer (forudsat Slutbrugeren kontinuerligt er aktiv), hvorefter slutbrugeren skal re-autentificeres.

Hvis en Tjenesteudbyder af sikkerhedsmæssige grunde vil sikre sig, at Slutbrugeren bliver påtvunget aktiv autentifikation i NemLog-in løsningen, kan Tjenesteudbyderen sætte parameteren ForceAuthn=”true” i kaldet til NemLog-in (se OIOSAML for detaljer).

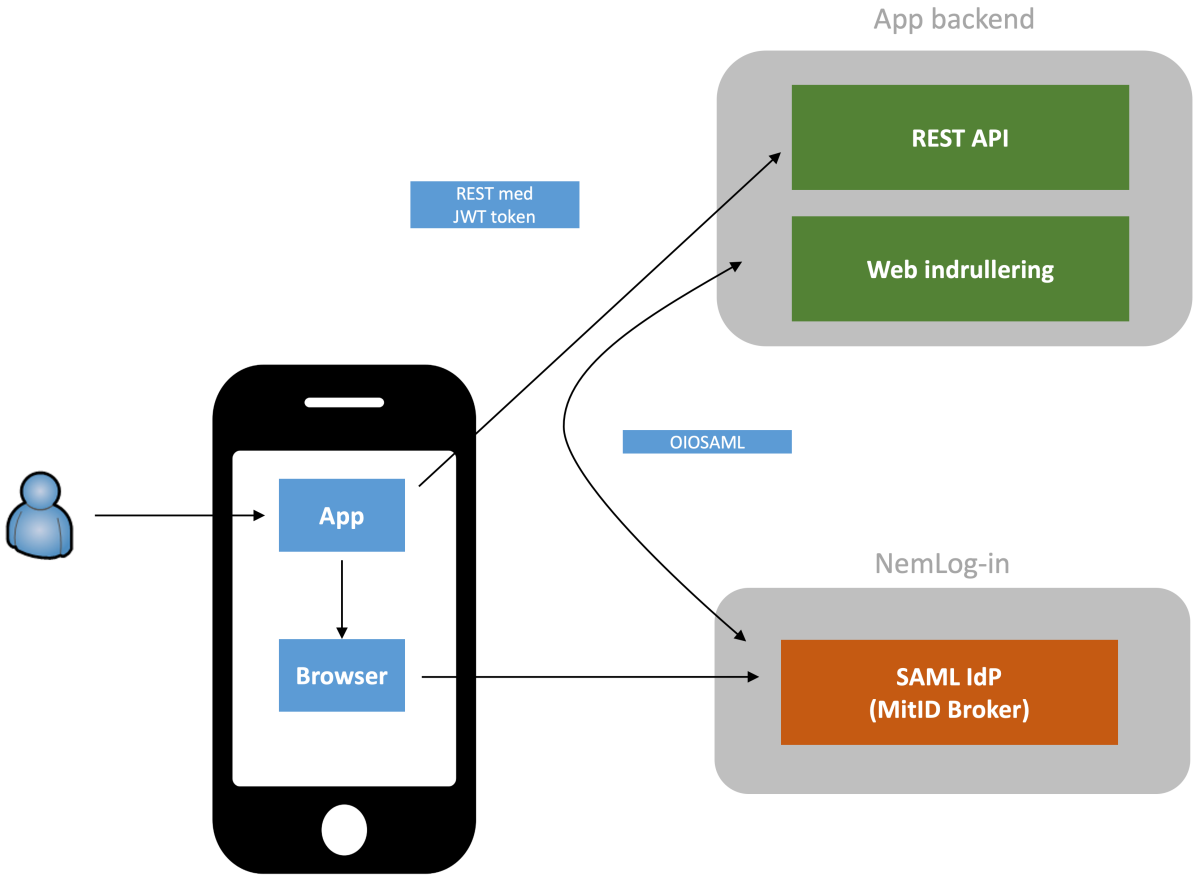
3.1.2 Timeout i NemLog-in

Ved timeout af NemLog-in’s IdP-session vil Slutbrugeren skulle autentificere sig aktivt over for NemLog-in, næste gang en Tjenesteudbyders it-system viderestiller en Slutbruger for log-in (via et SAML <AuthnRequest>). Lokale sessioner hos Tjenesteudbydere kan vedblive med at være aktive (såfremt Slutbrugeren holder dem i live), selvom NemLog-in’s session timer ud. Bemærk at NemLog-in ved timeout ikke sender beskeder til Tjenesteudbydere om, at de skal logge Slutbrugerne ud (såkaldt ”single logout”).

