DIGITALISERINGSSTYRELSEN

NemLog-in

Tekniske krav til Brokeres anvendelse af NemLog-in3

Version 1.2

Indholdsfortegnelse

1 Dokumenthistorik

Date	Version	Change description	Initials
17.09.2021	1.0	Første version klar til publicering	TG
18.10.2021	1.1	Opdatering af beskrivelser vedrørende signering samt tydeligere skelnen mellem brokeres organisation samt it-systemer. Tilpasning og udbygning af enkelte definitioner.	TG
14.03.2022	1.2	Opdateret til at matche seneste brokeraftale, herunder håndteringen af NSIS sikringsniveauer. Tilføjet referenceliste.	TG

2 Tekniske krav og politikker

Herunder fremgår tekniske krav og politikker relateret til Sub-Brokere tilsluttet NemLog-in. De tekniske krav og politikker er underlagt *NemLog-in's Sub-brokeraftale*.

Målgruppen for beskrivelsen er teknisk personale hos Brokere 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 og adgang til NemLog-in Sub-brokeraftale henvises til [BAT].

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 og Brokere kan administrere tilslutningen af deres it-systemer til NemLog-in, herunder hvilke attributter, der skal leveres i autentifikationssvaret samt certifikater og øvrige tekniske oplysninger relevant for integrationen.
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. En Broker tilsluttet NemLog-in benævnes også en Sub-broker.
Digital Selvbetjeningsløsning	Et it-system, hvor privatpersoner eller erhvervsbrugere med digitale identiteter kan tilgå digital selvbetjening efter at være blevet autentificeret. Benævnes også Selvbetjeningsløsning eller it-system. En Digital selvbetjeningsløsning svarer til begrebet tjeneste som nærmere defineret 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 serviceområdet 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	Et system tilsluttet NemLog-in enten som Tjenesteudbyder eller Broker.
Kvalificeret elektronisk signatur	En kvalificeret elektronisk signatur afgivet i Signeringsløsningen på baggrund af et kvalificeret certifikat. Medmindre andet specifikt er anført omfattet betegnelsen også kvalificeret elektronisk segl, der ligeledes kan afgives i Signeringsløsningen. Kvalificerede elektroniske signaturer svarer til

	traditionelle, papirbaserede 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 Sub-Brokere. Lokale IdP'er tilsluttet NemLog-in skal være NSIS-anmeldt (som Identitetsbroker) og skal baseres på identifikationsmidler fra en NSIS-anmeldt elektronisk Identifikationsordning.
MitID	Den nationale identitetsløsning, som afløser NemID. MitID er 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. 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.
Organisation	Juridisk enhed med et CVR-nummer. I dette dokument kan termen organisation dække over både offentlige myndigheder, offentligretlige organer og andre typer organisationer med CVR-nummer.
NSIS	National Standard for Identiteters Sikringsniveauer.
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 mod en Tjenesteudbyder via en eller flere mellemliggende Brokere.
Tjenesteudbyder	En organisation, der stiller én eller flere Digitale Selvbetjeningsløsninger til rådighed for Slutbrugere, og som autentificerer disse via en eller flere Brokere.
Tredjepartsbroker	En Broker, der er tilsluttet NemLog-in indirekte via en anden Sub-Broker (brokere i flere led) med henblik på at videreføre Services til

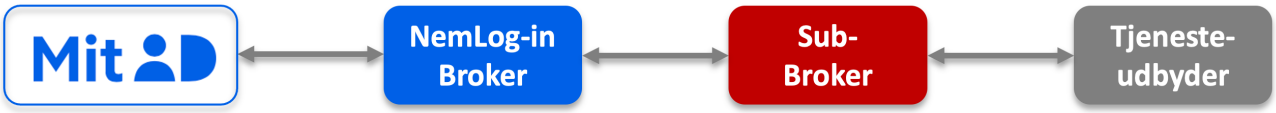
Tjenesteudbydere. Tredjepartsbrokere har modsat Sub-Brokere ikke et direkte aftaleforhold med NemLog-in.

Der henvises i øvrigt til brokeraftalens [BAT] definitioner, der skal fortolkes i overensstemmelse med ovenstående begreber.

2.2 Introduktion til Broker-begrebet

Ved en Broker (også betegnet 'Sub-Broker') forstås i dette dokument en organisation med et it-system, der er tilsluttet NemLog-in, og hvor it-systemet i NemLog-in's Administrationsportal er oprettet enten som 'Offentligt Brokersystem' eller 'Privat Brokersystem', jf. mere herom i afsnit 2.4.1 samt 2.4.3.

