Opfølgende informationsmøde for interesserede brokere

17. september 2019

Dagsorden

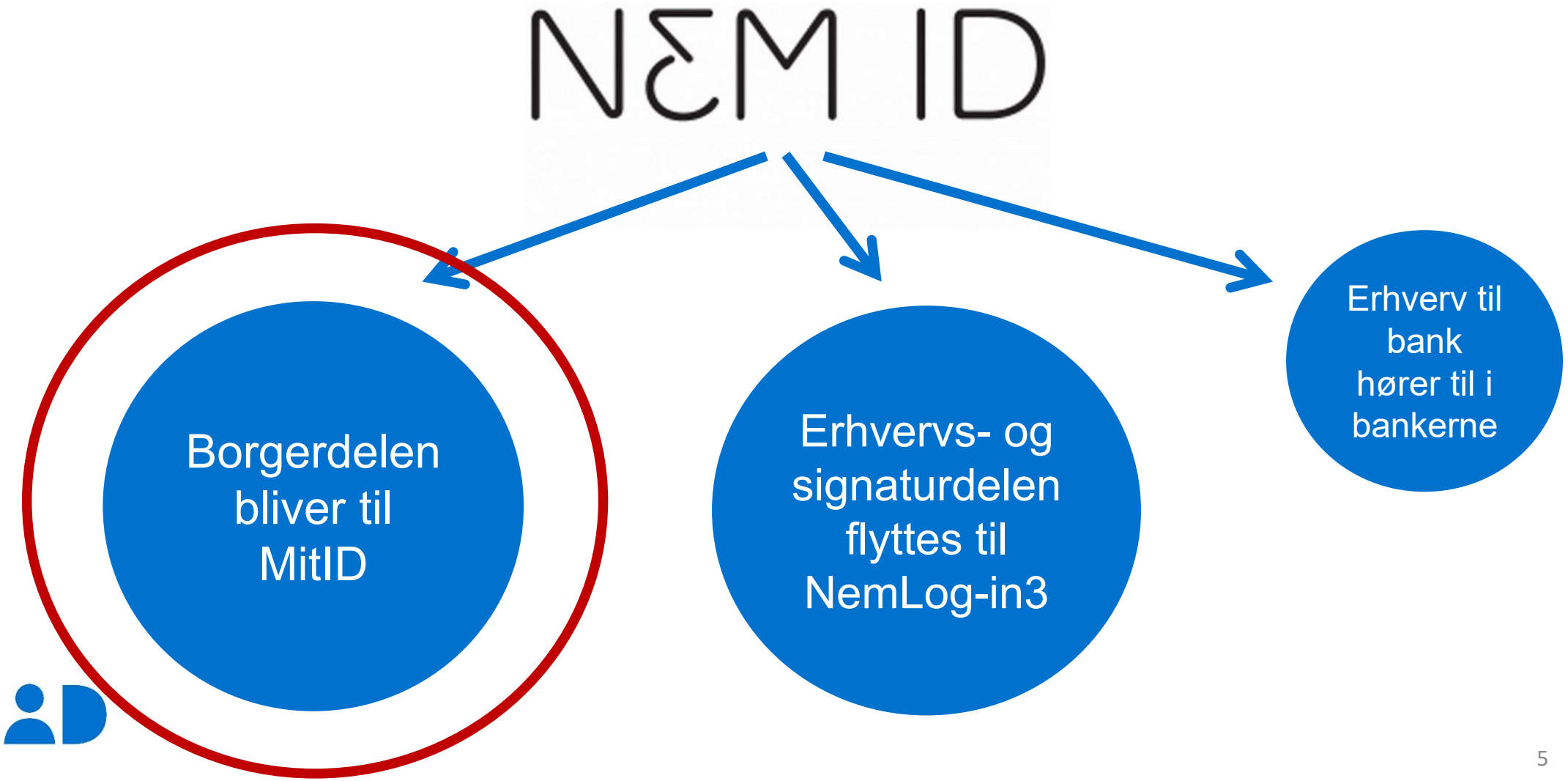
- Velkommen
- Hvorfor MitID?
- Hurtig genopfriskning
- Krav til brokere
  - NSIS og anvendelsesmodeller
  - Risk data model
  - Single sign on
  - Erhvervsidentiteter, NemLog-in som IdP
  - Samfundskritisk infrastruktur
  - Drift og support
  - Sikkerhed
  - Proces for at blive broker
- Betaling
- MitID's tidsplan
- Næste skridt for interesserede brokere

Allerførst: Hvorfor MitID?

Fundamentet for det digitale Danmark skal sikres – også i fremtiden

- Behov og krav ændrer sig
- Fremtidige udfordringer er svære at spå om
- Ønske om en styrket, sikker og fleksibel digital infrastruktur i Danmark
  - Fælles ønske på tværs af den private og offentlige sektor
  - MitID bliver til i et partnerskab mellem Digitaliseringsstyrelsen og FR1, datterselskab af Finans Danmark
- Visionen er at skabe langsigtede, sammenhængende og fleksible løsninger

NemID skiftes ud



Ny arkitektur med nyt snit mellem person- og erhvervsidentiteter

MitID

Person-identiteter

- Håndtering af loginmidler
- Oprettelse og administration
- Klient

NemLog-in3

Erhvervs-identiteter

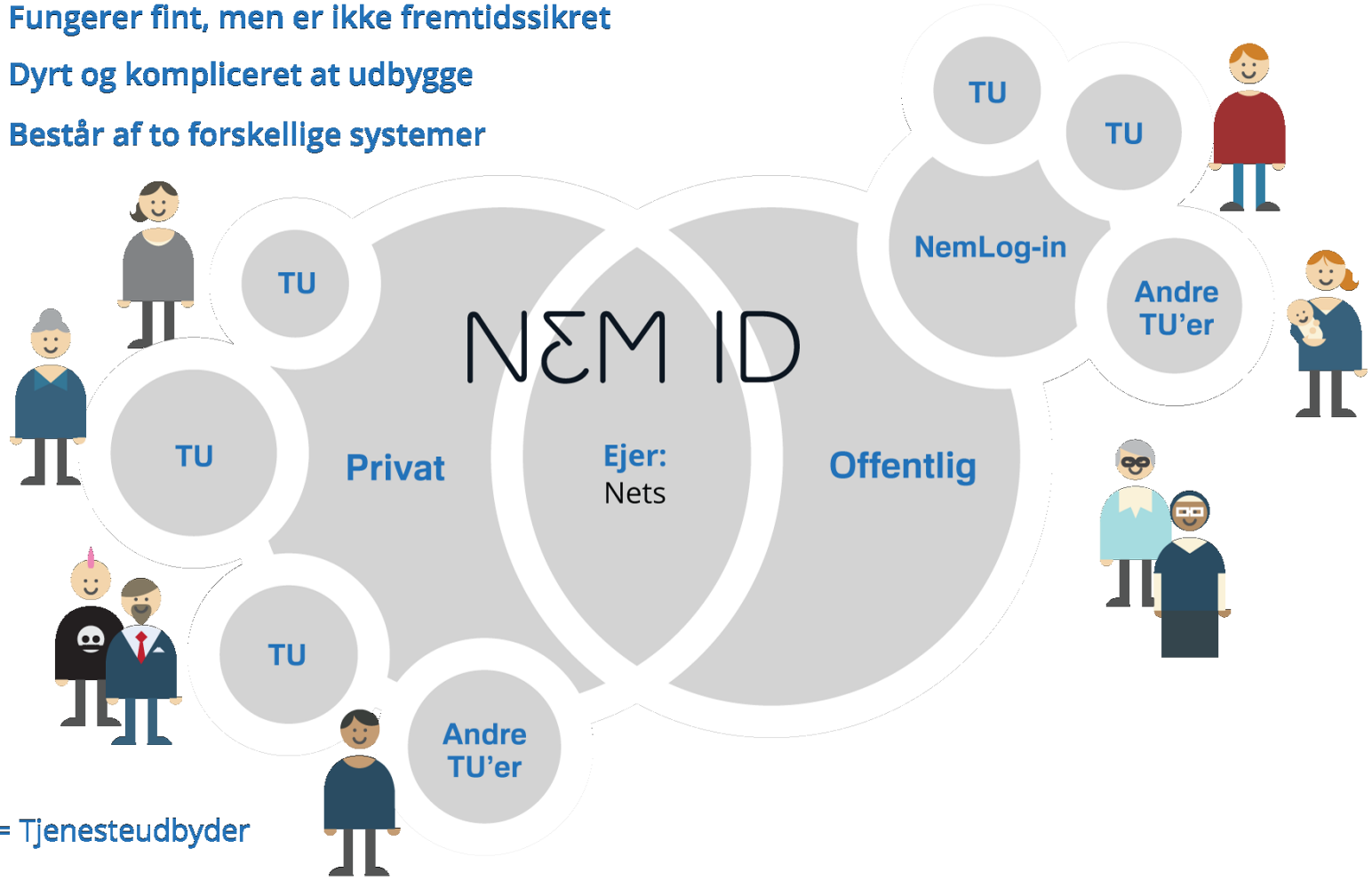
Videreførelse af NemLog-in2 plus:

- MitID broker
- Signering
- Udstedelse af certifikater

MitID

Fra NemID...

