Introduktion til NemID og NemID tjeneste-udbyderpakken

Indholdsfortegnelse

Versionsfortegnelse

31. januar 2014	Version 4.0	PHJER
17. februar 2014	Version 4.1	PHJER
11. april 2014	Version 4.2	BMATZ
19. maj 2014	Version 4.3	PHJER
22. maj 2014	Version 4.4	PHJER
2. juni 2014	Version 4.5	PHJER
4. juni 2014	Version 4.6	PHJER
17. marts 2016	Version 4.7	KMAIB
23. marts 2016	Version 4.8	KMAIB
30. maj 2016	Version 4.9	KMAIB
30. august 2016	Version 4.10	KMAIB
13. september 2016	Version 4.11	KMAIB
30. april 2018	Version 4.12	RMELG

1 Dokumentets formål og målgruppe

Dette dokument er en del af NemID tjenesteudbyderpakken.

Formålet med dokumentet er at give en generel introduktion til NemID og NemID tjenesteudbyderpakken, så der skabes det nødvendige overblik over de tilgængelige muligheder samt implementeringens omfang.

Dokumentet henvender sig til de personer hos NemID tjenesteudbyder, der er ansvarlige for de overordnede beslutninger vedrørende implementeringen af NemID.

2 Introduktion til NemID

NemID er danskernes sikkerhedsløsning til log-in og signering på internettet.

> Der henvises til dokumentet Termer og begreber i NemID for en forklaring af de termer og begreber, der anvendes i dette dokument og i NemID tjenesteudbyderpakken generelt (www.nets.eu/tu-pakke)

En typisk anvendelse af NemID er, at en slutbruger ønsker at logge på hos en tjenesteudbyder. Dette foregår ved, at slutbrugeren åbner tjenesteudbyderens hjemmeside og vælger en "Log på"-funktion. Derved initierer tjenesteudbyderen, at slutbrugeren bliver autentificeret, hvorefter resultatet af autentificeringen meddeles til tjenesteudbyderen. På baggrund heraf kan tjenesteudbyderen så vælge enten at afvise slutbrugeren eller at præsentere denne for en personaliseret hjemmeside.

> Digitaliseringsstyrelsen har fået udviklet en særlig tjenesteudbyderpakke, kaldet "LSS til NemID TU-pakke", der giver understøttelse af tablets og smartphones for brugere med en NemID medarbejdersignatur som nøglefil i virksomheder, der benytter en lokal signaturserver (LSS).
>
> Denne funktionalitet er nu fuldt integreret i NemID CodeFile-klienten (Klient uden OTP) og kræver ikke som tidligere separat implementering hos den enkelte tjenesteudbyder.
>
> Dokumentation af LSS til NemID er tilgængelig på adressen https://www.lss-for-nemid.dk

2.1 Anvendelse og opbevaring af privatnøgler

Når en bruger anvender NemID til at logge på tjenester eller til at signere dokumenter på internettet, sker der rent sikkerhedsmæssigt det, at brugeren anvender sin såkaldte privatnøgle. Brugerens privatnøgle kan opbevares på to forskellige måder:

- Central opbevaring: Brugerens privatnøgle opbevares på Nets DanID's server. Løsningen kaldes almindeligvis NemID med Nøglekort.
- Lokal opbevaring: Brugeren opbevarer selv sin privatnøgle, enten på dedikeret USB hardware eller i en fil på brugerens computer. Løsningerne kaldes almindeligvis NemID medarbejdersignatur som nøglefil og NemID på hardware.

2.2 NemID-klienter

For begge versioner gælder der, at privatnøglen anvendes gennem en såkaldt NemID-klient, værende et hjælpeprogram, der leveres af Nets DanID og afvikles på brugerens enhed (pc eller mobile enheder).

NemID-klienterne, som brugeren anvender til at tilgå sin privatnøgle, hedder henholdsvis: "Klient med OTP" til centralt opbevarede privatnøgler (ref. i teknisk dokumentation: NemID JavaScript-klienten og "Klient uden OTP" til lokalt opbevarede privatnøgler (ref. i teknisk dokumentation: NemID CodeFile-klienten).

For at en bruger kan tilgå en centralt opbevaret privatnøgle, skal vedkommende oplyse tre ting: Et bruger-id, en adgangskode og en engangs-nøgle ("One Time Password = OTP").

