Nets DanID A/S
Lautrupbjerg 10
DK – 2750 Ballerup

T +45 87 42 45 00
F +45 70 20 66 29
info@danid.dk
www.nets-danid.dk

CVR-nr. 30808460

Introduktion til NemID og Tjenesteudbyderpakken

Indholdsfortegnelse

Versionsfortegnelse

4. maj 2009	Version 1.0	MOBO
11. maj 2009	Version 1.1	MOBO
1. oktober 2009	Version 1.2	MOBO
4. december 2009	Version 1.3	MOBO
24. februar 2010	Version 1.4	MOBO
12. marts 2010	Version 1.5	MTV
15. april 2010	Version 1.6	MTV
20. april 2010	Version 1.7	MOBO
8. juni 2010	Version 1.8	MTV
29. oktober 2010	Version 1.9	MTV
15. juni 2011	Version 2.0	JV
25. oktober 2011	Version 2.1	MTVOL
12. oktober 2012	Version 2.2	MTVOL

1 Dokumentets formål og målgruppe

Dette dokument er en del af Tjenesteudbyderpakken for NemID.

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

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

Oversigt over alle dokumenter i Tjenesteudbyderpakken:

Overordnet dokumentation

- **Introduktion til NemID og Tjenesteudbyderpakken**
- Anbefalinger til interaktionsdesign og brugervalg af applet
- Drejebog for migrering til NemID
- Termer og begreber i NemID

Implementeringsdokumentation

- Implementeringsvejledning for NemID
- Konfiguration og opsætning

Testdokumentation

- Vejledning i brug af test tools
- Anbefalede testprocedurer

Referencedokumentation

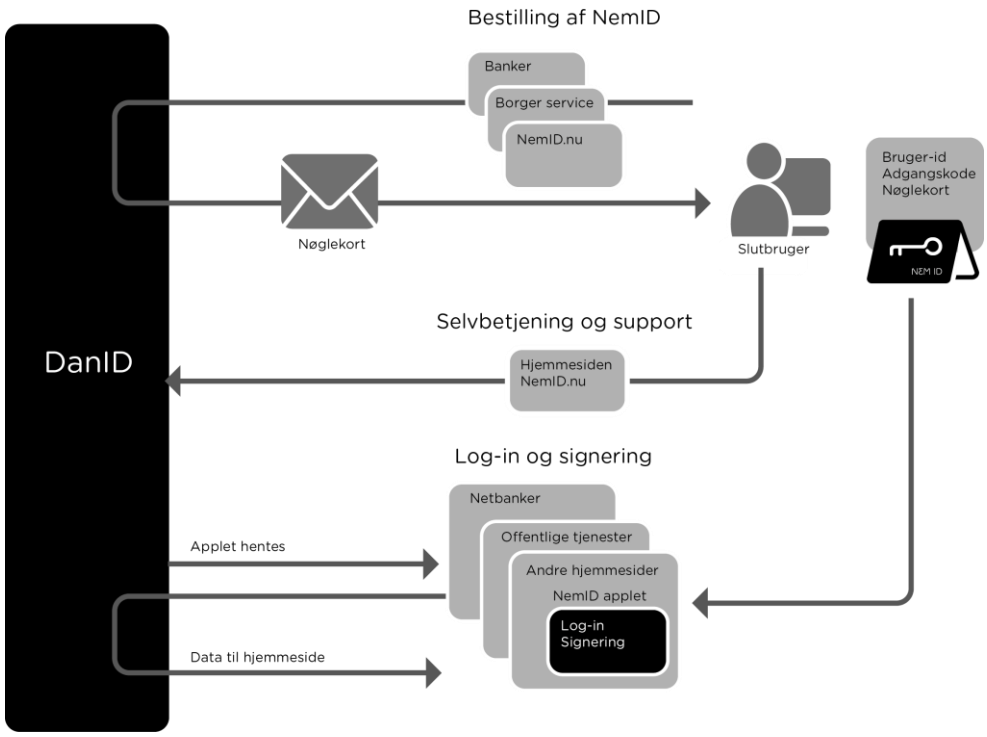
- Specifikationsdokument for servicen PID-CPR
- Specifikationsdokument for servicen RID-CPR
- Specifikationsdokument for LDAP API
- Specifikationsdokument for OCSP
- Specifikationsdokument for OCES II