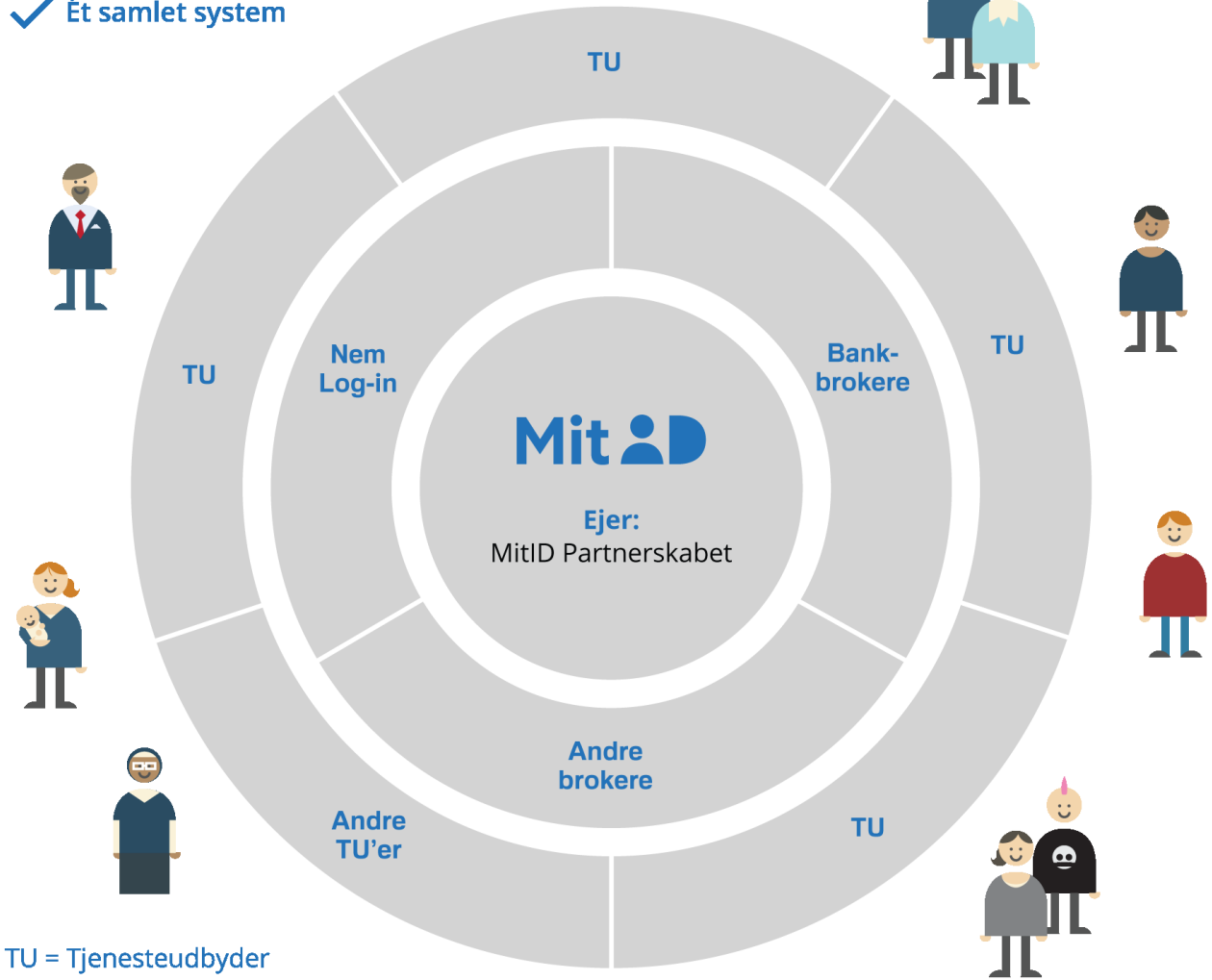
- ✓ Fungerer fint, men er ikke fremtidssikret
- ✗ Dyrt og kompliceret at udbygge
- ✗ Består af to forskellige systemer



TU = Tjenesteudbyder

...til MitID

- Fremtidssikret – fleksibelt og modulært opbygget
- Nemmere at udbygge i takt med, at behov og trusler ændres
- Ét samlet system



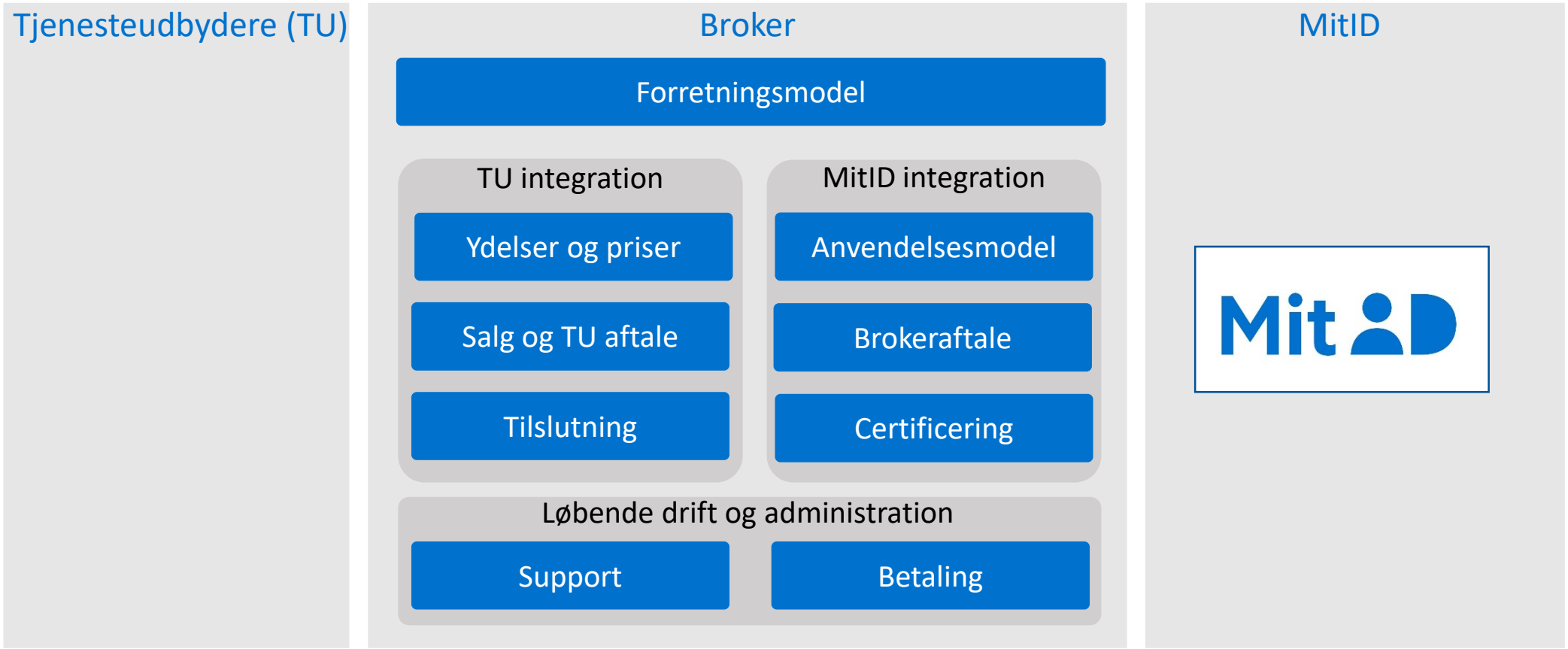
TU = Tjenesteudbyder

Tidsplan


Mar 2019
Kontrakten er skrevet under
6. marts 2020
Brokere kan koble sig på MitID
Sommer 2021
GO LIVE
Nu - 4. kvt. 2019
Udviklingsanalyser og aktørinvolvering
4. kvt. 2019 - 4. kvt. 2020
MitID udvikles
4. kvt. 2020 - sommer 2021
Test og pilotafprøvning
Sommer 2021 - ultimo 2021
Migrering af NemID-brugere
NemID og MitID bruges begge