Når et it-system er oprettet i Administrationsportalen, kan det anvende NemLog-in's Services og videreformidle autentificerede identiteter til bagvedliggende Tjenesteudbydere. En Sub-Broker agerer i rollen som Identitetsbroker beskrevet i NSIS-standarden og skal dermed leve op til kravene heri. Prefixet 'Sub-' indikerer alene, at der er tale om en Broker, der i den fysiske konstellation i forhold til NemLog-in er i andet led, mens Broker-begrebet i NSIS er på logisk/konceptuelt niveau.



Figur 1: Kæde af Brokere

En organisation tilslutter sig i rollen som Tjenesteudbyder-organisation til NemLog-in for at få adgang til NemLog-in Services herunder muligheden for at tilslutte it-systemer, der anvender NemLog-in Services. Ved tilslutning af et it-system kan Organisationen vælge, om it-systemet er en almindelig Digital Selvbetjeningsløsning eller et broker it-system. Organisationen indtræder i Broker-rollen i det øjeblik, der tilsluttes et it-system, som i NemLog-in's Administrationsportal markeres med typen offentlig- eller privat Brokersystem. Der kan i princippet indskydes flere lag af Sub-brokere mellem NemLog-in og Tjenesteudbydere. Her er det kun den øverste Sub-Broker i kæden, som tilsluttes og indgår aftale med NemLog-in. Alle øvrige Brokere i kæden (i NemLog-in regi benævnt Tredjepartsbrokere) er dog ligeledes Identitetsbrokere, som defineret i NSIS-standarden.

Ovennævnte betyder, at Organisationer skal acceptere NemLog-in's vilkår for Tjenesteudbydere, uanset om de vil agere i rollen som Tjenesteudbyder eller broker. Dette skyldes, at der kun er ét tilslutningsforløb, som anvendes til begge roller.

2.2.1 NemLog-in Brokerservices

Der findes to typer af Services i NemLog-in for it-systemer, der agerer i rollen som Broker:

- Simple Brokerservices, hvor Brokeren anvender de samme tekniske snitflader som Tjenesteudbydere tilsluttet NemLog-in, herunder [OIOSAML] snitfladerne til brugerautentifikation beskrevet i kapitel 3.1.
- Avancerede brokerservices, hvor Brokere anvender særlige services, der ikke er tilgængelige for Tjenesteudbydere.

Denne version af de tekniske krav til Brokere omfatter alene de simple Brokerservices i NemLog-in. Når de avancerede brokerservices bliver gjort tilgængelige i NemLog-in, er Broker forpligtet til at tiltræde opdaterede vilkår, hvis Brokeren ønsker at anvende de avancerede brokerservices.

2.3 Ændringer til krav og politikker

Digitaliseringsstyrelsen kan ændre aftalen og omfattede politikker med et varsel på 3 måneder.

Ved større ændringer, herunder ændringer, der vurderes at påvirke Brokers systemer, vil Digitaliseringsstyrelsen tilstræbe at give et varsel på 6 måneder.

Såfremt ændringer af Digitaliseringsstyrelsen vurderes væsentlige af hensyn til driftsmæssige forhold, herunder sikkerhed, kan ændringer gennemføres med kortere varsel med virkning fra meddelelsestidspunktet. Tilsvarende er ligeledes gældende for ændringer, som Digitaliseringsstyrelsen er forpligtet til at implementere i disse vilkår som følge af aftale med MitID-leverandøren om levering af MitID brokerservices.

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 Brokersitet. Der udsendes herudover særskilt meddelelse til de Brokere, der på varslingstidspunktet er tilsluttet NemLog-in. Meddelelsen sendes til de e-mailadresser, som Brokerne har opgivet i NemLog-in's Administrationsportal.

2.4 Opsætning i Erhvervsadministrationen i NemLog-in

2.4.1 Tilslutning, vedligehold og frakobling

En Organisation, der ønsker at anvende NemLog-in's Services til Brokere, skal først tilsluttes NemLog-in i rollen som Tjenesteudbyder. Tilslutningen foretages i serviceområdet Erhvervsadministration i NemLog-in. Når en organisation er oprettet som Tjenesteudbyder, er det efterfølgende muligt for organisationen at tilslutte It-systemer, der kan optræde som Brokersystemer over for NemLog-in.

Ved tilslutningen som Tjenesteudbyderorganisation vil NemLog-in ud fra et opslag i CVR-registret afgøre, hvorvidt foretages af en offentlig eller privat Organisation. En bemyndiget for Organisationen skal i forbindelse med tilslutningen udpege én eller flere administratorer til at håndtere den tekniske opsætning af It-systemer i NemLog-in's Administrationsportal.