3.1.3 Autentifikation til ’native Apps’

Udgangspunktet for NemLog-in’s autentifikationsservices har været autentifikation i traditionelle web-applikationer med en back-end, som der på forhånd er udvekslet SAML metadata med. Det er imidlertid også tilladt at anvende NemLog-in’s IdP’er til indrullering i native Apps installeret på en slutbrugerenhed. I dette scenarie vil en App typisk implementere indrullering baseret på mønstrene i OAuth eller OpenID Connect standarderne, hvor App’en ved indrullering åbner en browser, der peges mod app’ens back-end, som herefter gennemfører en NemLog-in-autentifikation baseret på OIOSAML protokollen. Efter succesfuld autentifikation producerer App’ens back-end ofte et personligt JWT-token som leveres til App’en til brug for efterfølgende API-kald på vegne af brugeren. For yderligere detaljer og inspiration til dette mønster henvises til Digitaliseringsstyrelsens OpenID Connect profiler[1].

[1] https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/openid-connect-profiler/



Figur 1: Eksempel på scenarie med App indrullering via NemLog-in

Ved udvikling af integrationer til NemLog-in baseret på ovenstående mønster, er der en række forhold, som tjenester skal være opmærksomme på:

- Der er krav til den browser-komponent, som der funger som user-agent på brugerens mobile enhed i interaktionen med NemLog-in. Eksempelvis er 'web views' af sikkerhedsmæssige grunde ikke tilladt. Se kapitel 3.6 om integrationskrav for yderligere detaljer.

- Kravene i dette dokument går alene på app'ens back-end, der er den komponent hos tjenesteudbyderen, der står for OIOSAML integrationen til NemLog-in. Den efterfølgende udstedelse af JWT-tokens[2] hos tjenesteudbyderen og levering til App'en er tjenesteudbyderens eget ansvar, ligesom levetid, udløb og fornyelse af disse tokens. Der henvises til de tidligere omtalte OIO OIDC profiler for yderligere anbefalinger.

- App'ens backend skal i sin SAML autentifikationsforespørgsel mod NemLog-in sætte flaget "ForceAuth=true" for at sikre, at brugeren logger aktivt på og ikke opnår single sign-on via en tidligere etableret session med NemLog-in.

- Ikke alle test cases i integrationstesten er relevante i App-scenarier som beskrevet i afsnit 1.6. Eksempelvis udstrækker NemLog-in's sessionshåndtering sig ikke til Apps. Dette betyder konkret, at der ikke er krav til, at Single Logout beskeder sendt fra NemLog-in til tjenesteudbyderens backend skal

[2] Dette gælder fx Access Tokens og Refresh Tokens.

medføre invalidering af lokalt udstedte JWT-tokens, eller at NemLog-in stiller hårde krav til automatisk udløb af disse tokens[3].

3.1.4 Afledte identiteter

Hvis Tjenesteudbydere baserer fremtidige Autentifikationer af en Slutbruger uden 8 timers perioden omtalt ovenfor og uden at re-autentificere Slutbrugeren, må denne Autentifikation ikke fremstilles, omtales eller på anden måde gengives som en Autentifikation fra NemLog-in eller et af de identifikationsmidler, der er tilgængeligt via NemLog-in.

Sådan brug uden for tidsperioden kan eksempelvis omfatte anvendelse af en MitID Autentifikation som grundlag for indrullering af Tjenesteudbyderens egen sikkerhedsløsning i en app-løsning på mobile enheder.

Tjenesteudbyderen er eneansvarlig og bærer risikoen for sådanne Autentifikationers validitet og sikkerhedsmæssig kvalitet og Digitaliseringsstyrelsen kan på ingen måde gøres ansvarlig for sikkerhed eller andre forhold relateret hertil.

Tjenesteudbyder skal særskilt være opmærksom på de særlige sikkerhedsmæssige risici sådanne Autentifikationer indebærer, idet oplysninger om spærring, suspendering af en Slutbrugers identifikationsmiddel eller yderligere forhold om identiteten ikke tilgår Tjenesteudbyderen.

Tjenesteudbyder skal informere Slutbrugere om de nærmere risici knyttet til den pågældende Autentifikation, og at Autentifikationen ikke har karakter af en Autentifikation fra NemLog-in eller et af de identifikationsmidler, der er tilgængelige herfra.