> I netbanker er der mulighed for at logge på ved kun at oplyse bruger-id og adgangskode, fx til konto-kik.

2.3 Engangs-nøgler

Brugere kan få engangs-nøgler fra et papkort (kaldet et nøglekort), fra en elektronisk nøgleviser eller via en opringning fra Nets DanID (Interactive Voice Response = IVR-løsning). Eller indirekte via en godkendelse på en nøgle-app.

Der findes altså en række måder at få engangs-nøgler på. I resten af dette dokument bruges nøglekort som eksempel.

2.4 Hvor kan NemID anvendes?

Brugeren kan anvende NemID på både pc og mobile enheder til log-in og signering i netbanker, hos offentlige tjenester som fx skat.dk og sundhed.dk samt hos private tjenesteudbydere. På mobile enheder understøttes centralt opbevarede nøgler generelt og lokalt opbevarede nøgler i virksomheder, der benytter en lokal signaturserver (LSS).

Herudover kan brugeren installere en særlig udvidelsespakke, så NemID også anvendes til fx sikker e-mail. For brugere med centralt opbevarede privatnøgler forudsættes, at der er installeret et udvidelsesprogram, som kan hentes på www.nemid.nu.

2.5 Bestilling og selvbetjening

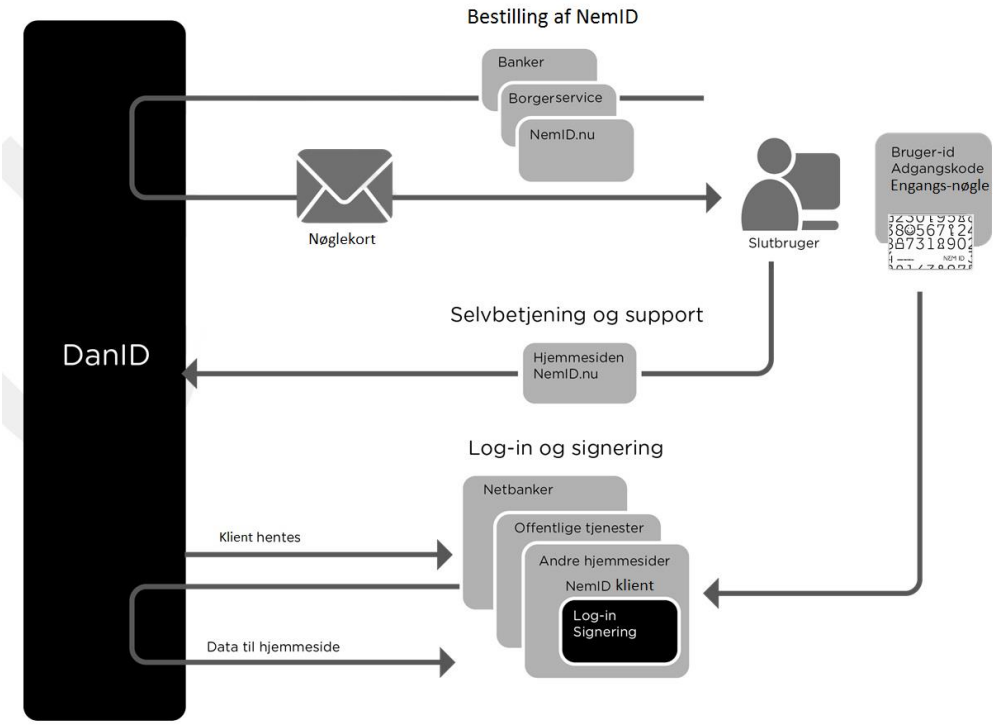
NemID findes til både private (kaldet "NemID til private") og til erhvervsbrug (kaldet "NemID til erhverv").

NemID til private kan bestilles i banken fx i forbindelse med en netbank-aftale eller hos borgerservice. Brugeren kan selv bestille NemID på www.nemid.nu, hvor brugeren også finder NemID selvbetjening.

NemID til private understøtter centralt opbevarede privatnøgler samt privatnøgler opbevaret på hardware.

Ved bestilling af NemID til private sendes et nøglekort med posten. Derudover modtager brugeren en midlertidige adgangskoder, som sendes med posten eller via sms. Nøglekort og/eller midlertidig adgangskode kan endvidere straks udstedes ved henvendelse i bank eller hos borgerservice.

