

Unilogin Broker

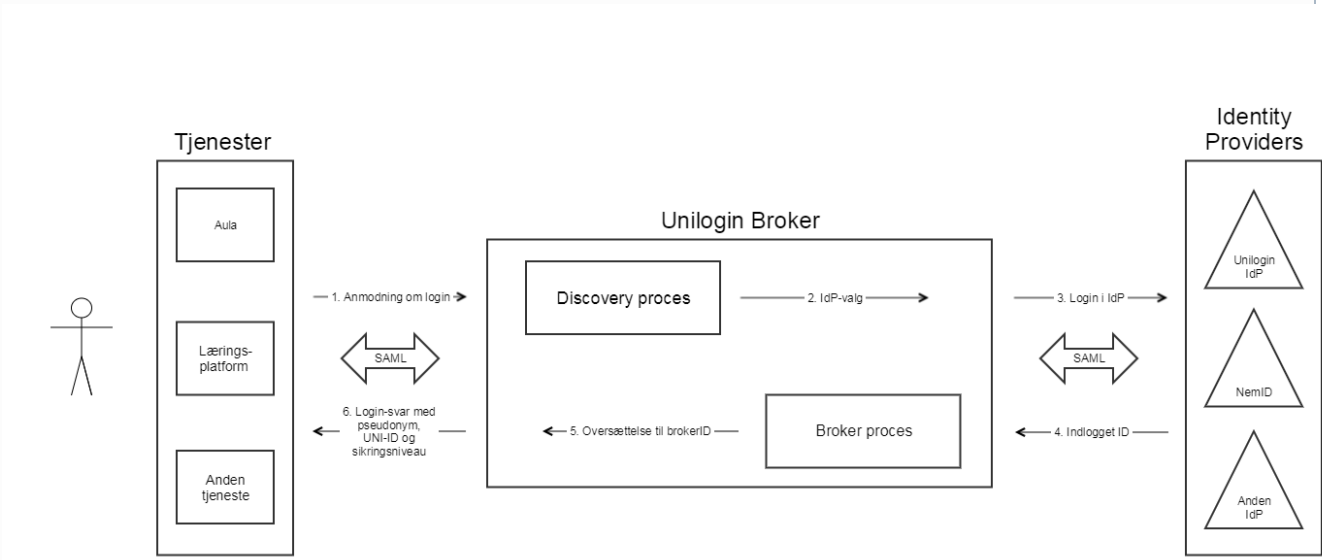
Primær målgruppe

Teknisk personale

Unilogin Broker

Unilogin Broker er en loginfordeler, dvs. en mellemmand mellem de tjenester, som ønsker at logge en bruger ind og samlingen af *Identity Providers* (IdP'er), som kan bekræfte brugerens identitet.

Model af Unilogin IdP-fordeler (Broker)



Unilogin Broker består af et discovery-modul til valg af Identity Provider (fx Unilogin IdP) og et broker-modul til håndtering af single sign-on og oversættelse af IdP'ernes ID'er til et brokerID, der er entydigt i Unilogin-federationen.

Et brokerID indeholder sammenhængen mellem hvad man kan **agere som** (fx medarbejder) i Unilogin og hvad man kan **identificeres med** (f. eks. CPR-nummer). Desuden oversættes til det gamle *Unilogin* brugernavn (UNI-ID) af hensyn til bagudkompatibilitet med [\[Brugerportalinitiativets Webservice API\]](#).

Eksempler på andre IdP-fordelere eller Brokere

IdP-fordeler (Broker)	Ejer	læs mere
NemLog-in2	DIGST	NemLog-in
NemLog-in3 og Private Brokere	DIGST	Brokere og krav til brokere i det kommende NemLog-in3 (herunder fordeling til MitID)

