DIGITALISERINGSSTYRELSEN

NemLog-in

Tekniske krav til Tjenesters anvendelse af NemLog-in

Version 2.1

Indholdsfortegnelse

1 Dokumenthistorik ... 4
2 Tekniske krav og politikker ... 5
2.1 Definitioner ... 5
2.2 Roller og aftalerelationer i NemLog-in ... 7
2.3 Ændringer til krav og politikker ... 8
2.4 Opsætning i NemLog-in's Administrationsportal ... 9
2.4.1 Tilslutning, vedligehold og frakobling ... 9
2.4.2 Konfiguration af attributter og dataminimering ... 9
2.5 Ansvar i relation til sikkerhed ... 10
2.5.1 Generelt om It-systemudbyderens egen organisation ... 10
2.5.2 Adgangskontrol i Tjenester ... 10
2.5.3 Certifikater hos It-systemudbydere ... 10
2.6 Forbrugsvarsling ... 10
2.7 Test af integrationer ... 10
2.8 Logningspolitik ... 11
2.9 Drift- og supportpolitik ... 11
3 Services i NemLog-in ... 12
3.1 Indledning ... 12
3.2 Autentifikationsservices ... 12
3.2.1 Sessionshåndtering og timeout ... 12
3.2.2 Timeout i NemLog-in ... 13
3.2.3 Autentifikation til 'native Apps' ... 13
3.2.4 Afledte identiteter ... 15
3.3 Opslags- og match tjenester ... 15
3.4 Rettighedsstyring for erhvervsbrugere ... 15
3.5 Digitale borgerfuldmagter ... 16
3.5.1 Håndtering af papirfuldmagter hos offentlige myndigheder og offentligretlige organer ... 18
3.6 Security Token Service ... 18
3.7 Integrationskrav ... 18
4 Tjenesters anvendelse af certifikater fra NemLog-in ... 20
4.1 Signering med kvalificerede signaturer og -segl ... 20
4.1.1 Den konkrete anvendelse af Signeringsløsningen ... 20
4.1.2 Signatur og segl ... 21
4.1.3 Angivelse af UUID ... 21
4.1.4 Signaturformat ... 21
4.1.5 Referencetekst ... 21

4.1.6 Digitaliseringsstyrelsens forpligtelser ved afgivelse af en elektronisk signatur eller segl 22
4.1.7 Tjenesters forpligtelser ved modtagelse af en elektronisk signatur eller segl 22
4.1.8 Sikring af dokumentation og bevisværdi for signaturer og segl 22
4.2 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
10.10.2021	1.2	Fjernet afsnit med beredskabspolitik da denne er slået sammen med drift- og supportpolitikken. Opdateret definitioner.	TG
22.11.2022	2.0	Omskrevet med fokus på tjenester og ikke tjenesteudbydere, så kravene bl.a. også kan anvendes i regi af Multi-tenant leverandører.	TG
09.04.2024	2.1	Links til dokumentation opdateret. Afsnit om NemID signering fjernet. Afsnit om ansvar præciseret i afsnit 3.5.	TG

2 Tekniske krav og politikker

Herunder fremgår tekniske krav og politikker relateret til Tjenester tilsluttet NemLog-in, som er underlagt og refereres fra følgende juridiske dokumenter:

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

I det omfang der er modstrid mellem nærværende tekniske krav og ovenstående juridiske dokumenter, er de juridiske dokumenter gældende.

Målgruppen for beskrivelsen er primært teknisk personale hos Tjenesteudbydere eller leverandører hertil, 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 It-systemudbydere kan administrere tilslutningen af Digitale Selvbetjeningsløsninger (it-systemer) til NemLog-in, herunder hvilke attributter, der skal leveres i autentifikationssvaret samt certifikater og øvrige tekniske oplysninger relevant for integrationen.
(Sub)-Broker	En organisation med et it-system tilsluttet NemLog-in i rollen som Brokersystem, der videreformidler Autentifikation af digitale identiteter til bagvedliggende Tjenesteudbydere og/eller Tredjepartsbrokere.
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.
Erhvervsbruger	En fysisk person, der er associeret med en Juridisk enhed, og som er oprettet med en erhvervsidentitet i MitID Erhverv (benævnt NemLog-in Erhvervsadministration i lov om MitID og NemLog-in).