Hurtig genopfriskning

Brokerrollen: Bindeled mellem tjenesteudbydere og MitID



Markedet for autentifikationer

Samlet

Antal NemID: ca. 5.1 mio + 3 % pr. år

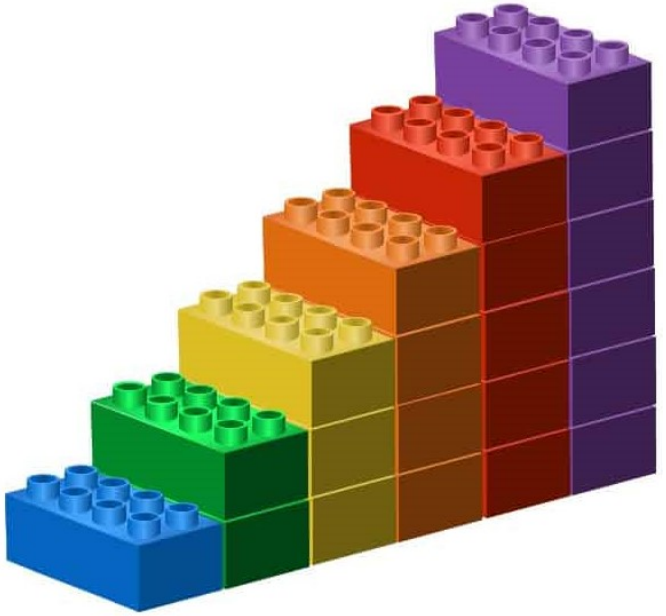
Autentifikationer: ca. 780 mio/år + 3-4 % pr. år

Segmenter

Bank	**Privat ej bank**	**Offentlig**
Autentifikationer: ca. 73% ca. 567 mio/år	Autentifikationer: ca. 18% ca. 137 mio/år	Autentifikationer: ca. 9% ca. 74 mio/år
	Ca. 380 tjenesteudbydere	Ca. 300 tjenesteudbydere

Brokere

5 bankbrokere	? private brokere (NemLog-in)	NemLog-in



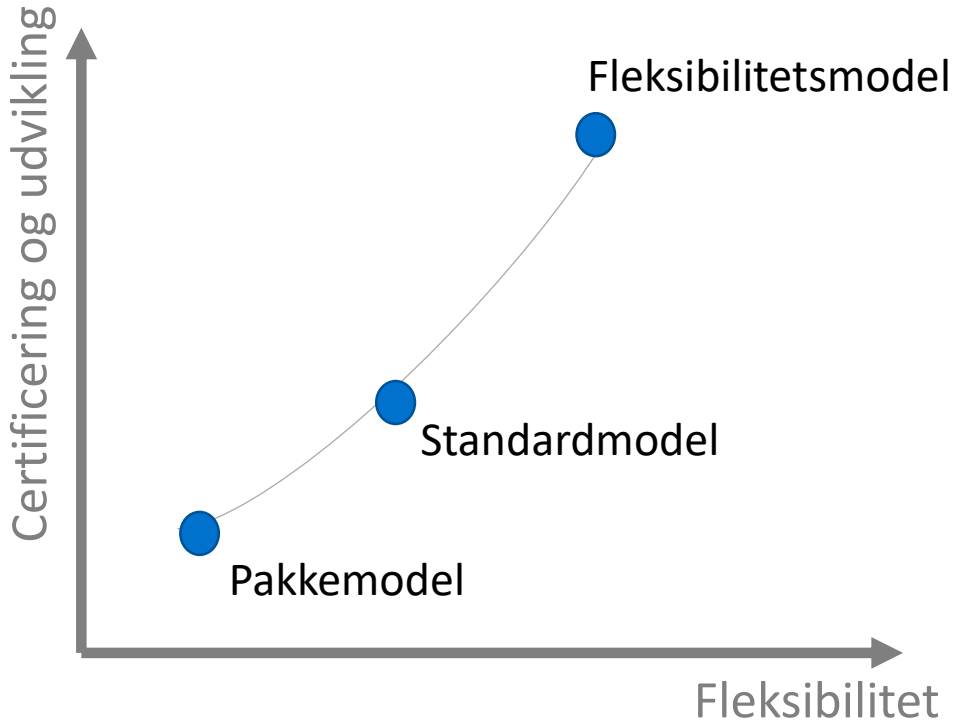
NSIS og anvendelsesmodeller

MitID bygger på NSIS-standarden

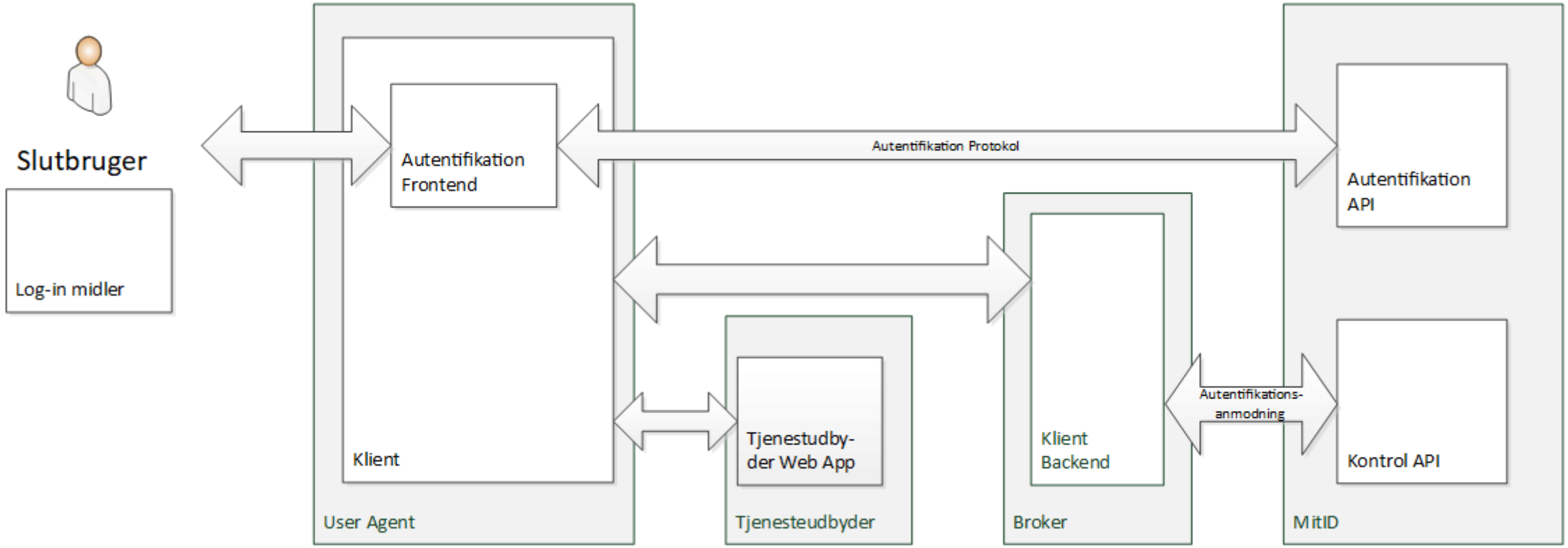
- National Standard for Identiteters Sikringsniveauer
- Fælles ramme for tillid til digitale identiteter og elektroniske loginmidler
- Tre sikringsniveauer
  - Lav, Betydelig, Høj
- Hvert sikringsniveau styres af en række klare procedurer og instruktioner, der sikrer, at brugerne placeres i den rigtige kasse
  - Niveau Lav stiller færrest krav
  - Niveau Betydelig vil være mest almindelig – ca. som OCES i dag
  - Niveau Høj bruges, når tjenesteudbyderen ønsker ekstra høj sikkerhed for, at brugeren er dén, vedkommende giver sig ud for at være. Fx sundhedsvæsenet
  - Man kan ”steppe up”

Anvendelsesmodeller og frihedsgrader

- Brokere kan vælge mellem 3 anvendelses-modeller:
  - Pakke
  - Standard
  - Fleksibilitet
- Modellerne understøtter forskellige grader af fleksibilitet
- Stor fleksibilitet stiller store krav til certificerings- og udviklingsindsats
- Anvendelsesmodeller kan kombineres
- Brokeren har frihed til selv at vælge integration til tjenesteudbyder (baseret på standardprotokoller, fx SAML, OIDC mv.)

