DIGITALISERINGSSTYRELSEN

Brokere i Identitetsinfrastrukturen

13. september 2018

Introduktion

Dette notat beskriver forhold vedr. identitetsbrokere i den kommende, nationale identitets-infrastruktur bestående af MitID og NemLog-in3. Notatet retter sig mod organisationer, der overvejer at indtræde i brokerrollen, og beskriver de tekniske, økonomiske og juridiske rammer for brokere.

Ved en *identitetsbroker* menes i dette notat en on-line tjeneste, som formidler en autentificeret digital identitet til en tjenesteudbyder (forretningstjeneste). Som eksempel på Identitetsbrokere kan bl.a. nævnes NemLog-in og WAYF løsningerne samt Context Handleren i den fælleskommunale rammearkitektur. For beskrivelse af øvrige begreber på identitetsområdet henvises til terminologiafsnittet i NSIS[1] standarden (National Standard for Identiteters Sikringsniveauer).

Baggrund

Med introduktionen af MitID og NemLog-in3 ændres der væsentligt på den digitale identitetsinfrastruktur, herunder hvorledes tjenesteudbydere kobles op på denne.

En af de væsentligste ændringer er, at tjenesteudbydere ikke vil kunne anvende MitID direkte i modsætning til i dag, hvor en lang række (fortrinsvis) private tjenesteudbydere integrerer direkte med NemID. Tjenesteudbydere skal i stedet kobles på via en såkaldt *broker* (også benævnt *Identitetsbroker* i NSIS[2]), som videreformidler en MitID autentifikation. Herved sker der en afkobling mellem tjenesteudbydere og MitID.

NemLog-in2 er i dag identitetsbroker for offentlige tjenester i forhold til NemID, og fremadrettet vil NemLog-in3 fortsætte som broker for offentlige tjenester i relation til MitID. Af hensyn til at garantere adgangen til den digitale identitetsinfrastruktur for private tjenester, vil NemLog-in3 (i modsætning til NemLog-in2) kunne anvendes af private tjenesteudbydere til basale funktioner som fx autentifikation og signering. Der vil være tale om en begrænset, basal anvendelse af NemLog-in3 for private tjenester, som ikke omfatter muligheden for Single Sign-On, rettighedsstyring eller digitale fuldmagter.

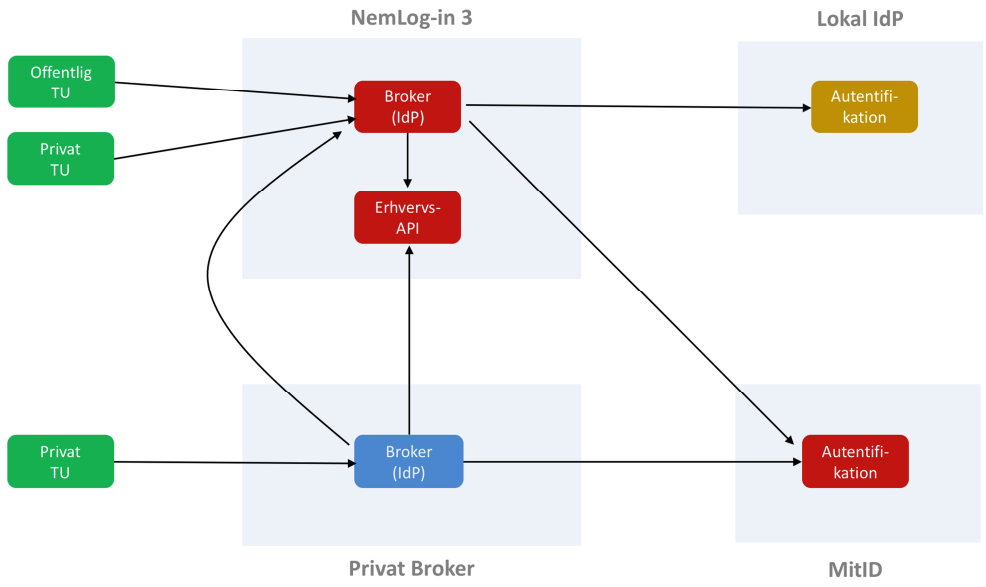
---

[1] https://www.digitaliser.dk/resource/3436586
[2] National Standard for Identiteters Sikringsniveauer

Samtidig ønsker Digitaliseringsstyrelsen, at det både er muligt og attraktivt for aktører i markedet at etablere private, kommercielle identitetsbrokere, som kan formidle adgang til infrastrukturen for private tjenester. Dette sikres ved at give private brokere alle nødvendige tekniske adgange for håndtering af identiteter samt ved at indrette betalingsmodeller og andre rammevilkår, så det er muligt at skabe en sund forretning for brokerne.