3.2 Opslags- og match tjenester

NemLog-in udstiller en række opslags- og match-tjenester, som kan anvendes af Tjenesteudbydere med særlige behov relateret til Autentifikation og signering – eksempelvis til at afgøre, om det er den samme Slutbruger, der logger ind og efterfølgende signerer et dokument. Ved at anvende disse tjenester er der mulighed for, at Tjenesteudbydere kan etablere deres løsninger med høj grad af databeskyttelse (privacy), idet der ikke er behov for at efterspørge globale identifikatorer (som fx globale UUID'er og CPR-numre) fra NemLog-in.

Tjenesteudbydere anmoder om adgang til opslagstjenester via NemLog-in's Administrationsportal, og adgang opnås med billet (token) udstedt af NemLog-in's Security Token Service.

Opslags- og match-tjenester er udstillet som et API og er dokumenteret her:

- https://migrering.nemlog-in.dk/nemlog-in-broker/test-og-dokumentation/

Dokumentationen af opslags- og match-tjenester beskriver de forskellige typer identifikatorer (i form af UUID'er) der kan optræde i SAML Assertions og i certifikater udstedt af NemLog-in, samt hvorledes disse matches og konverteres.

[3] Når NemLog-in på sigt forventes at udstille en OpenID Connect-baseret Authorization Server, vil der formentlig komme vilkår og retningslinjer for anvendelse af denne, som regulerer dette område.

3.3 Rettighedsstyring for erhvervsbrugere

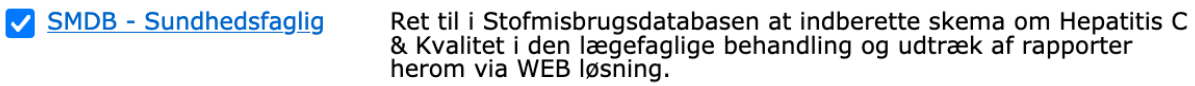
NemLog-in rummer funktionalitet til rettighedsstyring, der kan anvendes af **offentlige** tjenesteudbydere i deres selvbetjeningsløsninger rettet mod erhvervsbrugere. I løsningen kan Tjenesteudbydere definere rettigheder til deres it-systemer, som en brugerorganisation herefter kan tildele sine Erhvervsbrugere i egen organisation eller delegere til en anden organisation gennem en erhvervsfuldmagt.

Offentlige tjenesteudbydere tager rettighedsstyringen i anvendelse ved at oprette en eller flere rettigheder for deres it-systemer i NemLog-in's Administrationsportal, og er i den forbindelse forpligtet til:

a) At angive en korrekt og fyldestgørende beskrivelse af, hvad rettigheden giver adgang til, således at brugerorganisationens brugeradministratorer har et oplyst grundlag at tildele rettigheder til Slutbrugere på. Ved udformning af beskrivelsen bør man tage højde for, at brugeradministratoren ikke nødvendigvis kender til detaljerne i selvbetjeningsløsningen, og forklaringen bør derfor formidle tilstrækkelig kontekst til, at administratoren kan forstå implikationerne af en tildeling, så der ikke sker fejl. Et eksempel fra NemLog-in's brugeradministration er vist i Figur 1 nedenfor.

b) Ikke at tilføje nye adgange til eksisterende rettigheder eller ændre indholdet i en rettighed.

Ovenstående forpligtelser har til formål at sikre, at tildelte rettigheder er stabile over tid, således at Slutbrugere ikke på et senere tidspunkt opnår ændrede rettigheder uden deres brugeradministrators vidende eller godkendelse. Hvis Tjenesteudbydere har behov for at udvide en rettighed, skal der i stedet oprettes en ny rettighed eller en ny version af en eksisterende rettighed. Ved tvivlstilfælde skal Digitaliseringsstyrelsen kontaktes, før en eksisterende rettighed ændres for et tilsluttet it-system.



Figur 1: Eksempel på rettighedsbeskrivelse

Når en rettighed er oprettet i Administrationsportalen, kan den tildeles til Erhvervsbrugere af alle brugerorganisationer samt indgå i erhvervsfuldmagter. Det er muligt for en Tjenesteudbyder at afgrænse hvilke brugerorganisationer (udvalgte CVR-numre), der kan tildele en rettighed til Erhvervsbrugere, ved at kontakte NemLog-in forvaltningen med henblik på at få opsat et CVR-filter.