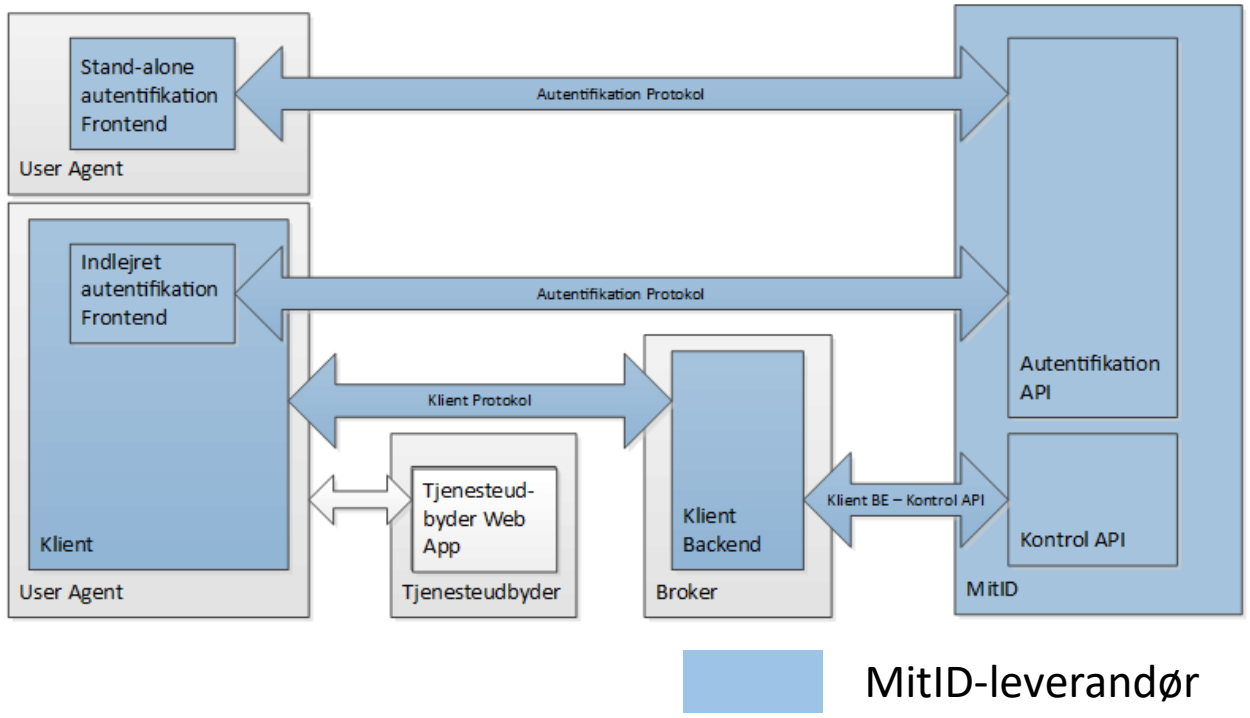


Autentifikationskoncept (recap fra første møde)

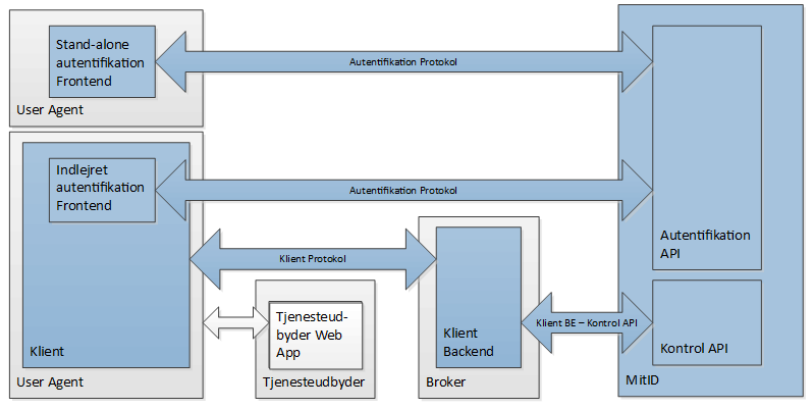


Pakkemodel

- Samtlige komponenter stilles til rådighed af leverandøren, herunder kerneklient og kerneklient backend
- Brokeren behøver ”kun” at initialisere/loade kerneklienten og håndtere autentifikationssvar fra kontrol API
- Certificering under pakkemodel