Begreb	Beskrivelse
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 MitID eller et NSIS anmeldt identifikationsmiddel fra en Lokal IdP.
It-system	Anvendes som synonym for Digital Selvbetjeningsløsning leveret af en It-systemudbyder.
It-systemudbyder	En organisation som har tilsluttet sig til NemLog-in og som herefter kan oprette og administrere it-systemer, der anvender services fra NemLog-in. En organisation agerer typisk som It-systemudbyder enten fordi den er dataansvarlig Tjenesteudbyder eller (multitenant)leverandør til en Tjenesteudbyder. For uddybning se afsnit 2.2 nedenfor.
Kvalificeret elektronisk signatur	En kvalificeret elektronisk signatur afgivet i Digitaliseringsstyrelsens signaturløsning på baggrund af et kvalificeret certifikat. Medmindre andet specifikt er anført omfattet betegnelsen også kvalificeret elektronisk segl, der ligeledes kan afgives i signaturløsningen. 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, elektroniske identifikationsordning for privatpersoner og tilhørende elektroniske identifikationsmidler, som kan tilknyttes privatpersoners og erhvervsbrugeres digitale identiteter. 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. Digitaliseringsstyrelsens login-tjeneste NemLog-in 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.
NSIS	National Standard for Identiteters Sikringsniveauer.

Begreb	Beskrivelse
Sikringsniveau	Graden af tillid til en autentificeret Identitet (på engelsk "Level of Assurance") og ofte benævnt autenticitetssikringsniveau. Niveauerne er defineret i NSIS standarden, hvor 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 eller signering i en Tjeneste via en eller flere mellemliggende Brokere.
Tjeneste	Digital selvbetjeningsløsning (It-system) som anvender en eller flere services fra NemLog-in fx til autentificering af Slutbrugere. En Tjeneste udbydes på vegne af en eller flere Tjenesteudbydere og tilsluttes samt administreres teknisk af en It-systemudbyder.
Tjenesteudbyder	En juridisk enhed, der som dataansvarlig stiller én eller flere Digitale Selvbetjeningsløsninger til rådighed for Slutbrugere.

2.2 Roller og aftalerelationer i NemLog-in

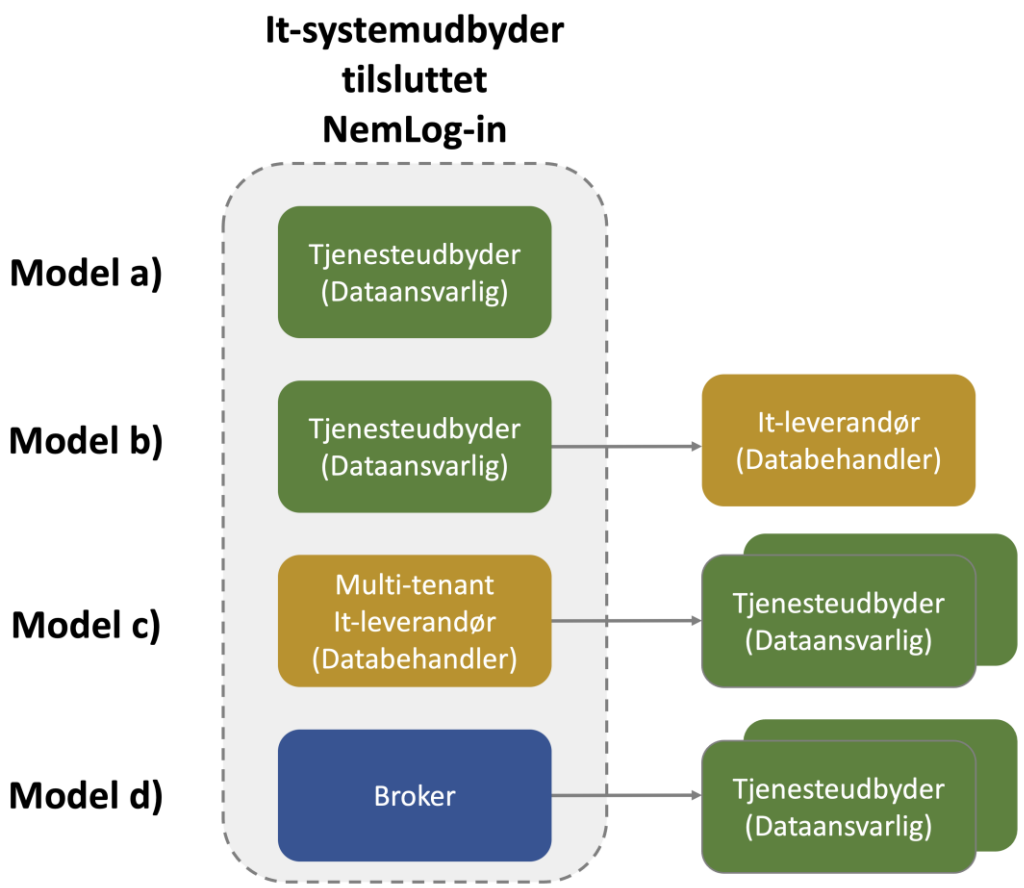
Digitale selvbetjeningsløsninger kan tilsluttes til NemLog-in efter forskellige modeller, som kan rumme forskellige leverandørkonstellationer:

a) Den dataansvarlige Tjenesteudbyder kan tilslutte sig til NemLog-in som It-systemudbyder og selv oprette og administrere it-systemer via NemLog-in's Administrationsportal.
b) Som model a) hvor Tjenesteudbyderen efter oprettelse af et it-system uddelegerer den tekniske administration til en it-leverandør, der er tilsluttet NemLog-in.
c) En it-leverandør kan tilslutte sig som It-systemudbyder til NemLog-in og oprette it-systemer på vegne af en eller flere bagvedliggende Tjenesteudbydere i rollen som Multi-tenant leverandør. F.eks. kan en Multi-tenant leverandør levere en Digital Selvbetjeningsløsning til en flerhed af kommuner på Software-as-a-Service vilkår. Tjenesteudbydere tilsluttet en Multi-tenant leverandøren er fortsat dataansvarlige for autentifikationssvar fra NemLog-in. Multi-tenant leverandøren er databehandler for Tjenesteudbydere.
d) En organisation kan i rollen som NemLog-in Broker (Sub-Broker) videreformidle Autentifikationer fra NemLog-in til bagvedliggende Tjenesteudbydere ved tiltrædelse af NemLog-in's brokeraftale. En broker indgår i tillidskæden ved selv at signere autentifikationssvar (security tokens) over for Tjenesteudbyderne og skal derfor være NSIS anmeldt som identitetsbroker. Detaljerede krav til Brokere fremgår på brokersitet: https://broker.nemlog-in.dk.

Rollerne og relationerne er illustreret i Figur 1 nedenfor.

Bemærk at i model a) og b) har Tjenesteudbyderen en direkte aftalerelation med Digitaliseringsstyrelsen, mens aftalerelationen med Digitaliseringsstyrelsen i model c) og d) går via en anden part end Tjenesteudbyderen.

Uagtet hvilken af ovennævnte modeller der anvendes, skal vilkår for Tjenester beskrevet i dette dokument overholdes. De tekniske krav til it-systemer er således uafhængige af, hvordan leverandørkonstellationen ser ud, eller hvem der har aftalerelationen til NemLog-in.



Figur 1: Tilslutningsmodeller i NemLog-in

2.3 Ændringer til krav og politikker

Digitaliseringsstyrelsen er berettiget til at opdatere nærværende krav og politikker for Tjenesters anvendelse af NemLog-in med et varsel på 3 måneder.

Ved væsentlige ændringer, der defineres som ændringer af grænseflader, der kræver ændringer i Tjenesterne gives som udgangspunkt et varsel på minimum 6 måneder. Hvis ændringer skyldes afhjælpning af et akut sikkerhedsmæssigt problem, kan en kortere frist dog være nødvendig. It-systemudbydere 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 It-systemudbydere, der på varslingstidspunktet er tilsluttet NemLog-in. Meddelelsen sendes til de e-mailadresser, som It-systemudbydere har opgivet.

2.4 Opsætning i NemLog-in's Administrationsportal

2.4.1 Tilslutning, vedligehold og frakobling

En organisation, der ønsker at tilslutte Tjenester til NemLog-in, skal først tilsluttes NemLog-in i rollen som It-systemudbyder.

Ved tilslutning vil NemLog-in ud fra et opslag i CVR-registret afgøre, hvorvidt der er tale om en offentlig myndighed eller privat organisation. På baggrund af denne registrering sikres det, at kun relevante services for den pågældende type af It-systemudbyder er tilgængelige i NemLog-in's Administrationsportal, således at en offentlig organisation ikke tilslutter private it-systemer og omvendt. En bemyndiget for It-systemudbyderen skal udpege en eller flere administratorer til at håndtere opsætning i administrationsportalen.