2 Intro til NemID

NemID er danskernes digitale signatur til log-in og signering på internettet. NemID til Borger så dagens lys d. 1. juli 2010 og er baseret på at brugeren har et bruger-id, en adgangskode og et nøglekort fra Nets DanID. Når disse bruges sammen med appletten fra Nets DanID gives adgang til brugerens centralt opbevarede nøgler – brugerens NemID. NemID findes også som den decentral løsning; NemID på hardware

> Der henvises til dokumentet **Termer og begreber i NemID** for en forklaring af de termer og begreber der anvendes i dette dokument og i Tjenesteudbyderpakken generelt.

Brugeren kan anvende NemID til log-in og signering i netbanken, hos offentlige tjenester som f.eks. skat.dk og sundhed.dk, samt hos private tjenesteudbydere. Herudover kan brugeren installere en særlig udvidelsespakke, så NemID også kan anvendes til f.eks. sikker e-mail. "Sikker E-mail"-softwaren kan hentes på www.nemid.nu.



Figur 1: Slutbrugerens muligheder med NemID til Borger

Der findes en lang række forskellige steder en bruger kan få NemID til Borgere; i banken i forbindelse med en netbank-aftale, hos borgerservice eller i et skattecenter og endelig kan brugeren selv bestille NemID på www.nemid.nu.

Nøglekort og midlertidige adgangskoder bliver sendt med posten eller udleveres med det samme, hvis man henvender sig i sin bank, hos borgerservice eller i et skattecenter.

De steder der udsteder NemID kan også hjælpe brugeren med at spærre certifikater eller udlevere ekstra nøglekort. Brugeren kan også bruge Nets DanIDs selvbetjeningsside, www.nemid.nu, eller henvende sig til NemID telefonsupport.

2.1 Særligt for NemID til Erhverv

NemID til Erhverv bliver afløseren for den eksisterende OCES I løsning for Medarbejdersignaturer. Bestilling og vedligehold af medarbejdercertifikater vil foregå via et selvbetjeningsunivers på www.nets-danid.dk, og det vil både være muligt at udstede software certifikater såvel som certifikater med nøglekort (OTP). På sigt vil der også være mulighed for at få medarbejdercertifikater på hardware (fx chipkort eller e-token).

3 Om NemID og Tjenesteudbyderpakken

Med NemID introduceres et sikkert identificeringsværktøj og log-in/signeringsmulighed på internettet, hvor brugeren i langt de fleste tilfælde kan anvende den samme løsning til at få adgang til sin netbank og til en lang række offentlige og private tjenesteudbydere.

Tjenesteudbyderpakken er en samling dokumenter og software-elementer, der giver eksisterende og nye tjenesteudbydere et overblik over og vejledning i de opgaver, den enkelte tjenesteudbyder skal igennem for at:

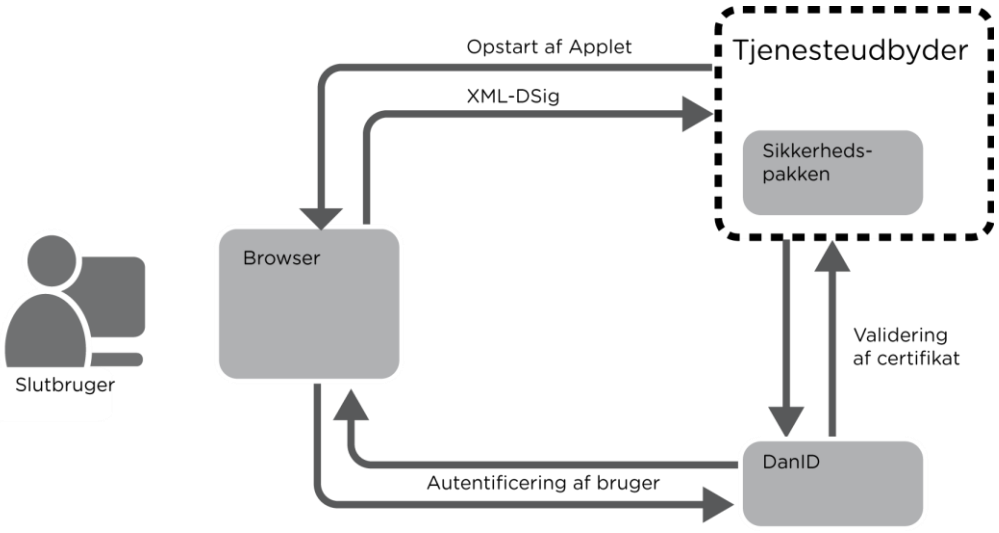
1. *migrere* fra den eksisterende Digital Signatur til NemID til Borger og Erhverv