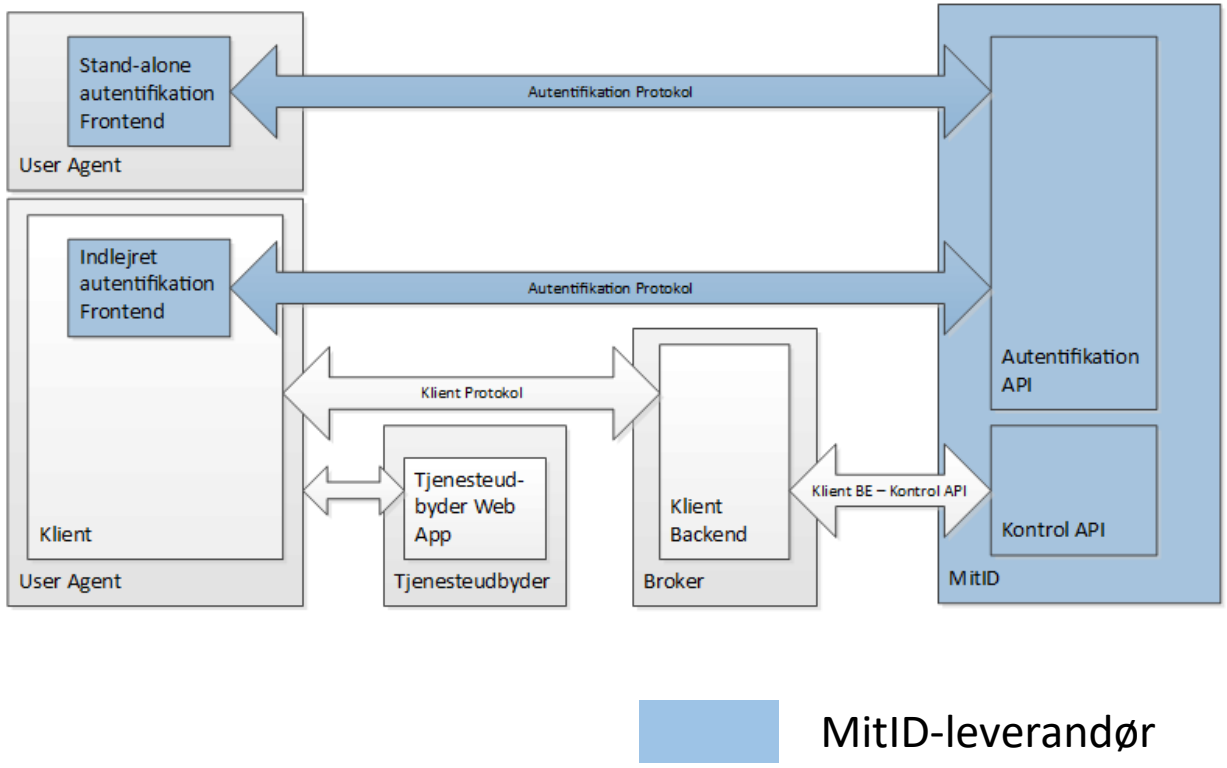
Pakkemodel



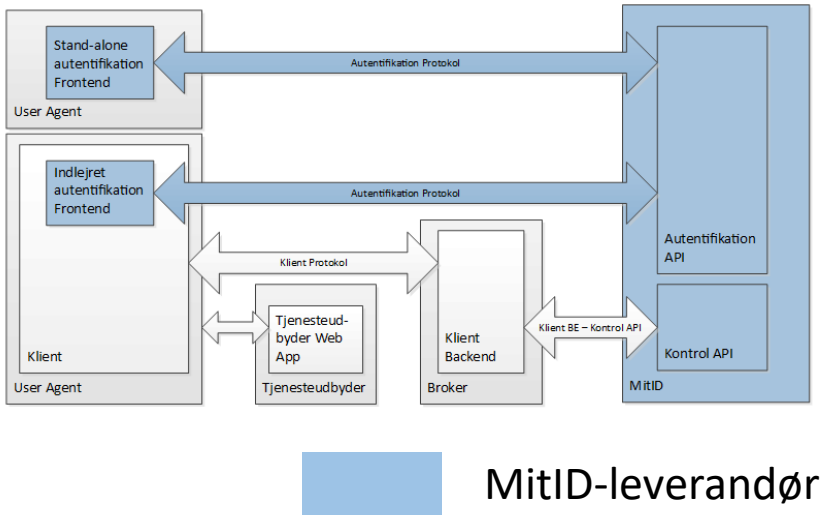
- Nets stiller dokumentation og eksempelkode til rådighed, der viser:
  - Hvordan kerneklienten loades på broker landing page (baseret på HTML/JavaScript)
  - Hvordan brokeren modtager authentication response fra kernen (baseret på Java og C#)
  - Hvordan authentication response valideres (baseret på Java og C#)

Standardmodel

- Samtlige komponenter stilles til rådighed af leverandøren, undtagen klient og klient backend
- Brokeren har mulighed for at udvikle egne klienter, under overholdelse af UX scheme og codex
- Certificering under standardmodel
- Brokeren har mulighed for at inkludere yderligere funktionalitet i egenudviklede klienter



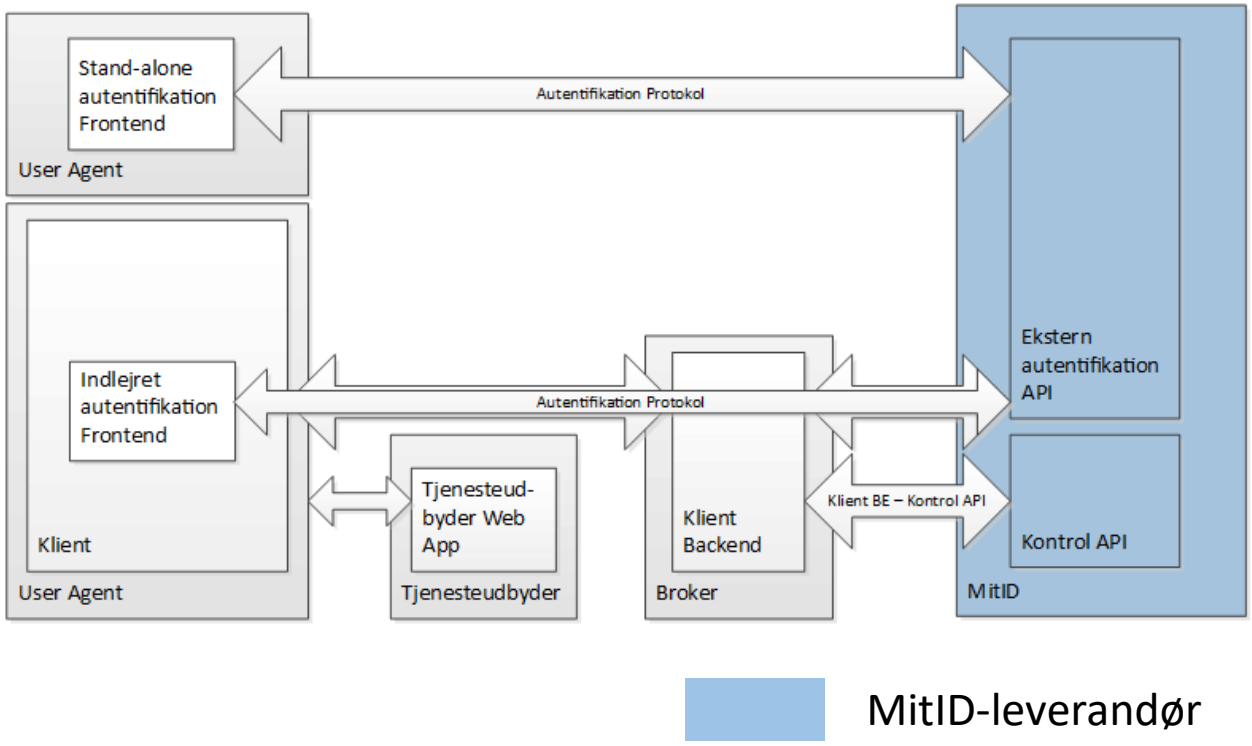
Standardmodel



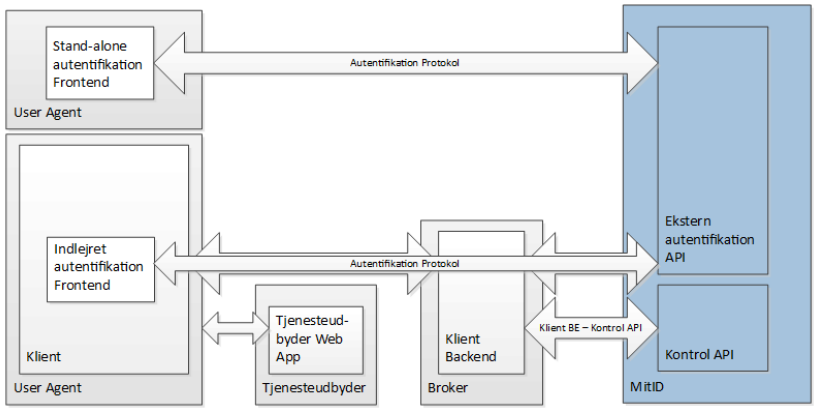
- Nets stiller dokumentation og eksempelkode til rådighed, der viser:
  - Hvordan en klient implementeres (baseret på kerneklient implementeringen via TypeScript transpileret til JavaScript og ren JavaScript)
  - Hvordan en klient backend implementeres (baseret på kerneklient backend implementeringen via Java og C#)

Fleksibilitetsmodel

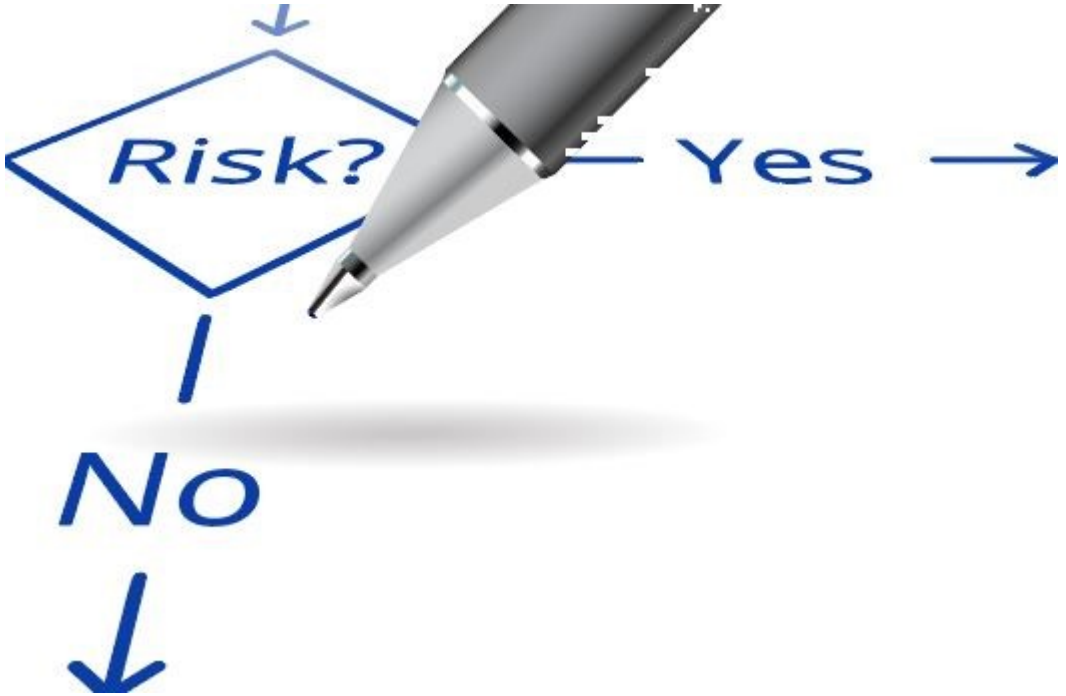
- Størst mulig fleksibilitet
- Brokere anvender kun de centrale API'ere, som leverandøren stiller til rådighed (kontrol API og eksternt rettede autentifikation API'ere)
- Brokere implementerer udover klient-komponenterne også autentifikation frontend og kommunikationen til autentifikation API'erne
- Certificering under fleksibilitetsmodel