Gennem Administrationsportalen kan en offentlig Tjenesteudbyderorganisation ved selvbetjening tilslutte It-systemer med rollen som offentlige Broker i NemLog-in (til brug for formidling af Autentifikation til Offentlige Selvbetjeningsløsninger). Ligeledes kan en privat Tjenesteudbyderorganisation alene tilslutte It-systemer i rollen som privat Brokere (til brug for formidling af Autentifikation til Private Selvbetjeningsløsninger).

Hvis ovenstående registreringer ikke korrekt afspejler de Digitale Selvbetjeningsløsninger, som Brokeren formidler Autentifikation til via tilsluttede Tjenesteudbydere, skal Brokeren kontakte NemLog-in forvaltningen i Digitaliseringsstyrelsen. Der henvises til afsnit 2.4.3 for en nærmere beskrivelse af offentlige og private brokersystemer og de tjenester, der formidles Autentifikation til.

Brokere skal ved oprettelse af It-systemer i NemLog-in's Administrationsportal sikre, at der anvendes sigende og retvisende beskrivelser, samt løbende at holde disse oplysninger ajour. Dette omfatter bl.a. It-systemets Sikringsniveau, der skal være i overensstemmelse med niveauet i den godkendte NSIS-anmeldelse. Forpligtelsen til ajourføring af oplysninger omfatter såvel tekniske oplysninger fx relateret til certifikater og

tekniske metadata og kontaktoplysninger på Brokeren, samt brugervendte beskrivelser, herunder referencetekst og alias som eksempelvis vises i MitID klienten og oplyser Slutbrugere om hvilken Tjenesteudbyder, der logges ind hos i loginsituationen. Brokeren er ligeledes ansvarlig for, at brugervendte referencetekster som beskriver kontekst for login, der modtages fra Brokerens bagvedliggende Tjenesteudbydere, og som sendes til NemLog-in, er retvisende.

Brokeren skal slette sine It-systemer i Administrationsportalen, når de ikke længere er aktive.

Brokeren skal endvidere sikre, at brugervendte beskrivelser skal udformes, så de er letforståelige for den almindelige Slutbruger, der ikke har et specifikt kendskab til Brokerens eller Tjenesteudbyderes systemer. Digitaliseringsstyrelsen anbefales at brugerteste beskrivelserne med henblik på at sikre, at de fungerer i praksis. Digitaliseringsstyrelsen kan pålægge en Broker at ændre brugervendte beskrivelser, såfremt de ikke sikrer tilstrækkelig klarhed eller transparens for slutbrugere. Brokeren er forpligtet til inden for rimelig tid at imødekomme Digitaliseringsstyrelsens pålæg.

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.

Brokere er ansvarlige for alle aspekter af deres egne It-systemer (herunder funktionalitet, sikkerhed, overholdelse af NSIS-standarden, brugervenlighed, tilgængelighed og aftestning), uanset om der til integrationen med NemLog-in anvendes en referenceimplementering[1] fra Digitaliseringsstyrelsen eller anden type software. NemLog-in's ansvar er således alene begrænset til de Services, der leveres til Brokere.

2.4.2 Krav om NSIS-anmeldelse

Brokere tilsluttet NemLog-in skal NSIS-anmeldes forud for levering af Services til sine kunder.

I henhold til NSIS-standarden må en Identitetsbroker ikke formidle Autentifikationer til en tredjepart på et højere sikringsniveau, end brokeren selv er anmeldt til.

Et It-system, der agerer i rollen som Broker, skal være anmeldt som Identitetsbroker, før det kan tilsluttes NemLog-in's produktionssystemer. Det er dog muligt at få adgang til at teste i NemLog-in's testmiljøer i forbindelse med udviklingen af en Broker, inden NSIS-anmeldelsen er gennemført. I NemLog-in's brugerflade er det kun muligt at tilslutte Brokersystemer på sikringsniveau Betydelig samt Høj. Ønsker Organisationen at tilslutte en Broker anmeldt på sikringsniveau Lav, skal der rettes henvendelse til Digitaliseringsstyrelsen med henblik på særlig, teknisk håndtering heraf.