2. *implementere* NemID til Borger og Erhverv.

Tjenesteudbyderpakken er sammensat, så der så vidt muligt tages højde for de forskellige implementeringsbehov, der måtte være hos forskellige typer tjenesteudbydere.

3.1 Nets DanIDs anbefalinger

Ved valg af implementeringsmetode af NemID anbefales det, at I tager udgangspunkt i Nets DanIDs OOAPI (også kaldet OpenOCES API eller Sikkerhedspakken). OOAPI'et dækker de fleste integrationsmuligheder.



Figur 2: OOAPI'ets (Sikkerhedspakkens) 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 applet
3. Slutbrugeren bliver autentificeret af Nets DanID
4. Der kommer svar til Tjenesteudbyderen
5. Bruger er nu autentificeret korrekt (validering af certifikat)

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

3.2 De fire faser ved implementering

Implementering af NemID involverer følgende 4 faser:

1. Indgåelse af tjenesteudbyderaftale med Nets DanID, således at begge parter er bekendt og indforstået med de vilkår og forpligtigelser, der gælder for NemID. Aftaleindgåelse sker ved at underskrive en Tjenesteudbyderaftale, som kan rekvireres hos Nets DanID Salg på salg@danid.dk eller downloades på www.nets-danid.dk/produkter/for_tjenesteudbydere/nemid_tjenesteudbyder/bestil_nemid_tjenesteudbyder.

2. Efter aftaleindgåelse følges den trinvise vejledning på www.nets-danid.dk/tu-support til implementering og test. Der kan findes uddybende vejledninger på www.nets-danid.dk/tu-doc. Under denne proces testes de udviklede komponenter/funktioner lokalt i eget miljø hos tjenesteudbyderen bl.a. ved hjælp af Nets DanID's testfaciliteter, som primært dækker de fejlsituationer, der kan opstå i kommunikationen med slutbrugeren.

3. Efter implementering og integration på portal/hjemmeside testes systemkaldene fra serversiden til Nets DanID's infrastruktur. Dette forudsætter, at man er oprettet som tjenesteudbyder i Nets DanID's testmiljø, herunder at man har et test-VOCES certifikat (Nets DanID kan gratis bestille et til jer). Der opnås adgang til testsystemet ved at udfylde formularen på https://www.nets-danid.dk/produkter/for_tjenesteudbydere/nemid_tjenesteudbyder/nemid_tjenesteudbyder_support/adgang_til_testsystem og man kan få adgang til testmiljøet, allerede inden man har besluttet, om man ønsker at indgå aftale med Nets DanID.

4. Efter endt test sættes jeres løsning i produktion. Dette sker bl.a. ved at anvende et produktions-VOCES certifikat, og ved at anmode om adgang til produktionssystemet via online formularen på https://www.nets-danid.dk/produkter/for_tjenesteudbydere/nemid_tjenesteudbyder/nemid_tjenesteudbyder_support/adgang_til_produktionssystem.

Sådan kommer I i gang:

På www.nets-danid.dk/tu-support har vi oprettet en trinvis guide og vejledning, som fører jer sikkert igennem alle faser fra indgåelse af aftale, test og implementering til produktion.

3.3 Særligt for offentlige tjenesteudbydere

Offentlige tjenesteudbydere, som er tilsluttet den fællesoffentlige single sign-on løsning NemLog-in eller Virk.dk, skal ikke selv søge for, at der migreres til NemID. Migreringen håndteres af NemLog-in eller Virk.dk for alle tilsluttede løsninger.