Tildelte rettigheder vil optræde som attributter i autentifikationssvaret for Erhvervsbrugeren som Slutbruger, som beskrevet i OIOSAML.

Dokumentationen for Administrationsportalen findes her:

- https://migrering.nemlog-in.dk/media/kgeliazh/25-brugermanual-til-nemlog-in-administration-v-3.pdf

3.4 Digitale borgerfuldmagter

NemLog-in rummer en fuldmagtsservice (benævnt serviceområdet 'Digital repræsentation' i Lov om MitID og NemLog-in), der muliggør at offentlige Tjenesteudbydere kan håndtere digitale fuldmagter i deres selvbetjeningsløsninger henvendt til private borgere og erhvervsbrugere, der kan tegne en virksomhed alene. Tjenesteudbydere tager funktionaliteten i anvendelse ved at oprette et eller flere fuldmagtsprivilegier for deres it-systemer i NemLog-in's Administrationsportal. Efter oprettelse af fuldmagtsprivilegier kan disse indgå i digitale fuldmagter, som tildeles en repræsentant via brugergrænsefladen for fuldmagtsløsningen, der bl.a. er udstillet på Borger.dk.

Tildelte fuldmagter (repræsentationsforhold) vil optræde som attributter i autentifikationssvaret for Slutbrugeren (i rollen som repræsentant) som beskrevet i OIOSAML. Endvidere kan Tjenesteudbydere anvende et API udstillet af fuldmagtsløsningen til at hente fuldmagter uafhængigt af om repræsentanten er logget ind hos Tjenesteudbyderen.

Ansvarsfordelingen mellem Digitaliseringsstyrelsen og Tjenesteudbyder er, at NemLog-in attesterer hvem repræsentanten er, samt hvilke fuldmagtsprivilegier repræsentanten er tildelt af den borger, der har afgivet fuldmagten, mens Tjenesteudbyderens it-system ud fra disse oplysninger afgør hvilke data og hvilke handlinger, repræsentanten kan tilgå/ foretage i Tjenesteudbyders it-system.

Det er Tjenesteudbyders ansvar at afklare det juridiske grundlag for anvendelse af fuldmagter i Tjenesteudbyderens it-systemer samt etablere logning af en repræsentants handlinger i Tjenesteudbyders it-systemer i henhold til NemLog-in's logningspolitik.

Tjenesteudbyderen forpligter sig til at:

a) Designe adgangsstyring i eget it-system baseret på fuldmagtsprivilegier, der er meningsfulde i kontekst af den funktionalitet, som it-systemet udstiller, herunder afvise fuldmagter, som Tjenesteudbyderen vurderer ikke som gyldige eller anvendelige i sin løsning.
b) Oprette fuldmagtsprivilegier samt angive en korrekt beskrivelse af, hvad fuldmagtsprivilegier giver adgang til i NemLog-in's Administrationsportal, således at borgere har et oplyst grundlag at tildele fuldmagtsrettigheder til repræsentanter på.
c) Ikke at tilføje nye adgange til eksisterende fuldmagtsprivilegier eller på anden måde udvide effekten af et fuldmagtsprivilegie.

   Ovenstående har til formål at sikre, at tildelte rettigheder er stabile over tid, således at repræsentanter ikke på et senere tidspunkt opnår ændrede rettigheder eller udvidet effekt af et fuldmagtsprivilegie uden en borgers vidende eller godkendelse. Er der behov for at ændre et fuldmagtsprivilegie, skal der i stedet oprettes et nyt fuldmagtsprivilegie. Ved tvivlstilfælde skal Digitaliseringsstyrelsen kontaktes.

Tjenesteudbydere må alene anvende en modtaget digital fuldmagt fra NemLog-in i forbindelse med en konkret log-in-session. Den må således ikke lagres til senere brug i Tjenesteudbyders systemer, da dette ville kunne medføre brug af fuldmagten efter at den er tilbagekaldt af borgeren i NemLog-in. Endvidere skal Tjenesteudbyderen sikre, at en SAML billet med fuldmagtsrettigheder ikke anvendes på en senere dato, end hvor den er udstedt. Hvis en repræsentant anvender it-systemet hen over et datoskift (midnat), skal Tjenesteudbyderen forny SAML billetten ved kald mod NemLog-in og herefter kontrollere, at fuldmagtsprivilegierne stadig er til stede.