Fleksibilitetsmodel



- Nets stiller dokumentation og eksempelkode til rådighed, der viser:
  - Hvordan en klient udvikles (baseret på kerneklient implementeringen via TypeScript transpileret til JavaScript og ren JavaScript)
  - Hvordan en klient backend udvikles (baseret på kerneklient backend implementeringen via Java og C#)
  - Hvordan embedded authentication frontends udvikles (baseret på samme sprog/frameworks som klient)



Risk data model

Risk data model fra et brokerperspektiv

- Modellen giver brokerne adgang til indsamlede risk parametre i forbindelse med autentifikation
- Risk data kan bruges af brokere til at kvalificere risikoen ved en given autentifikation i forhold til kontekst og øvrige brokerdata
- Modellen understøtter aggregering af information på tværs af autentifikationer
- Brokerne er både ”producent” og ”konsument” af risk data
  - Brokerne kan opt’e ud af ”konsument”-delen
  - Brokerne kan **IKKE** opt’e ud af ”producent”-delen (omfang er afhængigt af anvendelsesmodel)

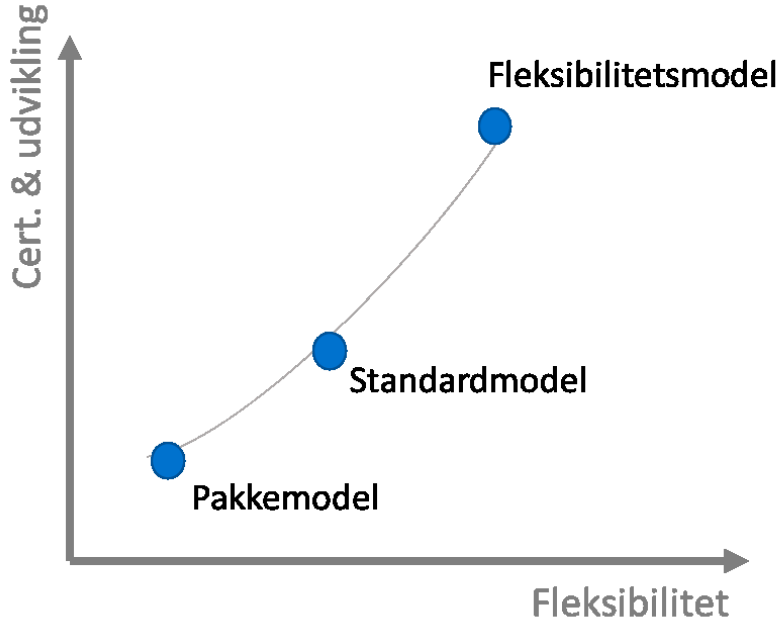
MitID

Risk data parametre (ikke-udtømmende)

- Location-based
  - GeoIP
- Network-based
  - IP-adresse(r) under autentifikation
- Device-based
  - User agent relaterede data
- Identity-based
  - eID relaterede data

MitID

Rapportering af risk data



- Rapportering af risk data er <u>obligatorisk</u> for brokere (brokerkodeks)
- Omfang er afhængig af den valgte anvendelsesmodel:
  - Pakkemodel
    - Kerneklient og KerneklientBE håndterer automatisk indsamling og rapportering af risk data. Brokere kan ikke deaktivere dette
  - Standardmodel
    - Brokere er ansvarlige for rapportering af klient-relaterede data via Control API
  - Fleksibilitetsmodel
    - Som i standardmodellen. Derudover er brokere ansvarlige for rapportering af AuthFE indsamlede risk data via authentication API'erne

Anvendelse af risk data

- Anvendelse er ikke obligatorisk
- Nogle data returneres som rå data, mens andre som aggregerede data på tværs af autentifikationer
- Risk data returneres som specifikke claims i authentication response
- Ingen formelle krav til, hvordan brokere skal vurdere modtagne risk data
  - Kontekstafhængigt

MitID

Jeres udviklingsprojekt skal følge denne tidsplan

Fire delleverancer

Delleverance 1: Dokumentation (6. feb. 2020), funktionalitet (6. mar. 2020)

- End-to-end autentifikation
- Password authenticator (single factor)

Delleverance 2: Dokumentation (24. apr. 2020), funktionalitet (25. apr. 2020)

- Multifactor autentifikation
- Password + TOTP authenticator

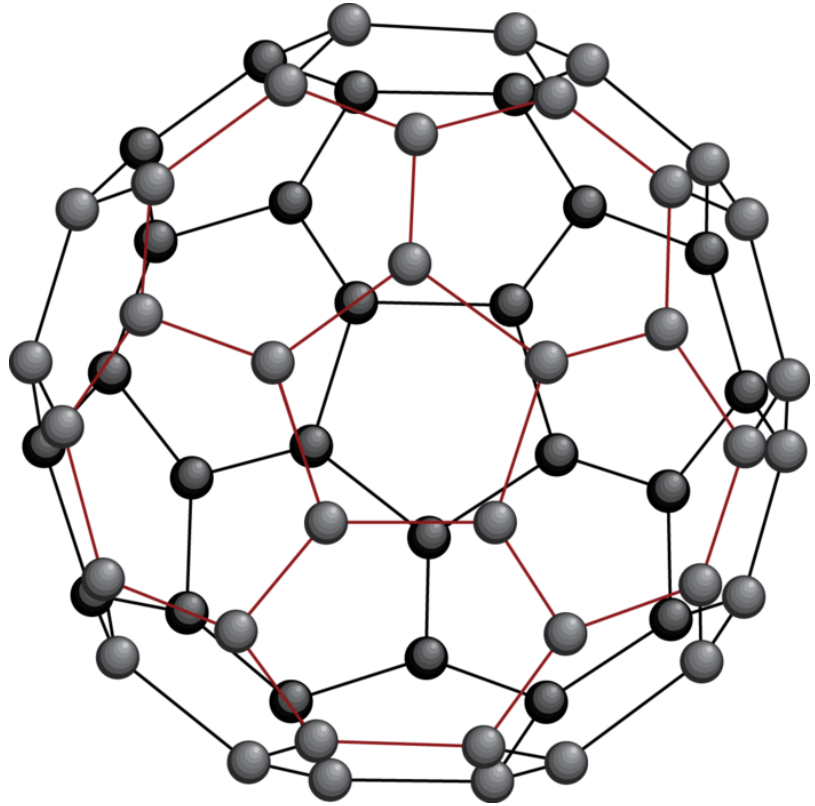
Delleverance 3: Dokumentation (11. aug. 2020), funktionalitet (11. sep. 2020)

- App Authenticator

Delleverance 4: Dokumentation (20. okt. 2020), funktionalitet (20. nov. 2020)

- U2F authenticator

Single Sign-on (SSO)



To SSO-modeller i kernen

Brokere kan vælge mellem to SSO-modeller, som stilles til rådighed:

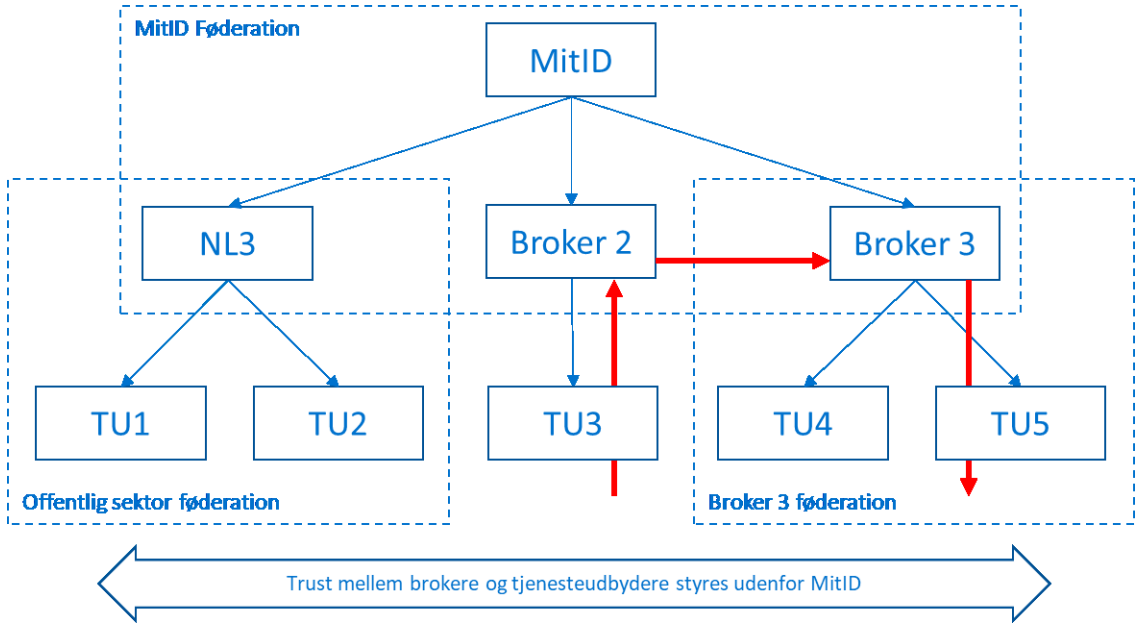
- Controlled Transfer of Authentication (punkt-til-punkt)
- Generel SSO (mellem brokere)

OBS: Brokere kan også vælge selv at implementere SSO-funktionalitet uden om kernen

Controlled Transfer of Authentication

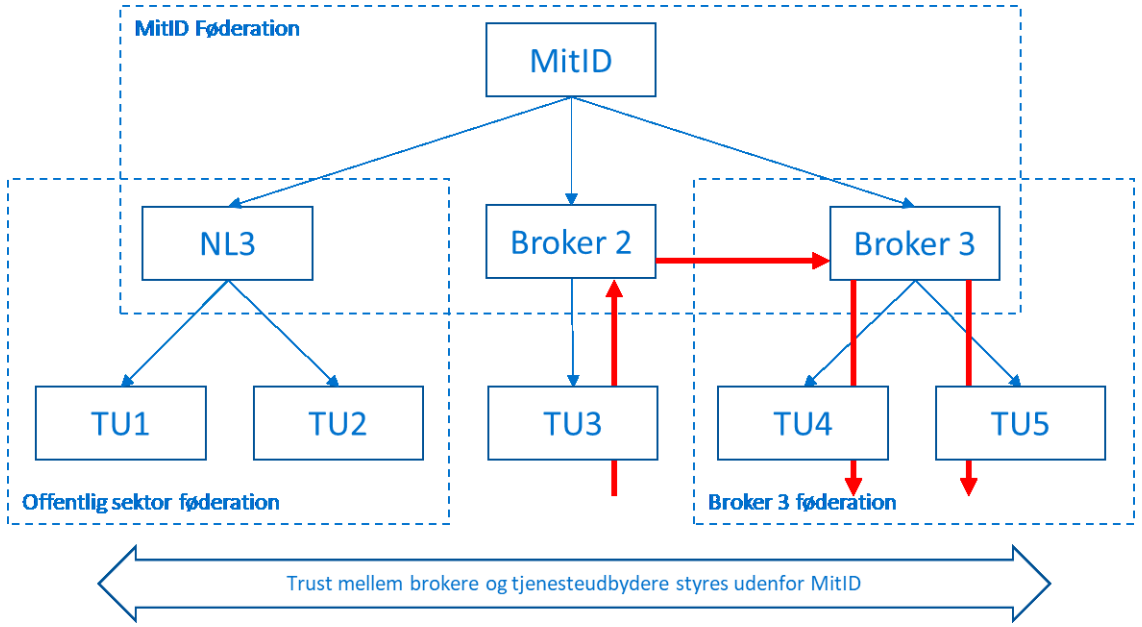
Controlled Transfer of Authentication

- Punkt til punkt mellem to tjenesteudbydere
  - Tilknyttet enten den samme broker
  - Eller to forskellige brokere
- Udelukkende teknisk infrastruktur
- Trust mellem brokere og tjenesteudbyderne knyttet til brokerne skal håndteres af brokerne selv



Generel SSO

- SSO mellem tjenesteudbydere knyttet til forskellige brokere
- Baseret på OpenID Connect Session management
- Udelukkende teknisk infrastruktur
- Trust mellem brokere og tjenesteudbydere knyttet til brokerne skal håndteres af brokerne selv