Øvrige offentlige tjenesteudbydere, som overvejer at benytte NemID, har to muligheder for tilslutning:

- Tilslutning via NemLog-in eller Virk.dk. Der henvises til tilslutningsvejledningen for NemLog-in på www.skat.dk/nemlog-in og for virk.dk på www.virk.dk

- Tilslutning direkte i forhold til Nets DanID som beskrevet i Tjenesteudbyderpakken.

3.4 Særligt for private tjenesteudbydere

3.4.1 For nye tjenesteudbydere

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

Tjenesteudbyderaftale kan rekvireres ved henvendelse til Nets DanID på salg@danid.dk eller kan hentes på www.nets-danid.dk/tu.

3.4.2 For eksisterende tjenesteudbydere

For tjenesteudbydere, som har implementeret understøttelse af OCES I Digital Signatur eller net-ID, skal den eksisterende aftale erstattes af en ny Tjenesteudbyderaftale med Nets DanID.

Denne nye aftale regulerer overgangen fra den gamle til den nye løsning, således at understøttelse af begge løsninger er mulig i en overgangsperiode.

I dokumentet **Drejebog for migreringen** kan du læse mere om de forskellige muligheder.

4 Implementering hos tjenesteudbyderen

Når der er indgået en Tjenesteudbyderaftale med Nets DanID kan I som tjenesteudbydere begynde at implementere løsningen på jeres hjemmeside.

Tjenesteudbyderaftale kan rekvireres ved henvendelse til Nets DanID Salg på salg@danid.dk eller kan hentes på www.nets-danid.dk/tu.

4.1 Autentificering og signeringsmuligheder

Tjenesteudbydere skal præsentere slutbrugeren for to forskellige log-in muligheder (applets) på deres hjemmeside. Det skyldes, at der er to forskellige måder, brugerens private nøgle kan opbevares på: *Lokalt* eller *centralt*.

De to applets kaldes hhv. *Applet uden OTP* og *Applet med OTP*.

4.1.1 Applet uden OTP

Applet uden OTP benyttes, hvor brugerens private nøgle opbevares lokalt.

Det gælder for følgende løsninger:

- Den gamle Digital Signatur (OCES I) løsning, hvor brugerens private nøgle opbevares i en nøglefil på brugerens pc, og den offentlige nøgle opbevares i et OCES I-certifikat. Denne løsning udfases i takt med, at udstedte certifikater udløber, men løsningen skal dog understøttes i en overgangsperiode.

- NemID til Borger (OCES II personcertifikater) - hvor brugerens private nøgle opbevares på hardware.

- NemID til Erhverv (OCES II medarbejdercertifikater) - hvor brugerens private nøgle opbevares på en chip (f.eks. chipkort/USB-token). Ved lanceringen af NemID til erhverv vil medarbejdercertifikater kunne udstedes som softwarecertifikater svarende til den nuværende OCES I-løsning.

Generelt omfatter Applet uden OTP alle nuværende OCES I og fremtidige løsninger OCES II, hvor autentificering og signering, kan ske direkte på brugerens pc. Denne applet vil være en videreførelse af den allerede eksisterende OpenOCES-applet.

4.1.2 Applet med OTP

Applet med OTP benyttes, hvor brugerens private nøgle opbevares på en central server hos Nets DanID:

- Generelt omfatter Applet med OTP alle nuværende og fremtidige løsninger, hvor appletten kontakter Nets DanIDs nøgleserver med henblik på autentificering og signering. Både NemID til Borger og NemID til Erhverv vil kunne benytte denne, såfremt der er tilknyttet et nøglekort (OTP device).

4.1.3 Aktivering af appletter

Brugeren skal på tjenesteudbyderens hjemmeside vælge, hvilken af de to log-in mekanismer (Applet uden OTP eller Applet med OTP) der skal benyttes. Tjenesteudbyderen skal på sin webside præsentere de relevante valg for brugeren og sørge for, at den rigtige applet startes. Der er til dette formål udviklet et anbefalet interaktionsdesign, som er at finde i tjenesteudbyderpakken.