En privat It-systemudbyder vil som udgangspunkt alene kunne oprette it-systemer (Tjenester), der optræder som private over for NemLog-in. Hvis en privat It-systemudbyder ønsker at oprette et it-system, der agerer som offentlig Tjeneste, er dette muligt, hvis systemet **alene** anvendes af offentlige Tjenesteudbydere. Et eksempel på dette er, når It-systemudbyderen er en privat Multi-tenant leverandør og i denne rolle leverer Digitale Selvbetjeningsløsninger til offentlige Tjenesteudbydere (se model C ovenfor). I dette tilfælde skal It-systemudbyderen kontakte NemLog-in forvaltningen med henblik på at få omklassificeret it-systemet i NemLog-in fra 'privat' til 'offentligt'.

It-systemudbydere er (via deres udpegede administratorer) forpligtet til ved oprettelse af deres it-systemer i NemLog-in's Administrationsportal at anvende sigende og retvisende beskrivelser heraf og i øvrigt løbende sikre at alle registrerede oplysninger er opdaterede. Forpligtelsen omfatter såvel tekniske oplysninger som fx certifikater og tekniske metadata, kontaktoplysninger samt brugervendte beskrivelser, herunder referencetekst og alias som oplyser Slutbrugere om, hvad der logges ind på i loginsituationen.

It-systemer skal slettes i Administrationsportalen, når de ikke længere er aktive.

De brugervendte beskrivelser skal udformes, så de er letforståelige og sigende for den almindelige Slutbruger uden kendskab til It-systemudbyderens løsninger. Det anbefales at brugerteste beskrivelser med henblik på at sikre, at de fungerer i praksis. Digitaliseringsstyrelsen forbeholder sig ret til at kontakte en It-systemudbydere med henblik på forbedring af tekster, der ikke sikrer tilstrækkelig klarhed eller transparens for Slutbrugere. It-systemudbyderen er forpligtet til inden for rimelig tid at imødekomme Digitaliseringsstyrelsens henvendelse.

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.

It-systemudbydere 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 Tjenesterne.

2.4.2 Konfiguration af attributter og dataminimering

It-systemudbydere 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 Tjenester 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 3.7.

2.5 Ansvar i relation til sikkerhed

2.5.1 Generelt om It-systemudbyderens egen organisation

Det er It-systemudbyderens ansvar, at sikkerheden i egen organisation og egne systemer er tilstrækkelig, og at de sikkerhedskrav, der er gældende for den pågældende It-systemudbyder, efterleves.

2.5.2 Adgangskontrol i Tjenester

Tjenester tilsluttet NemLog-in 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, tildelte rettigheder og fuldmagter.

Ansvarsfordelingen mellem Digitaliseringsstyrelsen og Tjenesten er i denne situation således, at NemLog-in attesterer hvem Slutbrugeren er, sikringsniveauet for Autentifikationen, samt hvilke rettigheder og fuldmagter Slutbrugeren evt. er tildelt i NemLog-in. Det er Tjenestens adgangskontrol i egen løsning, der på denne baggrund beslutter, hvilke data og hvilke handlinger Slutbrugeren kan tilgå/foretage.

2.5.3 Certifikater hos It-systemudbydere

It-systemudbydere 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 egen hjemmeside. Certifikater skal anvendes i overensstemmelse med de certifikatpolitikker, de er udstedt i medfør af og de vilkår, som It-systemudbyderen har accepteret.

OIOSAML standarden stiller specifikke krav til tilladte CA'er og nøglelængder for certifikater anvendt til SAML-integrationen. Disse krav udelukker anvendelse af selvsignerede certifikater.

2.6 Forbrugsvarsling

It-systemudbydere 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 It-systemudbydere ressourcetræk på NemLog-in, således at der sikres kapacitet til at betjene øvrige Tjenester.

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

2.7 Test af integrationer

It-systemudbydere (sub-Brokere undtaget) er forud for anvendelse af NemLog-in's produktionsmiljø forpligtet til at gennemføre en integrationstest mod NemLog-in og indhente godkendelse heraf hos NemLog-in’s forvaltning. Testrapport uploades via administrationsportalen. Indholdet i integrationstesten fremgår af testdokumentet '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

Testdokumentet indeholder en række obligatoriske testcases, der sikrer at udvalgte aspekter af integrationen mellem NemLog-in og It-systemudbyderens systemer fungerer, således at den samlede føderation fremstår sammenhængende.

De beskrevne testcases dækker både offentlige og private Tjenesters anvendelse af NemLog-in services. Enkelte testcases skal dog alene gennemføres af offentlige Tjenester.