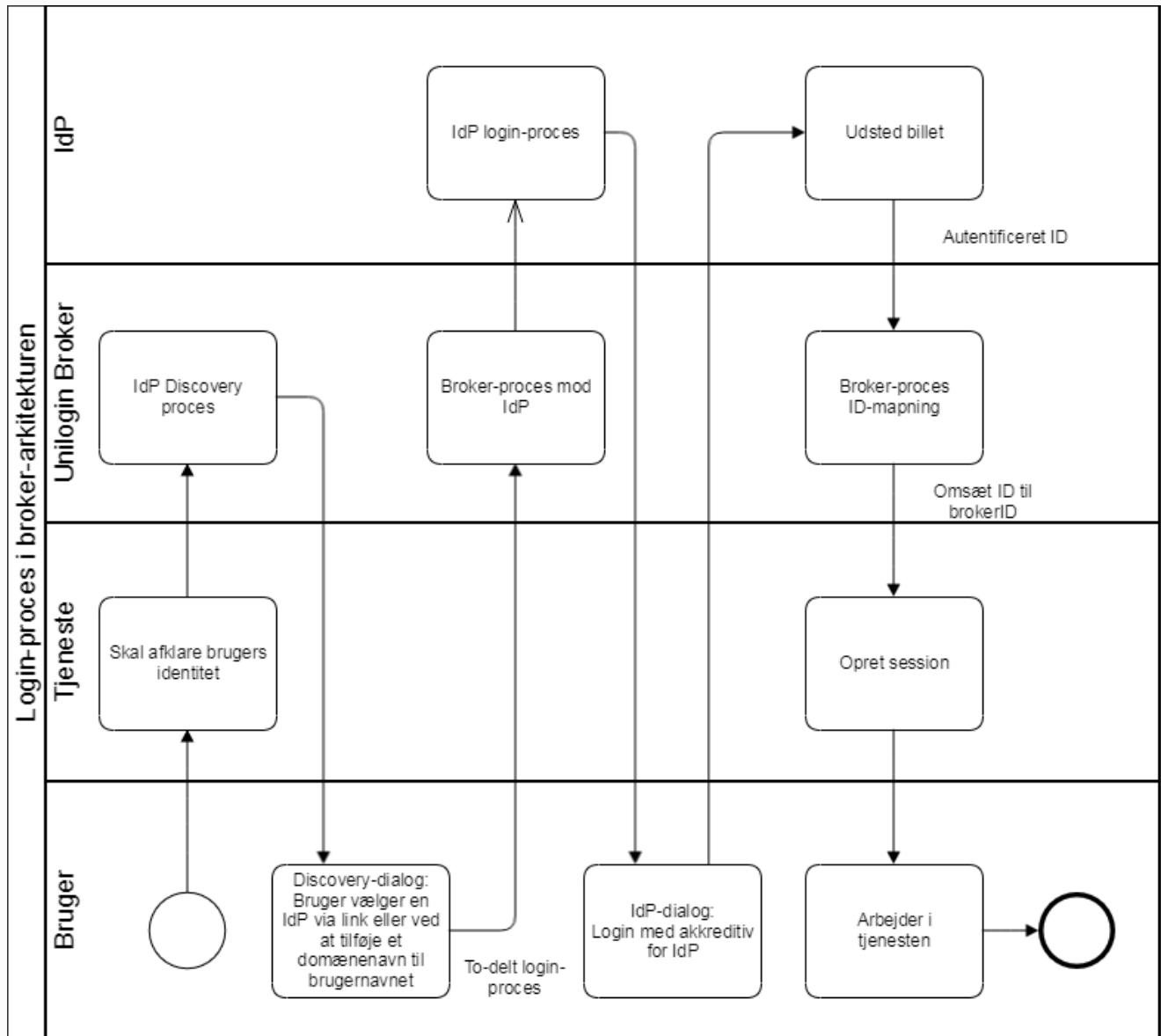
Der er pt følgende IdP'er tilknyttet Unilogin Broker:

Navn	Ejer	Tilsluttet siden	Noter	Læs mere
Unilogin IdP	STIL	1. aug. 2019		Unilogin IdP
NemID	STIL (integrationen)	1. aug. 2019	Både NemID og NemID medarbejdersignatur (med CPR) kan benyttes	NemID NemID medarbejdersignatur

Loginproces i Unilogin Broker

Nedenfor er login-processen med Unilogin Broker vist. Brugere og de forskellige komponenter i Unilogins broker-arkitektur optræder som svømmebaner.

Brugeren indtaster et brugernavn eller vælger IdP direkte via et link i Unilogin Broker. Unilogin Broker anvender denne information til at afgøre hvilken IdP brugeren skal sendes til. Hvis der er indtastet et brugernavn afgør domæne-navnet efter "@" hvilken IdP, der skal anvendes og brugernavnet medsendes til IdP'en.



Unilogin Broker discovery- og broker eksempel

Brugeren vil logge ind i en tjeneste (SP), som viderestiller til IdP-fordeleren for at få brugeren autentificeret. IdP-fordeleren skal nu afklare hvilken IdP der skal anvendes (Discovery-proces).

SP'en kan kommunikere til IdP-fordeleren, hvilken IdP og hvilket sikringsniveau, der er relevant i det givne kontekst. Hvis tjenesten ikke fastlægger kontekst, er det nødvendigt at involvere brugeren i IdP-valget. Dette gøres ved at IdP-fordeleren præsenterer brugeren for en side, hvor man kan indtaste et brugerid i Unilogin IdP'en eller vælge en anden IdP eksplicit. Indtastes et brugerid er Unilogin IdP'en implicit valgt og brugeren viderestilles til Unilogin IdP'en. Forvalget af brugerid medsendes fra Unilogin Brokeren til Unilogin IdP'en, hvor brugeren afgiver sit akkreditiv.

Brugeren er nu autentificeret med et UPID i Unilogin IdP'en, og viderestilles tilbage til Unilogin Brokeren, som skal fastlægge hvilken identitet brugeren vil agere som i denne session (Broker-proces). Brokeren fremfinder via brokerID databasen en eller flere brokerID'er, som relaterer til UPID'et fra Unilogin IdP'en.

Hvis der er flere brokerID'er, må brugeren vælge hvilken der skal anvendes i den aktuelle session. Brokeren er i dette tilfælde nødt til at præsentere brugeren for brokerID'ernes tilknyttede aktører.

Der oprettes et nyt brokerID, når entiteten registreres med en ny aktør som hhv elev, medarbejder/ekstern eller kontakt.

Det betyder, at der vil findes netop et brokerID, der relaterer til alle entitetens aktører med en given type og brokeren kan derfor nøjes med at afklare, om brugeren vil agere som elev, medarbejder og kontakt.