I dokumentet **Vejledning til interaktionsdesign og brugervalg af applet** kan du læse mere om, hvordan dette valg kan præsenteres og hvilke elementer I bør anvende for at vejlede brugeren bedst muligt.

For en nærmere beskrivelse af, hvordan I skal interface til de to appletter, henvises til Afsnit 6 **Opstart af applet** og Afsnit 7 **Validering af certifikat**.

Desuden henvises til dokumenterne på www.nets-danid.dk/tu-doc under overskriften **Implementeringsdokumentation**.

4.2 Implementeringens omfang

Følgende tabel udtrykker Nets DanIDs vurdering af den tid, det vil tage en tjenesteudbyder, at integrere NemID afhængigt af eksisterende løsningstype.

Det anslåede ressourceforbrug dækker kun den tekniske implementering, dvs. uden de indledende aftaledrøftelser, test, osv.

Tabellen kan aflæses ved, at I tager udgangspunkt i jeres eksisterende løsning og derefter finder den løsningsmodel, I ønsker at integrere til. Bemærk, at offentlige tjenesteudbydere, der allerede er tilsluttet den fælles-offentlige SSO eller NemLog-in, automatisk vil blive integreret.

Nuværende løsning **Ny løsning**	Ingen nuværende løsning	Klientautentificeret SSL-løsning	Egen OpenOCES-baseret løsning
Klientautentificeret SSL-løsning	1 – 4 uger	1 uge	1 – 4 uger
OOAPI fra Nets DanID	1 – 4 uger	1 - 4 uger	1 – 4 uger
Egen OpenOCES-baseret løsning hos Tjeneste-udbyder	1 – 4 måneder	1 – 4 måneder	1 – 4 uger
Den fællesoffentlige SSO	1 – 4 uger	1 – 4 uger	1 – 4 uger

5 Migreringsspecifikke hensyn

I det følgende præsenteres de overordnede migreringsspecifikke hensyn, I bør foretage, i forbindelse med implementering af NemID.

5.1 OpenOCES-apletten fortsætter

Nets DanID understøtter i en overgangsperiode den nuværende Digital Signatur (OCES I) løsning.

Efter d. 1. juli 2010 udstedes ikke nye Digital Signatur (OCES I) *person*certifikater. Fra denne dato og frem udstedes der for private borgere kun NemID (OCES II *person*certifikater). Nets DanID vedligeholder dog spærrelister, modtager spærringsanmodninger m.v. af Digital Signatur (OCES I) certifikater, indtil det sidst udstedte certifikat er udløbet.

Efter lanceringen af NemID til Erhverv udstedes der efter en endnu ikke fastlagt migreringsperiode ikke længere OCES I Medarbejdercertifikater. Nets DanID vedligeholder dog spærrelister, modtager spærringsanmodninger m.v. af OCES I certifikater, indtil det sidst udstedte certifikat er udløbet.

5.2 SSL-klientautentifikation

Tjenesteudbydere der har implementeret log-in på baggrund af SSL-klientautentifikation kan fortsat gøre dette med NemID. Det forudsætter, at den bruger, der skal autentificeres, har installeret et stykke særligt software fra Nets DanID kaldet "Sikker E-mail" (da det også er det komponent der bruges til netop sikker e-mail). Softwaren ligger frit tilgængelig for download på www.nemid.nu.

Vær opmærksom på, at det på nuværende tidspunkt forventes, at kun et meget begrænset antal brugere vil installere "Sikker E-mail"-softwaren. Nets DanID anbefaler derfor, at tjenesteudbyderen overgår til en applet-løsning med integration via OOAPI'et, eller for offentlige tjenesteudbydere, at anvende den fælles offentlige SSO-løsning (NemLog-in).

Hvis tjenesteudbyderen fortsat vælger at benytte SSL-klientautentifikation, skal tjenesteudbyderen sikre at brugerne informeres om behovet for installation af "Sikker E-mail"-softwaren.

6 Opstart af applet

Som beskrevet i Afsnit 4 **Implementering hos tjenesteudbyderen**, skal I præsentere brugeren for et valg mellem to log-in metoder. Herefter skal I starte enten Applet med OTP eller Applet uden OTP.