2.4.3 Offentlige og private Brokersystemer

De It-systemer, som en Broker tilslutter til NemLog-in, kan enten optræde som offentligt- eller privat Broker. Kategoriseringen af It-systemerne sker i overensstemmelse med følgende:

- **Offentligt Brokersystem**
  Et Offentligt Brokersystem formidler via en Tjenesteudbyder Autentifikationer til Digitale Selvbetjeningsløsninger/tjenester, hvorfra der udføres en myndighedsopgave (Offentlige Selvbetjeningsløsning). Den dataansvarlige for tjenesten vil oftest være en offentlig myndighed eller et offentligretligt organ.

[1] OIOSAML referenceimplementeringer findes på Digitaliser.dk i denne gruppe: https://digitaliser.dk/group/42063/resources

- **Privat Brokersystem**
  Et Privat Brokersystem formidler via en Tjenesteudbyder autentifikationer til Digitale Selvbetjeningsløsninger/tjenester, hvorfra der ikke udføres en myndighedsopgave (Privat Selvbetjeningsløsning). Den dataansvarlige for tjenesten kan både være en privat organisation, offentlig myndighed eller et offentligretligt organ.

Brokeren skal sikre, at Tjenesteudbydere samt bagvedliggende Tredjepartsbrokere tilsluttet Brokeren kategoriserer egne It-systemer/Digitale Selvbetjeningsløsninger i overensstemmelse med ovenstående, og at tilslutningen sker korrekt til Brokeren.

En myndighed, der eksempelvis både har en Digital Selvbetjeningsløsning, hvorfra der udføres en myndighedsopgave og en selvbetjeningsløsning, hvorfra der *ikke* udføres en myndighedsopgave, skal således etablere to separate tilslutninger til Brokeren, og Brokeren skal ligeledes videreformidle til og fra NemLog-in via separate tilslutninger af hhv. et Offentligt Brokersystem og et Privat Brokersystem.

2.4.4 Entydigt ansvar for It-systemer

Et It-system oprettet i NemLog-in tilhører en entydig Broker(organisation), der er dataansvarlig for It-systemets behandling af Autentifikationssvaret fra NemLog-in i forbindelse med Brokerens videreformidling af Autentifikationsanmodninger samt svar herpå. Autentifikationsanmodninger fra Broker til NemLog-in skal entydigt identificere Brokeren i henhold til OIOSAML-standarden og Brokeren skal desuden entydigt angivne den bagvedliggende Tjenesteudbyder via 'ProviderName' feltet i SAML autentifikationsanmodningen, jf. desuden afsnit 3.1. Dette gælder uanset om der måtte være Tredjepartsbrokere mellem Sub-Brokeren tilsluttet NemLog-in og den bagvedliggende Tjeneste (brokere i flere led).

2.4.5 Konfiguration af attributter

Brokere skal ved opsætning i Administrationsportalen aktivt tage stilling til det sæt af attributter, som Brokers It-systemer efterspørger fra NemLog-in. Der bør ikke i Administrationsportalen konfigureres flere attributter i it-systemers metadata, end det er nødvendigt, ud fra principperne om dataminimering og privacy-by-design. Eksempelvis bør der kun efterspørges CPR-nummer og andre globale identifikatorer, hvis der er et sagligt behov for dette og der i øvrigt foreligger tilstrækkelig hjemmel. Der er forskelle på hvilke attributter, som offentlige hhv. private Brokere kan få udleveret- eksempelvis leverer NemLog-in ikke CPR-numre til private Brokere. For nærmere beskrivelse af tilgængelige attributter henvises til integrationskrav beskrevet i afsnit 3.3.

2.5 Ansvar i relation til sikkerhed

2.5.1 Generelt om Brokeres egen organisation

Det er Brokerens ansvar, at sikkerheden i egen organisation og egne systemer er tilstrækkelig i forhold til egne behov og at krav som brokeren er underlagt efterleves. Dette vil eksempelvis omfatte krav i NSIS-standarden, relevant lovgivning og vilkår samt de sikkerhedskrav, der er beskrevet i dette og refererede dokumenter.

2.5.2 Certifikater hos Brokere

Brokere er ansvarlige for at anskaffe, forny og registrere egne certifikater - dette gælder både certifikater anvendt i integrationen mod NemLog-in samt certifikater til øvrige formål, herunder certifikater anvendt på

Brokerens hjemmeside. Certifikater skal anvendes i overensstemmelse med de certifikatpolitikker, de er udstedt i medfør af. Det skal særskilt bemærkes, 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.

2.6 Forbrugsvarsling

Brokere 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 (herunder It-systemer hos Tjenesteudbydere tilsluttet Brokeren).

Ved uvarslet forbrugsstigning i trafikmængden forbeholder Digitaliseringsstyrelsen sig ret til teknisk at begrænse Brokers ressourcetræk på NemLog-in med henblik på at sikre kapacitet til at betjene øvrige Brokere og Tjenesteudbydere.