Hvis NemLog-in anvendes til 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'. Information herom fremgår af testdokumentet.

2.8 Logningspolitik

It-systemudbydere 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 It-systemudbydere 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.

2.9 Drift- og supportpolitik

It-systemudbydere er forpligtet til at overholde NemLog-in's drift- og supportpolitik, som er beskrevet her:

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

Dokumentet beskriver driftsvilkår for NemLog-in samt forhold vedrørende beredskab. Desuden beskrives supporten i forbindelse med opkobling og løbende drift af løsningen. Som beskrevet i ovennævnte politik tilbyder Digitaliseringsstyrelsen en række supportforums med relevant information på Digitaliser.dk.

3 Services i NemLog-in

3.1 Indledning

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

3.2 Autentifikationsservices

NemLog-in brokeren udstiller to SAML Identity Provider (IdP) endepunkter, der begge kan kaldes med henblik på Autentifikation af Slutbrugere, Single Logout og Attribute Query:

- En IdP baseret på OIOSAML 2.1.x specifikationen, som er forbeholdt offentlige Tjenester, og som skal udfases. Denne IdP bør ikke anvendes for nye Tjenester og eksisterende anvendere bør udforme en plan for migrering til OIOSAML 3.

- En IdP baseret på OIOSAML 3.0.x specifikationen, der kan anvendes til såvel offentlige som private Tjenester.

Begge IdP'er understøtter Autentifikation med MitID og 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 Tjenester har mulighed for Single Sign-On til it-systemer, hvorfra der udføres en myndighedsopgave, når Slutbruger i forvejen har en session med NemLog-in. Derimod skal Slutbrugere altid autentificere sig aktivt i NemLog-in, når de tilgår en privat Tjeneste eller en offentlig Tjeneste, hvorfra der ikke udføres en myndighedsopgave.

OIOSAML specifikationerne er tilgængelige her:

- https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

3.2.1 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.

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

Indtræder 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).