For NemID til Borger gælder det at Applet med OTP placeres på en server hos Nets DanID og overføres fra denne server, mens Applet uden OTP placeres hos jer og overføres derfra.

For NemID til Erhverv gælder det at både Applet med OTP og Applet uden OTP placeres på en server hos Nets DanID og overføres fra denne server (loades runtime).

Læs mere om opsætning af de to appletter i dokumentet **Implementeringsvejledning** under **Implementeringsdokumentation**.

6.1 Opstart/opsætning af Applet uden OTP

Den nuværende Applet uden OTP er beskrevet i detaljer på OpenOCES.org og her kan man finde alt relevant implementeringsdokumentation.

6.2 Opstart/opsætning af Applet med OTP

For at starte denne applet, skal tjenesteudbyderen generere en webside med et applet-tag indeholdende en normaliseret parameterliste.

Efter normaliseringen beregnes den normaliserede strengs SHA-256 hash-værdi, og resultatet heraf signeres med tjenesteudbyderens VOCES-certifikat. Både strengens hash-værdi og signatur sendes til appletten som parametre.

Såfremt tjenesteudbyderen ikke allerede har et VOCES-certifikat, der ønskes anvendt, vil Nets DanID gratis stille et VOCES-certifikat til rådighed, når tjenesteudbyderen har indgået aftale med Nets DanID.

Tjenesteudbyderpakken indeholder bl.a. følgende elementer der kan hjælpe tjenesteudbydere med at få løsningen sat op:

- Java og .Net-referencekode til generering af applet-tags og signering af parametrene.
- Eksempler på hvordan denne Java og .Net-kode kan inkluderes i en tjenesteudbyders webside.

- Beskrivelse af Java og .Net-koden.

6.3 Visuel implementering (opsætning)

Nets DanID har bl.a. i samarbejde med IT og Telestyrelsen udarbejdet et *interaktionsdesign*, som er en anbefaling til, hvordan de to log-in appletter skal præsenteres for brugeren.

> For en nærmere beskrivelse af denne anbefaling henvises til dokumentet **Vejledning til brugervalg af applet** under overskriften **Overordnet dokumentation på www.nets-danid.dk**/tu-doc

6.3.1 Applet uden OTP

Appletten uden OTP ser således ud:

Figur 3: Applet uden OTP

Applet uden OTP kan både være NemID uden engangsnøgle (NemID Erhverv softwarecertifikater eller NemID på hardware) samt Digital Signatur. Denne applet vil således understøtte både Digital Signatur, NemID på hardware og NemID Erhverv med lokalt lagrede certifikater.

6.3.2 Applet med OTP

Applet med OTP ser således ud:

Figur 4: Applet med OTP

I applet med OTP logger brugeren på med bruger-id og adgangskode, hvorefter systemet anmoder brugeren om en nøgle fra dennes nøglekort eller nøgleviser (OTP device).

6.4 Applet-interaktion med Nets DanID

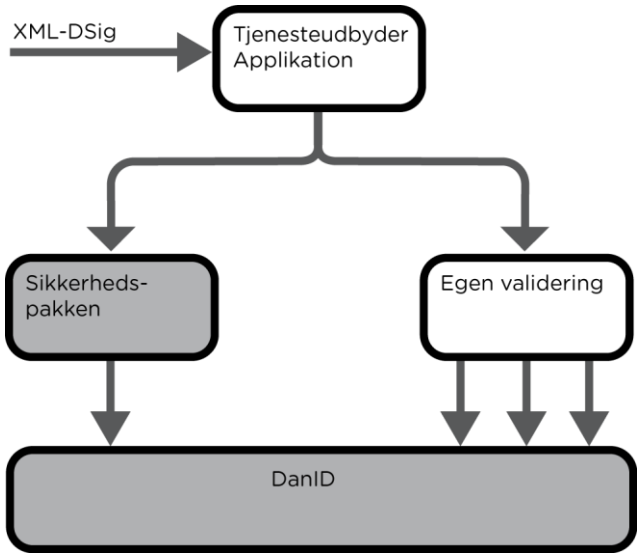
Efter appletten er startet hos brugeren, foregår der en autentifikation af denne, som varierer i forhold til, hvilken applet der kører, og hvilken digital signatur-løsning brugeren har. OTP-appletten kommunikerer i den forbindelse med Nets DanIDs bagvedliggende infrastruktur.