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

2.7 Test af Brokeres integration

Broker er inden anvendelse af NemLog-in's produktionsmiljø forpligtet til at gennemføre en dækkende integrationstest mod NemLog-in for at sikre, at integrationen fungerer korrekt.

Broker er ansvarlig for at udforme og afvikle integrationstesten, men kan evt. finde inspiration i den test-suite, som Digitaliseringsstyrelsen har udformet til Tjenesteudbydere:

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

Det anbefales i særdeleshed at Broker er opmærksom på test af single logout opførsel og sessionsstyring på tværs af NemLog-in, Brokeren og Brokerens bagvedliggende Tjenester.

2.8 Logningskrav

Brokeren skal logge alle forespørgsler til og fra NemLog-in, herunder forespørgsler knyttet til Autentifikation, single logout, signering samt API-kald.

Brokeren skal desuden logge autentifikationsanmodninger fra sine bagvedliggende Tjenesteudbydere samt svar på disse. Logningerne skal opbevares i minimum 6 måneder.

Brokere skal sikre, at logningen sker med præcist tidsstempel. Serverne skal hente deres tid fra en tidsserver, som er Stratum 2 eller højere (se http://en.wikipedia.org/wiki/Network_Time_Protocol), og skal desuden resynkronisere så ofte, at tiden højst afviger et millisekund fra UTC.

2.9 Drift- og supportpolitik

Brokere 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 den fællesoffentlige log-in-løsning, forhold vedrørende beredskab og support i forbindelse med opkobling og løbende drift af løsning. Som beskrevet i ovennævnte politik tilbyder Digitaliseringsstyrelsen en række supportforums med relevant information på Digitaliser.dk.

3 Services i NemLog-in3

Herunder beskrives de tekniske Services i NemLog-in3-løsningen med tilhørende krav til Broker ved dennes anvendelse af disse services. Der henvises til relevant teknisk dokumentation på Brokersitet[2], hvor yderligere detaljer om integrationer, protokoller og Services fremgår.

3.1 Autentifikationsservices

NemLog-in3 udstiller ét SAML Identity Provider (IdP) endepunkter [OIOSAML], der kan kaldes af Brokeres It-systemer med henblik på Autentifikation af Slutbrugere, Single Logout og Attribute Query:

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

IdP'en understøtter Autentifikation med NemID, MitID og på sigt lokale IdP'er.

Digitaliseringsstyrelsen forbeholder sig ret til at tilføje flere typer identifikationsmidler, der opfylder kravene til 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. Brokeren skal sikre, at dens tilsluttede It-systemer til enhver tid overholder kravene i de gældende [OIOSAML] specifikationer hørende til de anvendte IdP'er.

Brokere skal entydigt angivne den bagvedliggende Tjenesteudbyder via 'ProviderName' feltet i SAML autentifikationsanmodningen (SAML AuthnRequest). Da feltet skal vises i brugergrænseflader (log-in klienter) skal denne angivelse på en entydig og transparent måde identificere hvilken Tjeneste, Slutbrugeren logger ind på. Se endvidere afsnit 2.4.1.

En offentlig Broker har mulighed for Single Sign-on i NemLog-in, når der i den bagvedliggende Digitale selvbetjeningsløsning udfører en myndighedsopgave og Slutbruger i forvejen har en session med NemLog-in. NemLog-in sikrer derimod, at Slutbruger altid skal autentificere sig aktivt i NemLog-in, når autentifikationsanmodningen sker gennem en privat Broker - dvs. Single Sign-on er ikke muligt her.

OIOSAML specifikationerne er tilgængelige her:

- https://broker.nemlog-in.dk/dokumentation-og-integration

3.1.1 Sessionshåndtering og timeout

En SAML Assertions udløbstidspunkt skal valideres som beskrevet i [OIOSAML] standarderne (NotOnOrAfter attributten). Hvis SAML Assertion præsenteres efter udløb, skal den afvises.

Brokere (og bagvedliggende Tjenesteudbydere) kan oprette en brugersession på baggrund af en gyldig Autentifikation med NemLog-in. I den forbindelse skal Broker og dennes Tjenesteudbydere konfigurere deres respektive 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 Brokers It-system (dvs. såkaldt 'sliding expiration'), eller om den er uafhængig af brugeraktivitet. Brokerens timeout-periode må maksimalt sættes til 50 min. Digitaliseringsstyrelsen anbefaler dog generelt en timeout-periode på 30 min.