Brugeren kan spærre sit NemID og bestille ekstra nøglekort i NemID selvbetjeningen på www.nemid.nu. Derudover kan de fleste steder, der udsteder NemID, også hjælpe brugeren med at spærre NemID og/eller udlevere ekstra nøglekort.



Figur 1: Delmængde af slutbrugerens muligheder med NemID

NemID til erhverv findes i varianter til brug for medarbejdere, for virksomheder samt for it-systemer hos virksomheder. Løsningen til medarbejdere kaldes også for "NemID medarbejdersignatur". Bestilling og selvbetjening foregår på www.medarbejdersignatur.dk.

NemID til erhverv understøtter centralt opbevarede privatnøgler samt privatnøgler opbevaret på hardware eller i nøglefiler.

2.6 Certifikater

Til en brugers privat-nøgle hører der en offentlig nøgle, der bruges til at validere anvendelser af den tilhørende privat-nøgle. Fx kan en bruger signere et dokument med sin privat-nøgle, og den offentlige nøgle kan efterfølgende anvendes til at validere, at signaturen er korrekt. Offentlige nøgler gøres derfor alment tilgængelige i form af såkaldte certifikater, der er en sammenbinding

af en offentlig nøgle og identitetsinformationer om indehaveren af den tilhørende privat-nøgle.

Til brug for offentlige tjenesteudbydere er der etableret en standard for certifikater kaldet Offentlige Certifikater til Elektroniske Services (OCES). OCES findes i forskellige varianter til privat- og erhvervsbrug:

- OCES til private kaldes for ”POCES” (Privat-OCES)
- OCES til medarbejdere kaldes ”MOCES” (Medarbejder-OCES)
- OCES til virksomheder kaldes ”VOCES” (Virksomheds-OCES)
- OCES til virksomheders it-systemer kaldes ”FOCES”, (Funktions-OCES).

Banker bruger deres egen standard for certifikater, mens øvrige tjenesteudbydere accepterer certifikater efter en eller flere af OCES-standarderne.

3 Om NemID tjenesteudbyderpakken

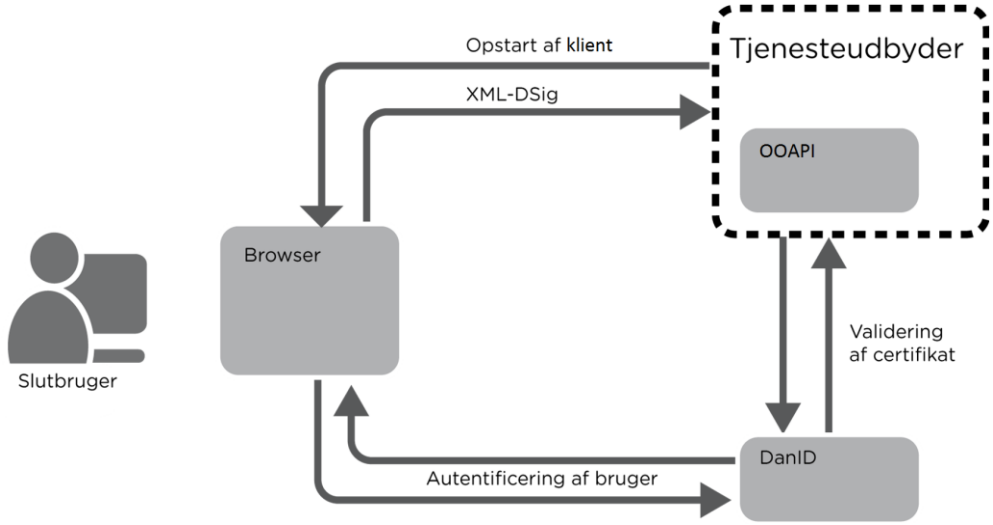
NemID tjenesteudbyderpakken indeholder den nødvendige dokumentation og kodeeksempler, som NemID tjenesteudbyderen kan bruge til at teste og implementere NemID på sin hjemmeside.

NemID tjenesteudbyderen kan danne sig et overblik over og vejledning i de faser, den enkelte tjenesteudbyder skal igennem for at implementere NemID til private og NemID til erhverv.

3.1 Brug af OOAPI

Ved implementering af NemID anbefales det, at tjenesteudbyderen tager udgangspunkt i Nets DanID's OOAPI, der er en del af NemID tjenesteudbyderpakken.