Når brugerautentificeringen er vellykket, sender appletten via http POST et XMLDSig-respons til tjenesteudbyderens webserver indeholdende brugerens signatur.

Herefter skal tjenesteudbyderen validere brugerens signatur og certifikatet. Se Afsnit 7 **Validering af certifikat**.

7 Validering af certifikat

Uanset om brugeren har valgt at bruge Applet med eller uden OTP, så er opgaven med at validere certifikatet den samme. Der er som udgangspunkt to forskellige måder, man kan lave denne validering på. Man kan enten benytte OOAPI'et (Sikkerhedspakken) fra Nets DanID eller selv udvikle sit eget valideringsmodul og tilgå infrastruktur-komponenter som spærrelister (CRL) og PID-tjeneste direkte.



Figur 5: Validering af certifikat

7.1 OOAPI fra Nets DanID

Hvis I vælger at anvende OOAPI'et (Sikkerhedspakken) fra Nets DanID, skal man kun ekstrahere XMLDSig svaret til webserveren, og herefter kalde en Java-funktion, der så svarer tilbage med et PID/RID-nummer, hvis certifikatet er gyldigt. Hvis certifikatet er ugyldigt, svares med en fejlkode.

I behøver ikke bekymre jer om hvorvidt det er et Digital Signatur- (OCES I) eller NemID certifikat (OCES II) og dermed holde styr på, hvilke spærrelister, der skal anvendes.

Hvis I selv ønsker at konstruere valideringen skal tjenesteudbyderen selv foretage de enkelte skridt i valideringen ved at anvende forskellige metodekald til at konstruere valideringen.

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

7.2 Direkte infrastruktur

For tjenesteudbydere, der ikke ønsker at gøre brug af Nets DanIDs OOAPI, er der mulighed for, at udvikle sin helt egen løsning og tilgå de enkelte infrastrukturkomponenter direkte.

Tjenesteudbyderpakken indeholder specifikationer af, hvordan hver enkelt af nedenstående infrastrukturkomponenter kan tilgås direkte:

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

Der henvises til dokumenterne på www.nets-danid.dk/tu-doc under overskriften **Referencedokumentation**.

Læs også afsnit **3.1 Nets DanIDs anbefalinger** tidligere i dette dokument.

8 Testmiljø

Nets DanID stiller testmiljø tilgængeligt for alle nuværende og kommende tjenesteudbydere til udvikling og test. Testmiljøet ligger på en platform, der svarer til produktionsmiljøet.

For at få adgang til testmiljøet skal tjenesteudbyderen udfylde online formularen "Adgang til testsystem", som findes på https://www.nets-danid.dk/produkter/for_tjenesteudbydere/nemid_tjenesteudbyder/nemid_tjenesteudbyder_support/adgang_til_testsystem. Når I har udfyldt og indsendt formularen vender vi tilbage med henblik på hvordan I selv opretter testbrugere, m.m.

Der henvises endvidere til guiden på www.nets-danid.dk/tu

9 Support

Der kan findes hjælp og vejledning til hele forløbet i den trinvise guide på www.nets-danid.dk/tu-support.

Nets DanID yder desuden support til tjenesteudbydere i testforløbet på følgende områder:

- Info om Nets DanID-dokumentation
- Info om brug af sikkerhedsmoduler og grænseflader
- Info om brug af de nødvendige certifikater

Support skal ske ved henvendelse til tu-support@danid.dk.

Nye tjenesteudbydere: 2 timers support uden beregning.

Eksisterende tjenesteudbydere: 4 timers support uden beregning.

Er der behov for yderligere support, kan det efter aftale ydes til gældende timepris.

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

Hvis I ønsker support til integrationen med egne forretningssystemer, kan Nets DanID henvise til vores partnere, som bistår med hjælp og vejledning til denne opgave. Der er udviklet et certificeringsprogram, der sikrer et højt kvalitetsniveau for den rådgivning, som tilbydes af partnere. Kontakt TU-support på tu-support@danid.dk hvis I ønsker henvisning til vores partnere.