Indtræder timeout hos Broker eller Tjenesteudbyder, skal der sendes en ny autentifikationsanmodning til NemLog-in. Hvis Slutbrugerens browser fortsat har en session med NemLog-in, kan

[2] https://broker.nemlog-in.dk

autentifikationsanmodningen evt. besvares af NemLog-in, uden at Slutbrugeren skal autentificere sig aktivt igen (dvs. via Single Sign-on).

Den samlede sessionslængde hos en Broker og dennes bagvedliggende Tjenesteudbydere må højst være 8 timer (forudsat Slutbrugeren kontinuerligt er aktiv), hvorefter Slutbrugeren skal re-autentificeres via NemLog-in.

Tjenesteudbydere tilsluttet en Broker 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.

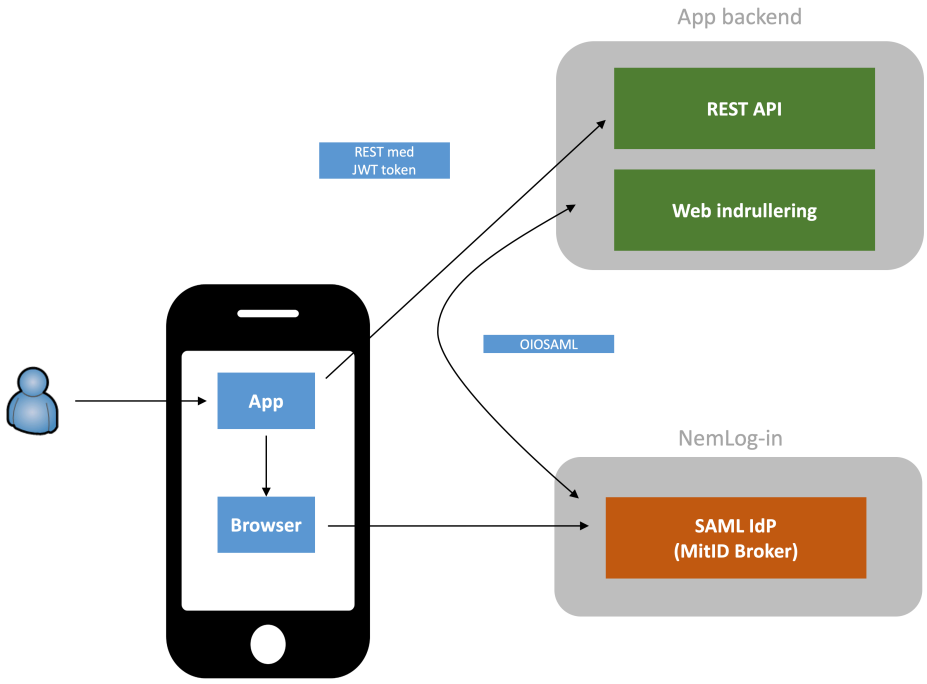
Hvis en Broker (evt. på forespørgsel fra en bagvedliggende Tjeneste) af sikkerhedsmæssige grunde vil sikre sig, at Slutbrugeren bliver påtvunget aktiv Autentifikation i NemLog-in løsningen, kan Brokeren sætte parameteren ForceAuthn=”true” i kaldet til NemLog-in (se [OIOSAML] for detaljer).

3.1.2 Timeout i NemLog-in

Efter timeout af NemLog-in’s IdP-session, vil NemLog-in gennemtvinge, at Slutbrugeren autentificerer sig aktivt over for NemLog-in, næste gang en Brokers It-system viderestiller en Slutbruger for log-in (via et SAML <AuthnRequest>). Lokale sessioner hos Brokere kan vedblive med at være aktive, jf. dog afsnit 3.1.1, selvom NemLog-in’s session udløber. Bemærk, at NemLog-in ved timeout ikke sender beskeder til Brokere 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 webapplikationer 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 [OIDC].



Figur 2: 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:

- I integrationsdokumentet [INT-TU] er der er fastlagt krav til den browser-komponent, der fungerer som user-agent på Slutbrugerens mobile enhed i interaktionen med NemLog-in. Eksempelvis er 'web views' af sikkerhedsmæssige grunde ikke tilladt. Kravene fremgår i integrationsdokumentationen [INT-TU] hørende til OIOSAML snitfladerne, der er ens for Brokere og Tjenesteudbydere.