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

3.2.1.1 Maksimal sessionslængde

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

Tjenesten 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

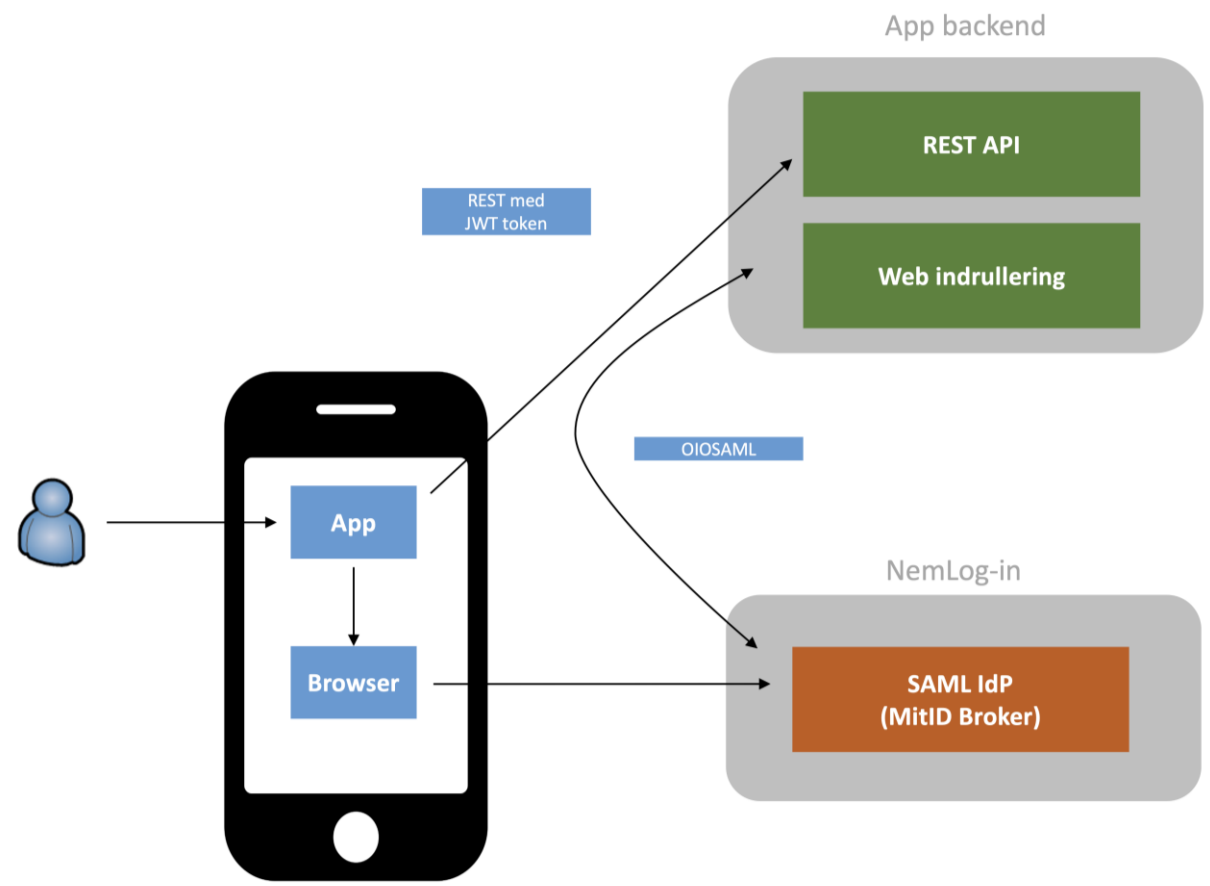
3.2.2 Timeout i NemLog-in

Ved timeout af NemLog-in's IdP-session vil Slutbrugeren skulle autentificere sig aktivt over for NemLog-in, næste gang en Tjeneste viderestiller en Slutbruger for log-in (via et SAML <AuthnRequest>). Lokale sessioner hos Tjenesten 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 Tjenester om, at de skal logge Slutbrugerne ud (såkaldt "single logout").

3.2.3 Autentifikation til 'native Apps'

Udgangspunktet for NemLog-in's autentifikationsservices er Autentifikation i traditionelle web-applikationer med en back-end, som der på forhånd er udvekslet SAML metadata med. Det er imidlertid også muligt at anvende NemLog-in's IdP'er til indrullering af brugere 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/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 fastlagt 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 3.7 om integrationskrav for yderligere detaljer.

- Kravene i dette dokument adresserer alene app'ens back-end, som er den komponent hos Tjenesten, der står for OIOSAML integrationen til NemLog-in. Den efterfølgende udstedelse af JWT-tokens[2] hos Tjenesten og levering til App'en står Tjenesten selv for, herunder håndtering af levetid, udløb og fornyelse af disse tokens. Der henvises til de tidligere omtalte OpenID Connect 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 testcases i integrationstesten er relevante i App-scenarier. Eksempelvis udstrækker NemLog-in's sessionshåndtering sig ikke til Apps. Dette betyder konkret, at der ikke er krav til, at Single Logout

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

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

3.2.4 Afledte identiteter

Hvis Tjenester baserer fremtidige Autentifikationer af en Slutbruger uden for 8 timers perioden beskrevet i afsnit 3.2.3 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 Slutbrugeren i egen sikkerhedsløsning i en app-løsning på mobile enheder.

It-systemudbydere 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.

It-systemudbydere skal særskilt være opmærksomme 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.

It-systemudbydere 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.

3.3 Opslags- og match tjenester

NemLog-in udstiller en række opslags- og match-tjenester, som kan anvendes af Tjenester med særlige behov relateret til Autentifikation og signering, f.eks. 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 Tjenester kan etableres 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.

It-systemudbydere anmoder om adgang til opslagstjenester via NemLog-in's Administrationsportal, og efterfølgende 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://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/log.in/dokumentation-og-guides/

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.

3.4 Rettighedsstyring for erhvervsbrugere

NemLog-in rummer funktionalitet til rettighedsstyring, der kan anvendes af **offentlige** Tjenester i deres selvbetjeningsløsninger rettet mod erhvervsbrugere. I løsningen kan Tjenester definere rettigheder til deres

[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.

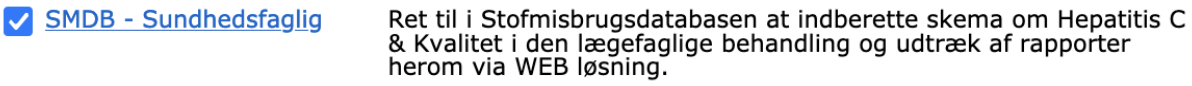
it-systemer, som en brugerorganisation herefter via MitID Erhverv kan tildele sine Erhvervsbrugere i egen organisation eller delegere til en anden organisation gennem en erhvervsfuldmagt.