Arkitektur

Nedenstående figur illustrerer arkitekturen på logisk niveau[3]:



Figur 1: Logisk arkitektur

Som det fremgår af figuren, vil offentlige tjenesteudbydere fortsat anvende NemLog-in som identitetsbroker. Herudover kan et antal private, kommercielle brokere formidle MitID autentifikation til private tjenesteudbydere.

MitID forestår kun 'rå' autentifikation af personer, og al funktionalitet omkring erhvervsidentiteter og signering ligger i NemLog-in3. Dette betyder bl.a., at en privat broker vil skulle integrere til NemLog-in3's erhvervsAPI'er eller SAML IdP snitflade for at kunne formidle autentificerede erhvervsidentiteter. NemLog-in's erhvervsAPI udstiller bl.a. relationen mellem MitID akkreditiver og en erhvervsidentitet i NemLog-in3's register. Ved at benytte NemLog-in's SAML IdP interface kan en privat broker endvidere få adgang til at autentificere brugere, der

[3] Bemærk at forkortelsen TU står for tjenesteudbyder, altså en forretningstjeneste som aftager digitale identiteter og services relateret til disse (autentifikation, signering osv.)

er tilknyttet en lokal IdP for en brugerorganisation. Brokere skal selv integrere til MitID for at kunne gennemføre MitID transaktioner.

NemLog-in3 vil endvidere stille funktionalitet til digital signering til rådighed for private brokere, men dette kan også etableres af brokerne selv baseret på den underliggende MitID autentifikation. Brokere får ikke adgang til NemLog-in's funktionalitet til brugerrettighedsstyring.

Fordele ved brokerarkitekturen

Der er en lang række fordele, som ligger til grund for valg af brokerarkitekturen, herunder:

- Der sker en logisk afkobling af tjenesteudbydere og de bagvedliggende udstedere af akkreditiver (MitID), hvilket gør arkitekturen mere robust over for ændringer. Eksempelvis vil MitID kunne indføre nye typer akkreditiver eller ændre autentifikationsprotokoller uden at påvirke tjenesteudbyderne direkte.
- Leverandøren af MitID får en smallere og mere veldefineret opgave, som appellerer til et bredere udvalg af aktører i markedet.
- Der kan opnås nogle sikkerhedsmæssige fordele herunder bedre governance af sikkerheden, når kun nogle få specialiserede brokere kan få adgang til at integrere direkte med MitID.

Endvidere kan det nævnes, at arkitekturen i brokermodellen er i fuld overensstemmelse med principperne i den fællesoffentlige referencearkitektur for brugerstyring.

Muligheder for brokere

Nedenfor er angivet udvalgte eksempler på områder, hvor private brokere kan differentiere deres tilbud til private tjenesteudbydere i forhold til NemLog-in3's ydelser:

- De kan tilbyde varianter af signering eller brugerrettighedsstyring.
- De kan tilbyde alternative snitflader til integration for tjenesteudbydere.
- De kan samle muligheden for autentifikation med flere typer akkreditiver end MitID, herunder udenlandske akkreditiver.
- De kan tilbyde en alternativ brugeroplevelse.
- De kan berige autentifikationen med ekstra attributter fra andre kilder.
- De kan tilbyde en dybere integration med tjenesteudbydernes løsninger eller sektorspecifikke løsninger.

- De kan tilbyde attraktive betalingsmodeller (se senere afsnit om dette).