Dokumentationen for Administrationsportalen findes her:

- https://migrering.nemlog-in.dk/media/kgeliazh/25-brugermanual-til-nemlog-in-administration-v-3.pdf

Yderligere tekniske oplysninger om fuldmagtsløsningen findes i fuldmagtsgruppen på Digitaliser.dk herunder API-beskrivelse og integrationsguide:

- https://www.digitaliser.dk/resource/5879999

3.4.1 Håndtering af papirfuldmagter hos offentlige myndigheder og offentligretlige organer

NemLog-in gør det muligt at digitalisere en fuldmagt underskrevet på papir, så den får effekt i forhold til myndighedernes digitale selvbetjeningsløsninger på samme måde, som hvis borgeren via fuldmagtsløsningen selv havde oprettet en digital fuldmagt.

En myndighed kan i rollen som Tjenesteudbyder således foretage en digital registrering af en modtaget papirfuldmagt fra en borger. Myndigheden skal fastlægge regler og kontrolprocedurer for modtagelse af en papirfuldmagt, registrering af papirfuldmagt ved en betroet medarbejder samt løbende kontrol heraf.

Myndighedens opgaver omfatter bl.a.:

- Instruks til de betroede medarbejdere, der skal registrere papirfuldmagter.
- Regler for registrering og opbevaring af papirfuldmagter, så der skabes sporbarhed. I NemLog-in kan der yderligere indtastes en reference til registreret papirfuldmagt f.eks. til et ESDH-system.
- Kontrolprocedurer i form af fx stikprøvekontrol af foretagne registreringer. Arbejdet med registrering af papirfuldmagter skal være omfattet af myndighedens revision.
- Procedurer til sikring af, at registrering af betroede medarbejdere er korrekt. Myndigheden skal etablere og vedligeholde sikre procedurer, så betroede medarbejderes rettigheder i NemLog-in straks fjernes, når de ikke længere har et arbejdsbetinget behov for at kunne foretage registrering af fuldmagter i NemLog-in.

3.5 Security Token Service

NemLog-in udstiller en Security Token Service (STS) til autentifikation og autorisation af systembrugere baseret på OIO IDWS-specifikationerne. Anvendelse af NemLog-in's STS kan alene ske fra it-systemer oprettet i NemLog-in's Administrationsportal i rollen som Web Service Consumer (WSC) mod en registreret Web Service Provider (WSP). Herefter kan it-systemet i rollen som klient (WSC) anmode om en billet (token) fra NemLog-in's STS, der giver adgang til en bestemt web service (WSP).

De tekniske specifikationer for STS'en er publiceret her:

- https://www.digitaliser.dk/resource/5988041

3.6 Integrationskrav

Som supplement til OIOSAML specifikationerne er der publiceret et integrationsdokument, som indeholder yderligere detaljer og teknisk beskrivelse af, hvordan en Tjenesteudbyder kan integrere til NemLog-in, herunder forskellene på services der tilbydes offentlige- hhv. private tjenesteudbydere. Integrationsguiden findes publiceret her:

- https://migrering.nemlog-in.dk/media/3e3mhvzi/10-integration-with-nemlog-in-v1-2.pdf

Tjenesteudbydere skal overholde tekniske krav og anvisninger i integrationsdokumentet. Herunder fremhæves en række udvalgte forhold:

- Private Tjenesteudbydere skal - uagtet at disse ikke kan deltage i single sign-on - implementere et SAML single logout endepunkt, der svarer NemLog-in korrekt på SAML Single Logout forespørgsler. Der er omvendt ikke krav om, at private Tjenesteudbydere initierer Single Logout mod NemLog-in.
- En Tjenesteudbyder skal terminere lokale sessioner, når NemLog-in fremsender forespørgsel om Single Logout. Tjenesteudbyder kan søge Digitaliseringsstyrelsen om dispensation herfor i en konkret

løsning, hvis der er særlige behov eller omstændigheder, der gør sig gældende. Bemærk at der i givet fald stadig skal svares korrekt på single logout forespørgsler som beskrevet ovenfor.