Offentlige Tjenester 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 på et oplyst grundlag kan tildele rettigheder til erhvervsbrugere uden at der opstår fejl. Ved udformning af beskrivelsen bør der tages højde for, at brugeradministratoren ikke nødvendigvis kender til detaljerne i selvbetjeningsløsningen. Forklaringen bør derfor formidle tilstrækkelig kontekst til, at administratoren kan forstå implikationerne af en tildeling. Et eksempel fra NemLog-in's brugeradministration er vist i Figur 2 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 Tjenester 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 2: 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 Tjeneste 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. Herved er rettigheden ikke tilgængelig for brugerorganisationer, der ikke indgår i CVR filteret.

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

Dokumentationen for Administrationsportalen findes her:

- https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/

3.5 Digitale borgerfuldmagter

NemLog-in rummer en fuldmagtsservice (serviceområdet 'Digital repræsentation' i Lov om MitID og NemLog-in), der muliggør at offentlige Tjenester kan håndtere digitale fuldmagter/repræsentationsforhold i deres selvbetjeningsløsninger henvendt til private borgere og erhvervsbrugere, der kan tegne en virksomhed alene. Tjenester tager funktionaliteten i anvendelse ved at oprette et eller flere fuldmagtsprivilegier (repræsentationsforhold) for deres it-systemer i NemLog-in's Administrationsportal. Efter oprettelse af fuldmagtsprivilegier kan disse indgå i digitale fuldmagter, som tildeles en fuldmagtshaver 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 fuldmagtshaver) som beskrevet i OIOSAML. Endvidere kan Tjenester anvende et

API udstillet af fuldmagtsløsningen til at hente fuldmagter uafhængigt af om repræsentanten er logget ind hos Tjenesten.

3.5.1 It-systemudbyders ansvar

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

Det er It-systemudbyderens ansvar at afklare det juridiske grundlag for anvendelse af fuldmagter i Tjenesten samt etablere logning af en repræsentants handlinger i Tjenesten i henhold til NemLog-in's logningspolitik. Det er i denne forbindelse ligeledes It-systemudbyders ansvar at sikre, at der alene tilsluttes it-systemer til fuldmagtsløsningen, hvor it-systemudbyders lokale systemer og processer kan understøtte den digitale fuldmagtsafgivelse. Dette skal sikre, at borgere alene giver fuldmagt til Tjenester, hvor fuldmagt er tilstrækkeligt organisatorisk understøttet.

It-systemudbyderen skal:

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 It-systemudbyderen ikke vurderer 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 fuldmagtsgiver har et oplyst grundlag at tildele fuldmagtsrettigheder til fuldmagtshaver på.

For at sikre, at tildelte rettigheder er stabile over tid, må It-systemudbyder ikke tilføje nye adgange til eksisterende fuldmagtsprivilegier eller på anden måde udvide effekten af et fuldmagtsprivilegie.

Forbuddet mod at ændre i fuldmagtsprivilegier har til formål at forhindre, at fuldmagtshaver ikke på et senere tidspunkt opnår ændrede rettigheder eller udvidet effekt af et fuldmagtsprivilegie uden fuldmagtsgivers vidende eller godkendelse. Er der behov for at ændre et fuldmagtsprivilegie, skal der i stedet oprettes et nyt fuldmagtsprivilegie. Ved tvivlstilfælde skal Digitaliseringsstyrelsen kontaktes.

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

It-systemudbyder har mulighed for lade den praktiske udførelse af tilslutningsforløb og tekniske opsætning i NemLog-in udføre af en It-leverandør. It-systemudbyder er ansvarlig for alle handlinger, de udføres af en It-leverandør i NemLog-in. Tilsvarende er gældende for andre underleverandører eller rådgivere, som It-systemudbyder anvender i relation til NemLog-in.

Dokumentationen for Administrationsportalen findes her:

- https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester

Yderligere tekniske oplysninger om fuldmagtsløsningen findes på Tjenesteudbydersitet herunder API-beskrivelse og integrationsguide:

- https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/digital-fuldmagt/

3.5.1 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.

3.6 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://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/security-token-service/hjaelp-og-vejledning/

3.7 Integrationskrav

Som supplement til OIOSAML specifikationerne er der publiceret en integrationsguide, som indeholder yderligere detaljer og teknisk beskrivelse af, hvordan en It-systemudbyder kan integrere til NemLog-in. Guiden beskriver ligeledes forskellene på services der tilbydes offentlige og private Tjenester.

Integrationsguiden er publiceret på Tjenesteudbydersitet (https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/log-in/dokumentation-og-guides/).