Krav til brokere

Identitetsbrokere er en særlig betroet part i identitetsinfrastrukturen (en såkaldt *trusted third party*), og derfor er kravene til sikkerhed, forretningsførelse og modenhed høje. Kravene til brokere er udmøntet i en såkaldt 'brokeraftale' fra MitID, og endvidere vil der være en række vilkår for adgang til erhvervsAPI'erne på NemLog-in3.

Brokeraftalen er en aftale mellem brokeren og MitID leverandøren, som regulerer de ydelser, som modtages fra MitID leverandøren, og de vilkår der er forudsætning for at agere som broker. Aftalen regulerer fx tilslutning, test, support, sikkerhed, betaling, rapportering, logning, certificering, revision, garantier mv.

Betalingsmodeller

En privat broker skal afregne over for MitID per transaktion, som gennemføres på vegne af en bagvedliggende tjenesteudbyder. Transaktionsafgiften fra MitID, som opkræves hos brokere, vil være den samme uanset om tjenesteudbyderen er koblet på via NemLog-in eller en privat broker. I den henseende sker der en fuldstændig ligebehandling af brokere.

Hvis en privat broker har brug for at formidle autentifikation af erhvervs-identiteter, er det som nævnt en mulighed at slå disse op via et API udstillet af erhvervsløsningen i NemLog-in3. Det er endnu ikke afklaret, om dette opslag vil være betalingsbelagt, men i givet fald vil alle private tjenesteudbydere blive opkrævet samme betaling, så private brokere ligebehandles.

Endelig skal det bemærkes, at private tjenesteudbydere, som tilslutter sig NemLog-in3, skal betale for deres anvendelse af NemLog-in3. Prisen er endnu ikke fastsat, men skal bl.a. dække tilslutning til NemLog-in3 og løbende forvaltning.

Konceptuelt kan betalingsmodellen illustreres ved flg.:

For privat tjenesteudbyder (TU) tilsluttet NL3:

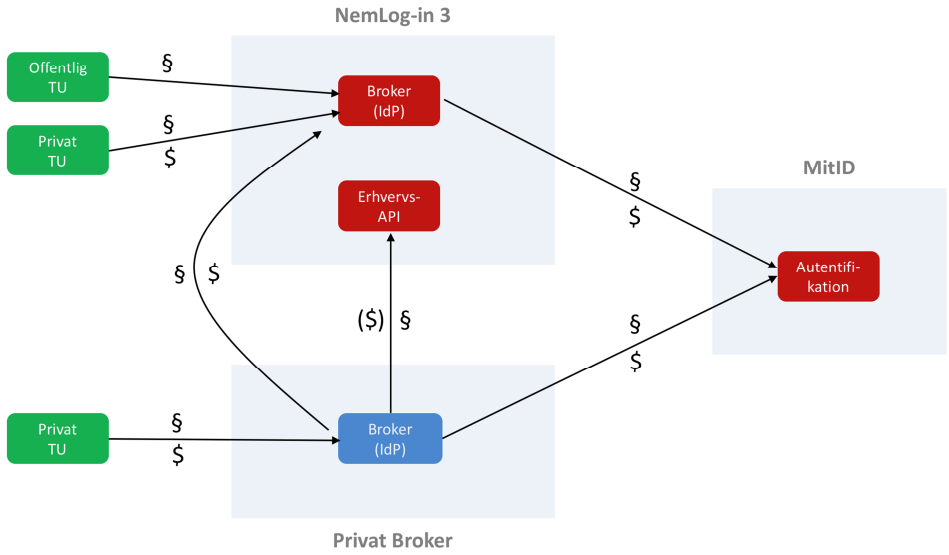
TU autentifikationspris = MitID autentifikationspris + NemLog-in omkostning

For privat tjenesteudbyder (TU) tilsluttet privat MitID broker:

TU autentifikationspris = MitID autentifikationspris + privat broker omkostning

Gennem betalingsmodellen vil det blive sikret, at markedet for private brokere ikke underbydes af NemLog-in. Digitaliseringsstyrelsen er i dialog med konkurrencemyndighederne med henblik på at sikre transparens og fair vilkår.

Nedenstående figur illustrerer aftalerelationer og betalingsrelationer i arkitekturen ('§' symboliserer en aftalerelation og '$' symboliserer en transaktionsbetaling):



Figur 2: Aftale og betalingsrelationer