- En Tjenesteudbyder skal ved modtagelse af autentifikationssvar fra NemLog-in altid kontrollere, om det sikringsniveau, der er påstemplet i SAML Assertion fra NemLog-in, lever op til tjenesteudbyderens krav - og herunder blokere for (eller evt. indskrænke) brugerens adgang til Tjenesteudbyderens it-system, hvis sikringsniveauet ikke lever op til Tjenesteudbyderens krav for adgang til det pågældende it-system. Dette gælder uagtet om Tjenesteudbyderen har forespurgt om et bestemt sikringsniveau i sin autentifikationsanmodning mod NemLog-in. Eksempelvis er det Tjenesteudbyderens ansvar at blokere for autentifikationer på sikringsniveau Lav, hvis dette sikringsniveau ikke lever op til tjenestens adgangspolitik.

- Det er ligeledes Tjenesteudbyderens ansvar at kontrollere Slutbrugerens alder inden der gives adgang til en digital selvbetjeningsløsning, der har begrænsninger i forhold til visse aldersgrupper. Bemærk at MitID kan udstedes til personer, der er fyldt 13 år.

- Der er begrænsninger knyttet til indlejring af NemLog-in's brugergrænseflader i applikationer og apps ved brug iFrame og 'web views', som skal respekteres. Der henvises til integrationsdokumentet for detaljer om dette.

3.7 NemID Signeringstjeneste i NemLog-in (’legacy’)

NemLog-in udstiller en signeringsløsning, der muliggør at Tjenesteudbydere kan indhente slutbrugeres elektroniske underskrifter på dokumenter afgivet via NemID-identifikationsmidler med tilhørende OCES-certifikater.

NemID-signeringstjenesten gør det enkelt for Tjenesteudbydere (interaktivt) at indhente en slutbrugers digitale underskrift på et elektronisk dokument. Dette er eksempelvis relevant i indberetningsløsninger, hvor det kræves, at en bruger skal godkende de indtastede oplysninger ved at afgive en bindende underskrift.

Signeringsløsningen består af en brugergrænseflade i form af en web-applikation, hvor slutbrugeren kan se den tekst, der skal signeres samtidig med, at det ved accept er muligt for Slutbrugeren at signere eksempelvis ved brug af NemID.

Efter Slutbrugeren har signeret, validerer NemLog-in Slutbrugerens NemID og det tilhørende OCES-certifikats gyldighed, og tilvejebringer under denne proces et stærkt signaturbevis i form af en integritetsbeskyttet logning, Digitaliseringsstyrelsen opbevarer signaturbeviset, og en kopi kan på anfordring leveres til Tjenesteudbyderen.

NemLog-in lagrer *ikke* den originale tekst, der ligger til grund for underskriften, men derimod kun den kryptografiske hashværdi, som signaturen er dannet over, samt resultatet af signaturvalideringen.

Det er derfor op til Tjenesteudbyderen at gemme den oprindelige aftaletekst *i uændret form* sammen med referencenummeret på signaturbeviset, der returneres fra signeringstjenesten. Hvis det ikke sker, kan det have som konsekvens, at det bliver vanskeligt for Tjenesteudbyderen at godtgøre, hvilken aftaletekst brugeren oprindeligt underskrev.

3.7.1 Type af signatur

Slutbrugeren kan afgive signaturer med:

- OCES Personcertifikat
- OCES Medarbejdercertifikat
- OCES Virksomhedscertifikat

3.7.2 NemID Signeringstjenestens validering af certifikater

Efter brugeren har signeret, validerer NemID Signeringstjenesten Slutbrugers NemID og det tilhørende certifikats gyldighed. Tjenesten sikrer således, at certifikatet gyldighedsperiode ikke er overskredet samt at certifikatet ikke er spærret.

Som en del af validering af certifikatet tilvejebringer signeringstjenesten et signaturbevis. Signaturbeviset består bl.a. af den kryptografiske hashværdi, som signaturen er dannet over, samt resultatet af signaturvalideringen.

Tjenesteudbyder modtager en kopi af dette signaturbevis og NemLog-in lagrer det i en integritetsbeskyttet log, der kan benyttes som tredjepartsbevis.

Digitaliseringsstyrelsen opbevarer signaturbeviset i hele NemLog-in's kontraktperiode, og en kopi kan på anfordring leveres til Tjenesteudbyder.

NemID Signeringstjenesten lagrer ikke det dokument/data, der underskrives af Slutbruger.