- Kravene i dette dokument adresserer alene app'ens back-end, som er den komponent hos Brokeren, der står for OIOSAML integrationen til NemLog-in. Den efterfølgende udstedelse af eksempelvis JWT-tokens[3] hos Brokeren og levering til App'en er er Brokeren ansvarlig for at håndtere, herunder i forhold til levetid, udløb og fornyelse af disse tokens. Der henvises til de tidligere beskrevne OpenID Connect [OIDC] profiler for yderligere detaljer og 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.

Broker er ansvarlige for, at deres bagvedliggende Tjenesteudbydere overholder ovennævnte krav for Apps, der autentificerer brugere gennem Brokeren (og NemLog-in).

3.1.4 Afledte identiteter

Hvis Broker eller Tjenesteudbydere baserer fremtidige Autentifikationer af en Slutbruger udenfor perioden beskrevet ovenfor i afsnit 3.1.1 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, herunder MitID.

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

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

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

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

Brokere og Tjenesteudbydere 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 Brokere 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 Brokere 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.

Brokere tilslutter sig opslagstjenester via NemLog-in's Administrationsportal. Den 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 på brokersitet [INT-BR].

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.

3.3 Integrationskrav

Detaljerede krav til og tekniske beskrivelser af hvordan Brokere kan integrere til NemLog-in, findes i dokumentationen, der supplerer [OIOSAML] specifikationerne.

Dokumentationen til Brokere findes publiceret på brokersitet [INT-BR].

Brokere skal overholde tekniske krav og anvisninger i integrationsdokumentet. Omfattet af disse krav er bl.a.:

- Private Brokere skal - uagtet at disse ikke kan deltage i single sign-on - implementere et SAML single logout endepunkt som beskrevet i [OIOSAML], der svarer NemLog-in korrekt på SAML Single Logout forespørgsler. Der er omvendt ikke krav om, at private Brokere initierer Single Logout mod NemLog-in.

- Offentlige Brokere er ansvarlige for at sikre, at deres Tjenesteudbydere logger Slutbrugeren ud, når Brokeren modtager en Single Logout forespørgsel fra NemLog-in. Logout forespørgsler skal således videreformidles til bagvedliggende Tjenester.

- En Broker skal terminere lokale sessioner, når NemLog-in sender forespørgsel om Single Logout. Brokere kan dog søge Digitaliseringsstyrelsen om dispensation herfor i en konkret løsning, hvis der er særlige behov eller omstændigheder, der gør sig gældende. Bemærk En dispensation ændrer ikke på kravet om, at der stadig skal svares korrekt på single logout forespørgsler som beskrevet ovenfor.

- En Broker skal ved modtagelse af autentifikationssvar fra NemLog-in altid kontrollere, det sikringsniveau, der er påstemplet i SAML Assertion fra NemLog-in. Der skal foretages kontrol selv om Brokeren ikke har forespurgt om et bestemt sikringsniveau i sin autentifikationsanmodning mod NemLog-in.

- Det er Brokerens ansvar at kontrollere Slutbrugerens alder, inden der gives adgang til en bagvedliggende digital selvbetjeningsløsning, der har begrænsninger i forhold til visse aldersgrupper. Broker og Tjenesteudbyder kan indbyrdes aftale, at Tjenesteudbyder foretager denne kontrol. Det bemærkes, 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 integrationsdokumentet for detaljer om dette.

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

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

NemID-signeringstjenesten gør det enkelt for Brokere (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 webapplikation, hvor Slutbrugeren kan se den tekst, der skal signeres samtidig med, at der afgives accept for signering.

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 anmodning leveres til Brokeren.

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 Brokerens eller dennes Tjenesteudbyderes eget ansvar 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 at godtgøre, hvilken aftaletekst brugeren oprindeligt underskrev.

3.4.1 Type af signatur

Slutbrugeren kan afgive signaturer med:

- OCES Personcertifikat
- OCES Medarbejdercertifikat
- OCES Virksomhedscertifikat

Certifikatpolitikkerne kan læses på: https://certifikat.gov.dk/politikker-for-tillidstjenester/

3.4.2 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.

Brokeren 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 Brokeren

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

3.4.3 Brokeres pligt ved anvendelse af NemID Signeringstjenesten

Broker 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 følgende fremgår: "Ung mellem 15 og 18 år - 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.

3.4.4 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.

3.5 Signering med kvalificerede certifikater

NemLog-in udstiller en signeringsløsning, der gør det muligt for Brokere at indhente Slutbrugeres kvalificerede elektroniske signaturer og segl på dokumenter og anden data.

I modsætning til legacy-løsningen beskrevet i ovenstående afsnit 3.4 afgives signaturer i denne løsning under anvendelse af slutbrugerens MitID-identifikationsmiddel eller evt. gennem autentifikation via en lokal IdP.