OOAPI'et er et softwarebibliotek, der indeholder en lang række funktioner, som dækker de fleste behov for integration, tjenesteudbydere kommer ud for under implementeringen af NemID, herunder hjælpefunktioner til start af klient, håndtering af signaturer og validering af certifikater.



Figur 2: OOAPI'ets rolle

Som vist i figuren ovenfor, sker der følgende, når slutbrugeren vil logge ind på tjenesteudbyderens side:

1. En slutbruger kontakter en tjenesteudbyder
2. Tjenesteudbyderen initierer opstart af klienten
3. Slutbrugeren bliver autentificeret af Nets DanID
4. Der kommer svar til tjenesteudbyderen
5. Tjenesteudbyderen validerer certifikatet
6. Brugeren er nu autentificeret

Såfremt en tjenesteudbyder ønsker at videreføre sin nuværende specialtilpassede løsning eller benytter sig af funktioner, som OOAPI'et ikke dækker, henvises til dokumenterne i NemID tjenesteudbyderpakken under Referencedokumenter for oplysninger om direkte integration til infrastrukturen.

3.2 De fire faser ved implementering

Implementering af NemID involverer følgende 4 faser:

Guide: Bestil NemID tjenesteudbyder, nets.eu/tu-bestil

3.3 Indgåelse af NemID tjenesteudbyderaftale

For at blive NemID tjenesteudbyder skal der indgås en NemID tjenesteudbyderaftale med Nets DanID, der beskriver de gældende vilkår for tjenesteudbydere.

NemID tjenesteudbyderaftalen indeholder to dokumenter: Standardvilkår for modtagelse af OCES-certifikater fra Nets DanID og Generelle handelsbetingelser.

3.4 Særligt for offentlige tjenesteudbydere

Offentlige tjenesteudbydere, som overvejer at benytte NemID, har to muligheder for integration:

- Integration via NemLog-in eller Virk.dk. Der henvises til tilslutningsguiden for NemLog-in på www.skat.dk og for virk.dk på www.virk.dk
- Integration direkte i egne løsninger.

I begge tilfælde skal offentlige tjenesteudbydere indgå en NemID tjenesteudbyderaftale med Nets DanID.

4 Implementering hos tjenesteudbyderen

Når der er indgået en NemID tjenesteudbyderaftale med Nets DanID, kan tjenesteudbyderen begynde at implementere løsningen på sine hjemmesider og i mobile applikationer.

Guide: test og implementering, nets.eu/tu-guide

4.1 Autentificerings- og signeringsmuligheder

Som nævnt i introduktionen er der to forskellige måder, brugerens privatnøgle kan opbevares på: Centralt eller lokalt. Tjenesteudbydere bør derfor som hovedregel præsentere slutbrugere for de to forskellige klienter, så begge muligheder understøttes. De kaldes hhv. NemID JavaScript-klienten og NemID CodeFile-klienten.

4.1.1 NemID JavaScript-klienten (Klient med OTP)

"Klient med OTP", også kaldet NemID JavaScript-klienten, benyttes hvor brugerens privat-nøgle opbevares på en central server hos Nets DanID.

Det gælder for følgende løsninger:

- NemID med nøglekort – hvor brugeren får engangs-nøgler fra et nøglekort eller fra et nøgle-ark med stor skrift.
- NemID med nøgleviser – hvor brugeren får engangs-nøgler fra en elektronisk enhed.
- NemID med IVR – hvor brugeren får engangs-nøgler via telefonopkald fra Nets DanID.
- NemID med nøgleapp – hvor brugeren godkender via en nøgleapp installeret på en mobil enhed.

Generelt omfatter løsningen NemID med nøglekort, at klienten kontakter Nets DanID's nøgleserver med henblik på autentificering og signering. Både NemID til private og NemID til erhverv vil kunne benytte denne løsning.

NemID JavaScript-klienten kan afvikles i de fleste browsere og kræver ikke plug-ins på slutbrugerens platform. Klienten kan derfor anvendes på de fleste mobile enheder.

4.1.2 NemID CodeFile-klienten (Klient uden OTP)

"Klient uden OTP", også kaldet NemID CodeFile-klienten, benyttes hvor brugerens privat-nøgle opbevares lokalt.