3.7.3 Tjenesteudbyders pligt ved anvendelse af NemID Signeringstjenesten

Tjenesteudbyder skal som modtager af OCES signatur med tilhørende certifikat baseret på et NemID sikre sig at:

- Det formål Certifikatet søges anvendt til, er passende i forhold til eventuelle anvendelsesbegrænsninger, der er angivet i Certifikatet, fx certifikater til unge mellem 15 år og 18 år, hvoraf det fremgår "Ung mellem 15 og 18 - kan som udgangspunkt ikke indgå juridisk bindende aftaler", samt
- Anvendelsen af Certifikatet i øvrigt er passende i forhold til det sikkerhedsniveau, som er beskrevet i den relevante certifikatpolitik.

3.7.4 Certifikattyper

NemID signeringstjenesten baserer sig på OCES-certifikater, der er udstedt på baggrund af certifikatpolitikker, udarbejdet og vedligeholdt af Digitaliseringsstyrelsen.

OCES-certifikater er ikke "kvalificerede certifikater" jf. eIDAS forordningen og bør ikke anvendes til formål, hvor kvalificerede certifikater er påkrævet.

3.8 Signering med kvalificerede signaturer og -segl

NemLog-in udstiller en signeringsløsning, der gør det muligt for Tjenesteudbydere at indhente slutbrugeres underskrifter på dokumenter afgivet via MitID-identifikationsmidler. Der er tale om kvalificerede signaturer (i henhold til eIDAS forordningen) baseret på (kvalificerede) kortidscertifikater.

Via Signeringstjenesten kan slutbruger afgive kvalificerede elektroniske signaturer baseret på personcertifikater og medarbejdercertifikater samt kvalificerede segl baseret på kvalificerede virksomhedscertifikater. Alle kvalificerede elektroniske signaturer og segl er sammenkoblet med et

kvalificeret tidsstempel, der sikrer, at det er muligt i forbindelse med verifikation at få en præcis oplysning om tidspunktet for afgivelse af henholdsvis signaturen og seglet.

Alle certifikater og tidsstempler fra NemLog-in Digital Signering er udstedt af Digitaliseringsstyrelsens certificeringscenter (CA er den danske stat). Certificeringscenteret har udarbejdet og vedligeholder en Certificate Practice Statement (CPS), der definerer det sikkerhedsniveau, som er gældende for certifikatydelser fra certificeringscenteret. Digitaliseringsstyrelsens CPS og bagvedliggende certifikatpolitik kan læses på https://certifikat.gov.dk

Certifikaterne i Signeringstjenesten har karakter af korttidscertifikater, der oprettes specifikt til afgivelse af én elektronisk signatur eller elektronisk segl. Efter afgivelse af signaturen eller seglet slettes de signaturgenereringsdata (den private nøgle), der er knyttet til certifikatet, hvorefter certifikatet ikke kan bruges som grundlag for yderligere elektroniske signaturer eller elektroniske segl. For at sikre at den elektronisk signatur eller segl og kan modtages og læses af en bred portefølje af systemer udløber certifikatet først efter 30 dage.

Den tekniske dokumentation findes på denne side:

- https://migrering.nemlog-in.dk/nemlog-in-broker/test-og-dokumentation/

3.8.1 Den konkrete anvendelse af Signeringstjenesten

Ved Tjenesteudbyders anvendelse af Signeringstjenesten skal Tjenesteudbyder tage stilling til følgende:

- Ønsket underskriver
- Type af signatur/segl
- UUID model
- Signaturformat
- Referencetekst

Opsætning sker ved det konkrete kald til Signeringstjenesten gennem opstartsparametre i overensstemmelse med den tekniske dokumentation angivet ovenfor.

Bemærk: referenceteksten skal være generisk og må ikke indeholde personoplysninger!

3.8.2 Signatur og segl

Tjenesteudbyder kan efterspørge følgende elektroniske signaturer/segl:

- Kvalificeret elektronisk signatur baseret på et kvalificeret Personcertifikat
- Kvalificeret elektronisk signatur baseret på et kvalificeret medarbejdercertifikater
- Kvalificeret elektronisk segl baseret på et kvalificeret virksomhedscertifikat

Alle kvalificerede elektroniske signaturer og segl er sammenkoblet med et kvalificeret tidsstempel og LTC.