Slutbrugeren kan afgive signaturer, der er knyttet til følgende certifikattyper:

- Kvalificeret Personcertifikat
- Kvalificeret medarbejdercertifikat
- Kvalificeret virksomhedscertifikat

Certifikatpolitikkerne kan læses på: https://certifikat.gov.dk/politikker-for-tillidstjenester/

I Signeringsløsningen afgives kvalificerede signaturer og segl (i henhold til eIDAS forordningen) baseret på (kvalificerede) kortidscertifikater.

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 Certificeringscenteret for den Danske Stat. Certificeringscenteret har udarbejdet og vedligeholder en Certificate Practice Statement (CPS), der definerer det sikkerhedsniveau, som er gældende for certifikatydelser fra certificeringscenteret. CPS og bagvedliggende certifikatpolitik kan læses 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 kan modtages og læses af en bred portefølje af systemer udløber certifikatet først efter 10 dage.

Dokumentationen findes på brokersitet [SIG].

3.5.1 Den konkrete anvendelse af Signeringsløsningen

Ved Brokers anvendelse af Signeringsløsningen, skal Broker tage stilling til følgende, som mere detaljeret beskrevet i [SIG]:

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

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

3.5.2 Signatur og segl

Broker 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.

3.5.3 Angivelse af UUID

Brokere skal træffe beslutning om hvilken model for UUID, der skal indeholdes i certifikatet som grundlag for Brokers efterfølgende behandling af det signerede dokument og tilhørende signatur. 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 Brokere og Tjenesteudbydere

b) Et UUID specifikt for Broker

c) Et unikt UUID per signering (sessions UUID)

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

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

Broker 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.

3.5.4 Signaturformat

Broker 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.

3.5.5 Referencetekst

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

Referenceteksten må ikke indeholde personoplysninger og bør derfor være overordnet (fx "underskrift af låneaftale").

3.5.6 Digitaliseringsstyrelsens forpligtelser ved afgivelse af en elektronisk signatur eller segl

Efter Slutbrugers afgivelse af en elektronisk signatur eller segl til brug for Broker, 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. Digitaliseringsstyrelsen indestår for, at der kun udstedes certifikater til identiteter, som er registreret med en sikkerhed, der svarer til personligt fremmøde.

3.5.7 Brokers forpligtelser ved modtagelse af en elektronisk signatur eller segl

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

Sådanne anvendelsesbegrænsninger vil fremgå af certifikatet og Digitaliseringsstyrelsens hjemmeside (http://certifikat.gov.dk).

3.5.8 Sikring af dokumentation og bevisværdi for signaturer og segl

Broker eller dennes Tjenesteudbydere er ansvarlige for at opbevare og arkivere det signerede dokument (i uændret form) og signaturbeviset fra NemLog-in, samt for at den Slutbruger, som underskriver, 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. Signeringsløsningen opnår på intet tidspunkt i signeringsprocessen adgang til det dokument eller de data, der signeres.

Broker eller dennes Tjenesteudbydere 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.

3.6 Validering af elektroniske signaturer og segl

Digitaliseringsstyrelsen stiller en kvalificeret valideringstjeneste til rådighed for validering af elektroniske signaturer og elektroniske segl udstedt af den Danske Stat CA repræsenteret ved Digitaliseringsstyrelsen.

Valideringstjenesten er offentlig tilgængelig og kan frit benyttes af alle.

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

Yderligere detaljer om tillidstjenester kan findes på hjemmesiden [TT].

4 Referencer

[INT-BR] ”Integration with NemLog-in for brokers”, Nets.

https://broker.nemlog-in.dk/dokumentation-og-integration

[INT-TU] “Integration with NemLog-in 3”, Digitaliseringsstyrelsen.

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

[OIDC] ”Open ID Connect Profile V0.91”, Digitaliseringsstyrelsen.

https://digst.dk/it-loesninger/nemlog-in/anvendelse/openid-connect-profiler/

[SIG] “Broker Signeringsdokumentation” (zip fil)

https://broker.nemlog-in.dk/dokumentation-og-integration/

[OIOSAML] "OIOSAML Web SSO Profile 3.0".

https://digst.dk/it-loesninger/nemlog-in/standarder/

[BAT] "Aftale - Sub-Broker tilsluttet NemLog-in" (Brokeraftale), Digitaliseringsstyrelsen.

https://www.nemlog-in.dk/broker/vilkaar/

[TT] "Den Danske Stat Tillidstjenester".

https://www.ca1.gov.dk/forside/