Det gælder for følgende løsninger:

- NemID medarbejdersignatur som nøglefil – hvor brugeren privat-nøgle hørende til MOCES-, VOCES- eller FOCES-certifikater opbevares i en fil på brugerens pc.
- NemID på hardware – hvor brugerens privat-nøgle hørende til POCES- eller MOCES-certifikater opbevares på hardware.

NemID CodeFile-klienten kan afvikles i browsere, som understøtter de nødvendige plug-ins (Java eller NemID nøglefilsprogram), der skal være installeret på slutbrugerens pc for at kunne tilgå den lokalt opbevarede privatnøgle. Dette udelukker brug på mobile enheder.

I virksomheder, der derimod benytter en lokal signaturserver (LSS), vil brugere med en NemID medarbejdersignatur som nøglefil kunne afvikle NemID CodeFile-klienten i de fleste browsere, både på pc og mobile enheder.

4.1.3 Aktivering af klienter

Brugeren skal på tjenesteudbyderens hjemmeside vælge log-in-metode.

Tjenesteudbyderen skal præsentere de relevante valg for brugeren og sørge for, at den rigtige klient startes fx "Login med nøglekort" eller "Login med nøglefil".

Tjenesteudbyderen kan i de visuelle guidelines i tjenesteudbyderpakken finde anbefalinger og råd til integration af NemID.

4.2 Implementeringens omfang

Nets DanID vurderer, at det vil tage en tjenesteudbyder en til fire uger at implementere NemID. Det anslåede tidsestimat er afhængig af den eksisterende løsningstype hos tjenesteudbyderen og dækker kun den tekniske implementering.

5 Opstart af klient

Som beskrevet i Afsnit 4 **Implementering hos tjenesteudbyderen**, bør tjenesteudbyderen præsentere brugeren for et valg mellem to log-in-metoder. Herefter skal tjenesteudbyderen starte enten NemID JavaScript-klienten eller NemID CodeFile-klienten.

I begge tilfælde gælder, at klienten er placeret på en server hos Nets DanID og skal overføres fra denne server.

5.1 Opstart/opsætning af NemID JavaScript-klienten

For at starte NemID JavaScript-klienten skal tjenesteudbyderen åbne en webside med en iframe, der peger på en bestemt URL på Nets DanID's server.

Med til iframen sendes en række parametre, der styrer klientens udseende og opførsel. Sammen med parametrene sendes en hash-værdi (SHA-256) af parametrene på en normaliseret form samt en signatur af hash-værdien lavet med tjenesteudbyderens privat-nøgle hørende til et VOCES- eller FOCES-certifikat.

Tjenesteudbyderpakken indeholder følgende elementer, der kan hjælpe tjenesteudbydere med at få løsningen sat op:

- Java- og .Net-referencekode til generering og signering af hashværdi af normaliseret parameterliste.
- Eksempler på hvordan denne Java- og .Net-kode kan inkluderes i en tjenesteudbyders webside.
- Beskrivelse af Java- og .Net-koden.
- Implementeringsvejledning til NemID, hvori de tekniske detaljer om integration af NemID beskrives.

5.2 Opstart/opsætning af NemID CodeFile-klienten

Opsætning af NemID CodeFile-klienten svarer til opsætningen af NemID JavaScript-klienten (se Afsnit 5.1).

5.3 Visuel implementering (opsætning)

Nets DanID har udarbejdet en række visuelle guidelines, der beskriver, hvordan NemID kan præsenteres for brugeren.

NemID tjenesteudbyderpakken indeholder løsningsbeskrivelse og visuelle guidelines for log-in og signering med NemID.

5.4 Klient-interaktion med Nets DanID

Efter klienten er startet hos brugeren, foregår der en autentificering af brugeren gennem klienten. I denne sammenhæng kontakter NemID JavaScript-klienten Nets DanID's server med de centralt opbevarede privat-nøgler, mens NemID CodeFile-klienten tilgår de lokalt opbevarede privat-nøgler.