3.8.3 Angivelse af UUID

Tjenesteudbyder skal træffe beslutning om hvilken model for UUID, der skal indeholdes i certifikatet som grundlag for Tjenesteudbyders efterfølgende behandling af det signerede dokument og tilhørende [signaturdata]. Der kan vælges mellem tre modeller med forskellige niveauer af databeskyttelse (Privacy) for Slutbrugeren (fra A til C, hvor C leverer det højeste niveau):

a) Slutbrugeren identificeres med en global UUID, der anvendes på tværs af alle Tjenesteudbydere

b) Et UUID specifik for Tjenesteudbyder

c) Et unikt UUID per signering (sessions UUID)

Tjenesteudbyder skal vurdere hvilke modeller, der opfylder det forretningsmæssige behov og herefter vælge den model, der tilbyder det højeste niveau af databeskyttelse.

Hvis Tjenesteudbyder ønsker at anvende Global UUID, skal Tjenesteudbyder sikre tilstrækkelig behandlingshjemmel forud for Slutbrugers afgivelse af en elektronisk signatur eller segl, eksempelvis ved indhentelse af et samtykke fra Slutbruger.

Tjenesteudbyder kan ved anvendelse af sessions UUID via matchtjenesten beskrevet ovenfor i afsnit 3.2 få verificeret, om to forskellige UUID'er tilhører den samme person. Tjenesten er nærmere beskrevet i afsnit 3.2 om opslags- og matchtjenester.

3.8.4 Signaturformat

Tjenesteudbyder skal vælge hvilket signatur- eller seglformat, dokumentet skal underskrives i. Der er mulighed for at vælge formater, der baserer sig på EU-profileringen af enten PAdES eller XAdES.

PAdES benyttes til at integrere den elektroniske signatur eller segl i et PDF-dokument, der herefter kan kopieres og distribueres.

XAdES understøtter XML formatet og benyttes til at signere en længere række af dokumenttyper.

3.8.5 Referencetekst

Tjenesteudbyder skal sørge for at opsætte en referencetekst, der over for Slutbruger beskriver den konkrete underskriftshandling. Referenceteksten indgår i opstartsparametrene, der medsendes ved kald til Signeringstjenesten.

3.8.6 Digitaliseringsstyrelsens forpligtelser ved afgivelse af en elektronisk signatur eller segl

Efter Slutbrugers afgivelse af en elektronisk signatur eller segl til brug for Tjenesteudbyder, kontrollerer og indestår Digitaliseringsstyrelsen for, at det anvendte certifikat er udstedt til den pågældende (autentificerede) Slutbruger og var gyldigt og ikke spærret på tidspunktet for afgivelse af den elektroniske signatur eller segl. CA'et indestår for, at der kun udstedes certifikater til identiteter, som er registreret med en sikkerhed, der svarer til personligt fremmøde.

3.8.7 Tjenesteudbyders forpligtelser ved modtagelse af en elektronisk signatur eller segl

Tjenesteudbyder er ansvarlig for at sikre, at anvendelse af elektroniske signaturer, segl og tilhørende certifikater fra Signeringstjenesten sker i overensstemmelse med de evt. anvendelsesbegrænsninger for certifikatet, der måtte være meddelt af Digitaliseringsstyrelsen.

Sådanne anvendelsesbegrænsninger vil fremgå af certifikatet og Digitaliseringsstyrelsens hjemmeside.

3.8.8 Sikring af dokumentation og bevisværdi for signaturer og segl

Tjenesteudbyder er ansvarlig for at opbevare og arkivere det signerede dokument (i uændret form) og signaturbeviset fra NemLog-in, samt for at underskriveren også har adgang til en kopi af det signerede dokument. Originaldokumentet, der signeres, er alene tilgængeligt i slutbrugerens browser og behandles ikke i NemLog-in's infrastruktur. Signeringstjenesten opnår på intet tidspunkt i signeringsprocessen adgang til det dokument eller de data, der signeres.

Tjenesteudbyder er desuden ansvarlig for ved egne handlinger at sikre bevisværdien over tid af data underskrevet med en elektronisk signatur eller segl fra NemLog-in digital signering.

3.9 Validering af elektroniske signaturer og segl

Digitaliseringsstyrelsen stiller en kvalificeret valideringstjeneste til rådighed for validering af kvalificerede elektroniske signaturer og elektroniske segl.

Valideringstjenesten kan benyttes til validering af signaturer og -segl afgivet i NemLog-in's signeringstjeneste. Valideringstjenesten kan frit benyttes af alle.

I forbindelse med valideringen foretages en kortvarig automatisk behandling i et sikret miljø af de data, der er underskrevet. Alle data slettes herefter.