It-systemudbydere skal overholde tekniske krav og anvisninger i integrationsguiden. Herunder fremhæves en række udvalgte forhold:

- Private Tjenester 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 stilles ikke krav om, at private Tjenester initierer Single Logout mod NemLog-in.
- En Tjeneste skal terminere lokale sessioner, når NemLog-in fremsender forespørgsel om Single Logout. It-systemudbydere kan søge Digitaliseringsstyrelsen om dispensation herfor i en konkret løsning, hvis der foreligger særlige behov eller omstændigheder. Bemærk at der i givet fald stadig skal svares korrekt på single logout forespørgsler som beskrevet ovenfor.

- En Tjeneste skal ved modtagelse af autentifikationssvar fra NemLog-in altid kontrollere, om det sikringsniveau, der er påstemplet i SAML Assertion fra NemLog-in, opfylder Tjenestens krav - og herunder blokere for (eller evt. indskrænke) Slutbrugerens adgang til Tjenesten, hvis sikringsniveauet ikke som minimum svarer til det fastsatte niveau. Dette gælder uagtet om Tjenesten har forespurgt om et bestemt sikringsniveau i sin autentifikationsanmodning mod NemLog-in. Eksempelvis er det Tjenestens ansvar at blokere for Autentifikationer på sikringsniveau Lav, hvis dette sikringsniveau ikke lever op til Tjenestens adgangspolitik.

- Det er Tjenestens 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.

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

4 Tjenesters anvendelse af certifikater fra NemLog-in

4.1 Signering med kvalificerede signaturer og -segl

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

Via Signeringsløsningen kan Slutbruger afgive kvalificerede elektroniske signaturer baseret på personcertifikater og brugercertifikater samt kvalificerede segl baseret på kvalificerede organisationscertifikater. 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 er udstedt af Digitaliseringsstyrelsens certificeringscenter (Den Danske Stat Tillidstjenester). Certificeringscenteret har udarbejdet og vedligeholder en Certificate Practice Statement (CPS), der definerer det sikkerhedsniveau, som er gældende for certifikatydelser fra certificeringscenteret. Digitaliseringsstyrelsens kan læses på https://www.ca1.gov.dk/. Certifikatpolitikker for de enkelte certifikater er tilgængelig på https://certifikat.gov.dk

Certifikaterne i Signeringsløsningen 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 10 dage.

Den tekniske dokumentation findes på denne side:

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

4.1.1 Den konkrete anvendelse af Signeringsløsningen

Ved Tjenesters anvendelse af Signeringsløsningen skal Tjenester tage stilling til følgende:

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

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

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

4.1.2 Signatur og segl

Tjenester kan efterspørge følgende elektroniske signaturer/segl:

- Kvalificeret elektronisk signatur baseret på et kvalificeret Personcertifikat
- Kvalificeret elektronisk signatur baseret på et kvalificeret brugercertifikat (også benævnt medarbejdercertifikat)
- Kvalificeret elektronisk segl baseret på et kvalificeret organisationscertifikat (også benævnt virksomhedscertifikat)

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

4.1.3 Angivelse af UUID

Tjenester skal træffe beslutning om hvilken model for UUID, der skal indeholdes i certifikatet som grundlag for Tjenestens 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 Tjenester

b) Et UUID specifik for Tjenesten

c) Et unikt UUID per signering (sessions UUID)

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

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

Tjenester kan ved anvendelse af sessions UUID via matchtjenesten beskrevet ovenfor i afsnit 3.3 få verificeret, om to forskellige UUID'er tilhører den samme person.

4.1.4 Signaturformat

Tjenester 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.

4.1.5 Referencetekst

Tjenester 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.

4.1.6 Digitaliseringsstyrelsens forpligtelser ved afgivelse af en elektronisk signatur eller segl

Efter Slutbrugers afgivelse af en elektronisk signatur eller segl til brug for Tjenester, kontrollerer og indestår Digitaliseringsstyrelsen som ansvarlig for CA'et 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. Digitaliseringsstyrelsen indestår ligeledes for, at der kun udstedes certifikater til identiteter, som er registreret med en sikkerhed, der svarer til personligt fremmøde.

4.1.7 Tjenesters forpligtelser ved modtagelse af en elektronisk signatur eller segl

Tjenester er ansvarlige 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 eller https://certifikat.gov.dk.

4.1.8 Sikring af dokumentation og bevisværdi for signaturer og segl

Tjenester er ansvarlige 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.

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

4.2 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.