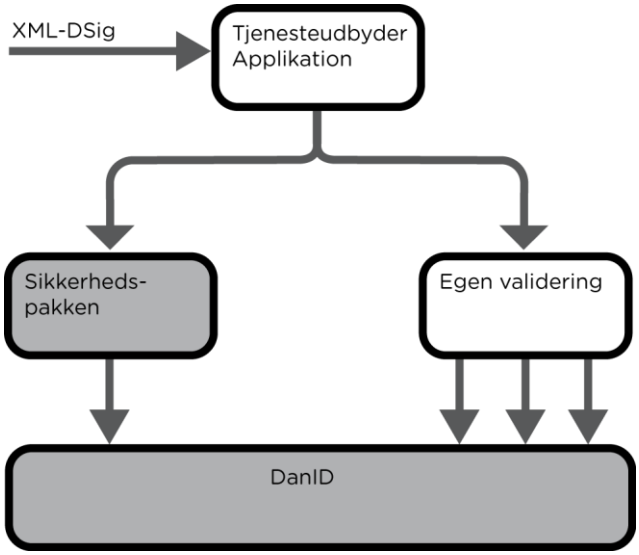
Når brugerautentificeringen er vellykket, sender klienten et XML-DSig-respons til tjenesteudbyderens webserver indeholdende brugerens signatur.

Herefter skal tjenesteudbyderen validere brugerens signatur og certifikat. Se Afsnit 6 **Validering af certifikat**.

6 Validering af certifikat

Uanset om brugeren har valgt at bruge NemID med nøglekort, NemID medarbejdersignatur som nøglefil eller NemID på hardware, er opgaven med at validere certifikatet den samme.

Der er som udgangspunkt to forskellige måder at lave denne validering på. Tjenesteudbyderen kan enten benytte OOAPI'et fra Nets DanID eller selv udvikle sit eget valideringsmodul og tilgå komponenter i infrastrukturen som spærrelister (CRL) og PID/RID cpr-tjenester direkte.



Figur 3: Validering af certifikat

6.1 OOAPI fra Nets DanID

Hvis tjenesteudbyderen vælger at anvende OOAPI'et fra Nets DanID, skal tjenesteudbyderen kalde en funktion med svaret fra autentificeringen. Funktionen svarer tilbage med et PID/RID-nummer, hvis autentificeringen var succesfuld. Hvis ikke, svares med en fejlkode.

Der stilles fuld Java- og .Net-dokumentation til OOAPI tilgængeligt samt komplet reference kode i Java og .Net.

Find mere information i specifikationsdokumenterne for PID/RID cpr-tjenester i NemID tjenesteudbyderpakken.

6.2 *Direkte infrastruktur*

For tjenesteudbydere, der ikke ønsker at gøre brug af Nets DanID's OOAPI, er der mulighed for at udvikle en helt egen løsning og tilgå de enkelte komponenter i infrastruktur direkte.

NemID tjenesteudbyderpakken indeholder specifikationer af, hvordan hver enkelt af nedenstående komponenter i infrastrukturen kan tilgås direkte:

1. PID cpr-tjenesten
2. RID cpr-tjenesten
3. OCSP-responder
4. Fuld spærreliste tilgængelig via LDAP
5. Fuld spærreliste tilgængelig via https
6. Partielle spærrelister tilgængelige via LDAP

Der henvises til NemID tjenesteudbyderpakken under Værktøjer og referencedokumenter.

7 Testmiljø

Nets DanID stiller testmiljø tilgængeligt for alle NemID tjenesteudbydere til udvikling og test.

Desuden har Nets DanID udviklet nogle hjælpeværktøjer (kaldet "Developer site"), der kan benyttes til at teste og verificere opbygningen af inputparametre og signaturstrenge til NemID JavaScript-klienten.

Adgang til testmiljøet og Developer site oprettes i forbindelse med indgåelse af NemID tjenesteudbyderaftalen.

For at få adgang til Developer site og testmiljø skal der åbnes for tjenesteudbyderens IP-adresser to forskellige steder: Developer site og Pre Production (PP).

8 Support

Hjælp og vejledning findes på nets.dk under Kundeservice og NemID tjenesteudbyder.

Derudover kan Nets DanID hjælpe med implementering, udvikling og opsætning af NemID i jeres løsning.

For support henvender NemID tjenesteudbydersupport sig via formularen på nets.dk, nets.eu/tu-support.

Ændringer og nødvendige tilpasninger i tjenesteudbyders eget miljø skal varetages af tjenesteudbyders egne ressourcer.

Nets DanID tilbyder to servicepakker; én til når du implementerer NemID i din løsning, og én til når du tilpasser og vedligeholder din NemID-løsning. Find yderligere information på nets.eu/nemid-servicepakker