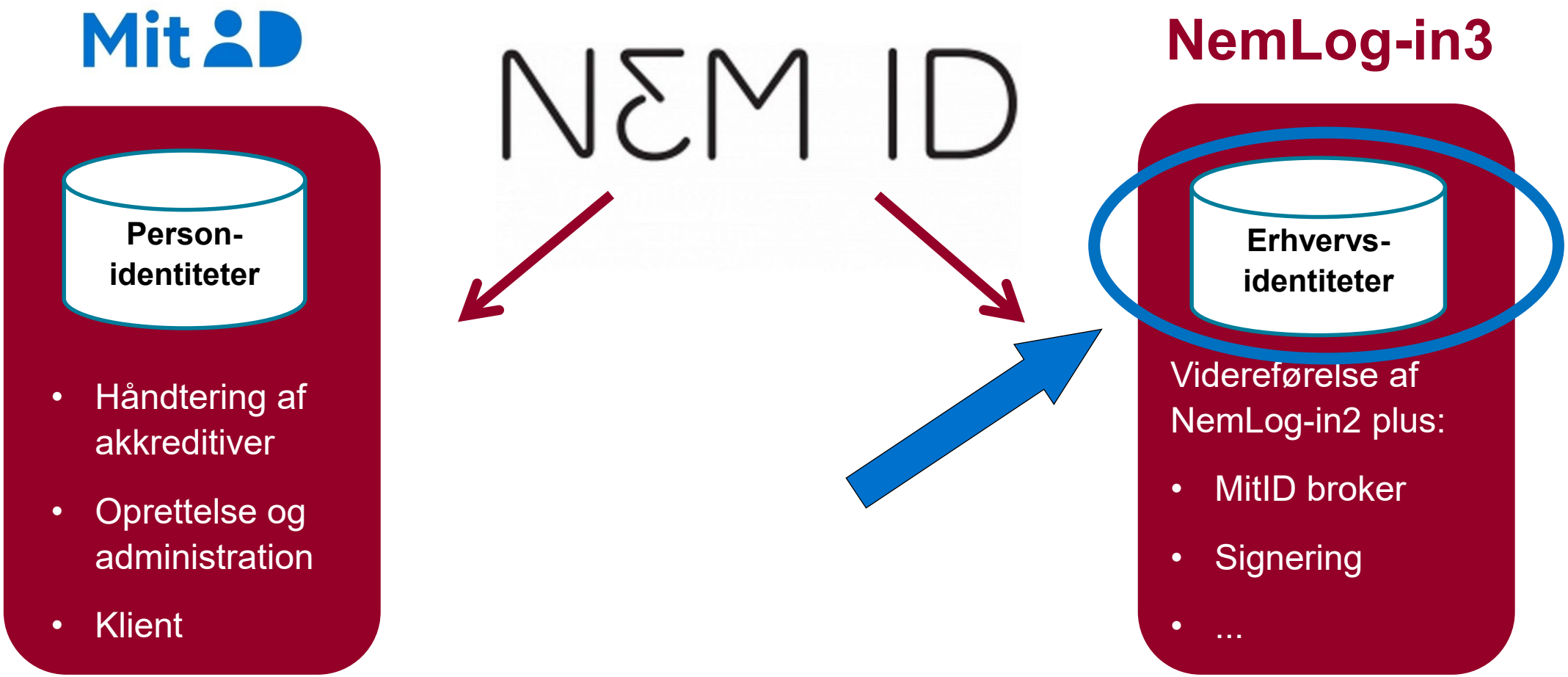


DIGITALISERINGSSTYRELSEN

Erhvervsidentiteter - NemLog-in som IdP

Maj 2019

Ny arkitektur, nyt snit



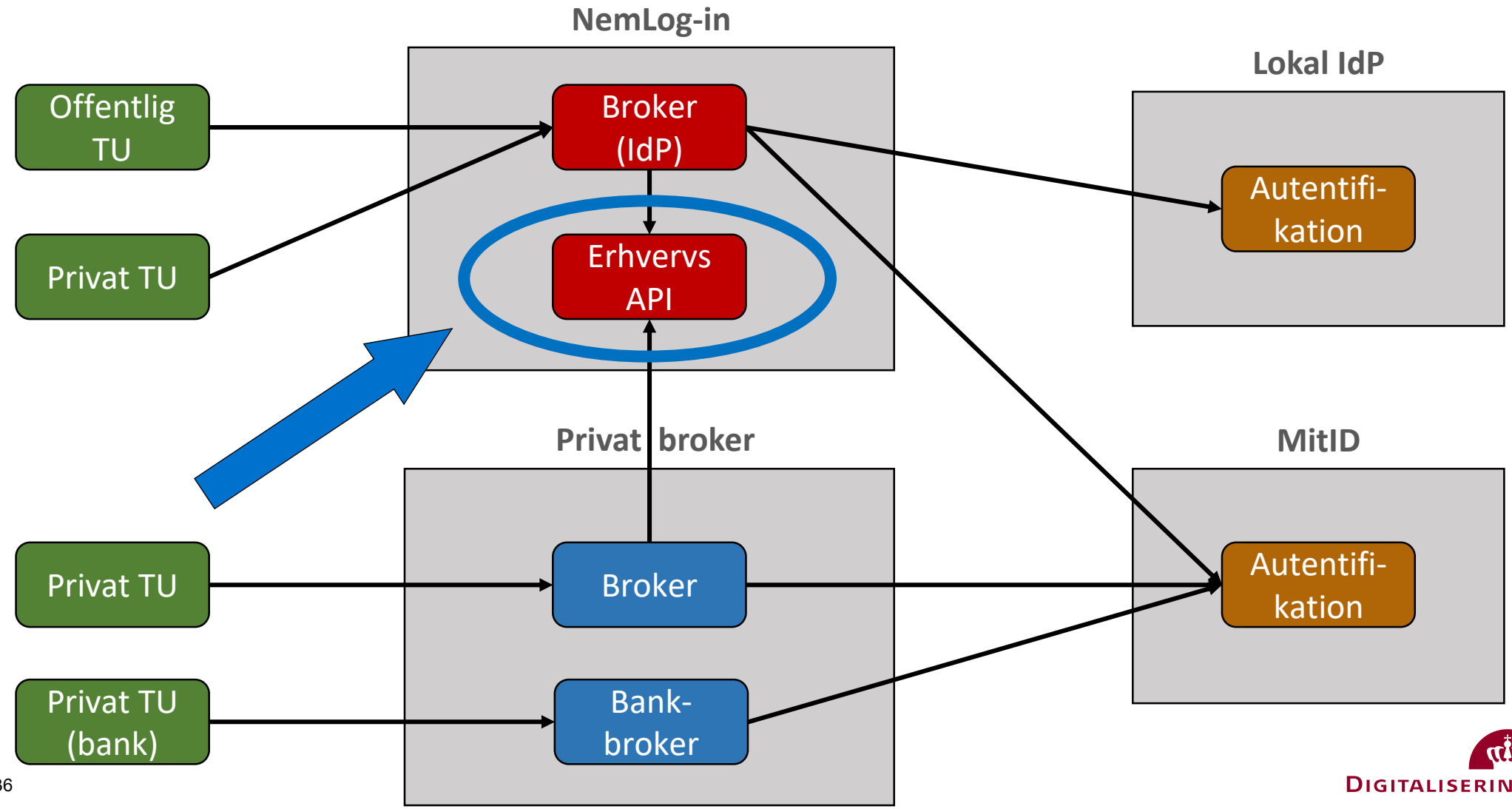
DIGITALISERINGSSTYRELSEN

Nye erhvervsidentiteter

- Erstatter NemID for Erhverv
- Etableres i regi af NemLog-in3
- Én aftaleindgåelse
- Benytter MitID-loginmidler
- Ny samlet portal på virk.dk
- Adgang for andre brokere via API

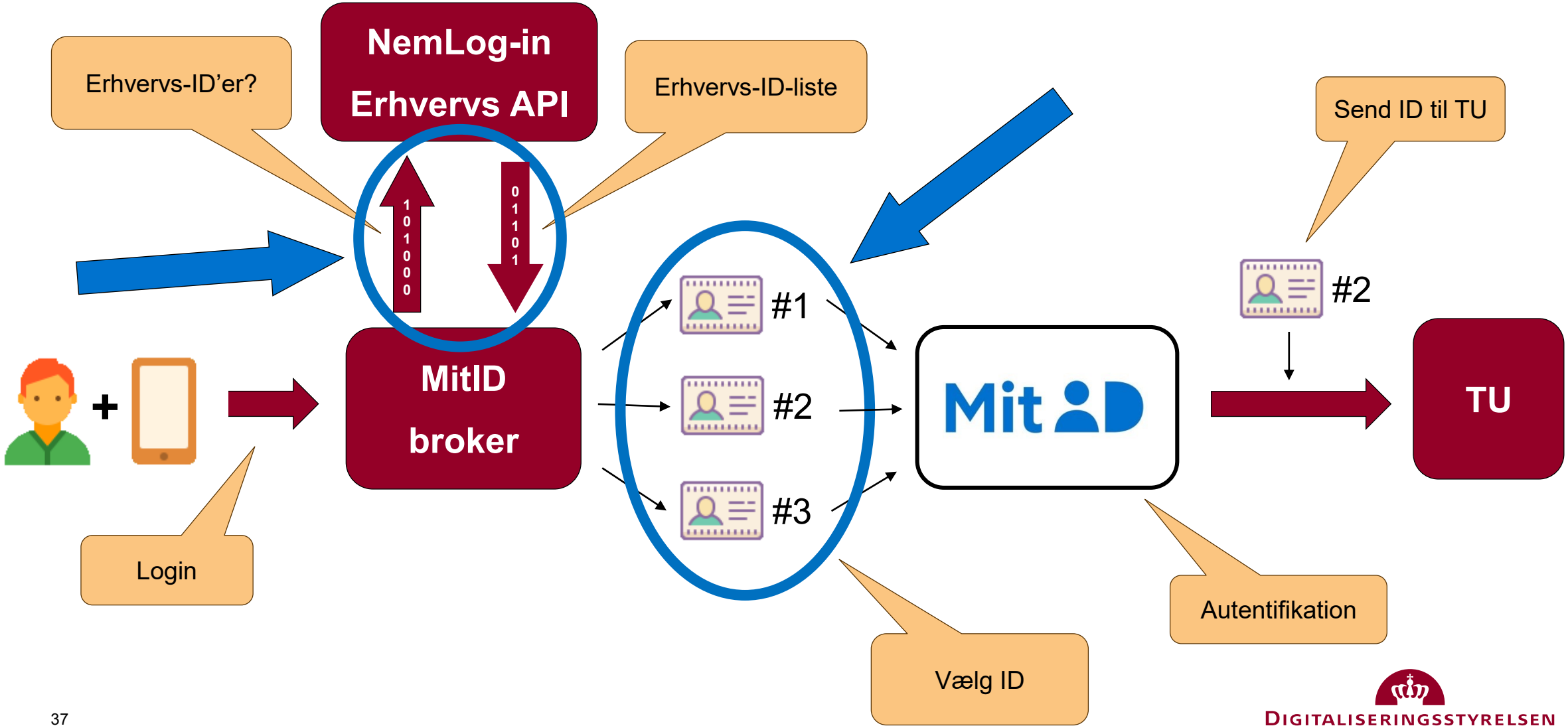
DIGITALISERINGSSTYRELSEN

Brokere i infrastruktur



DIGITALISERINGSSTYRELSEN

Konceptuelt login flow



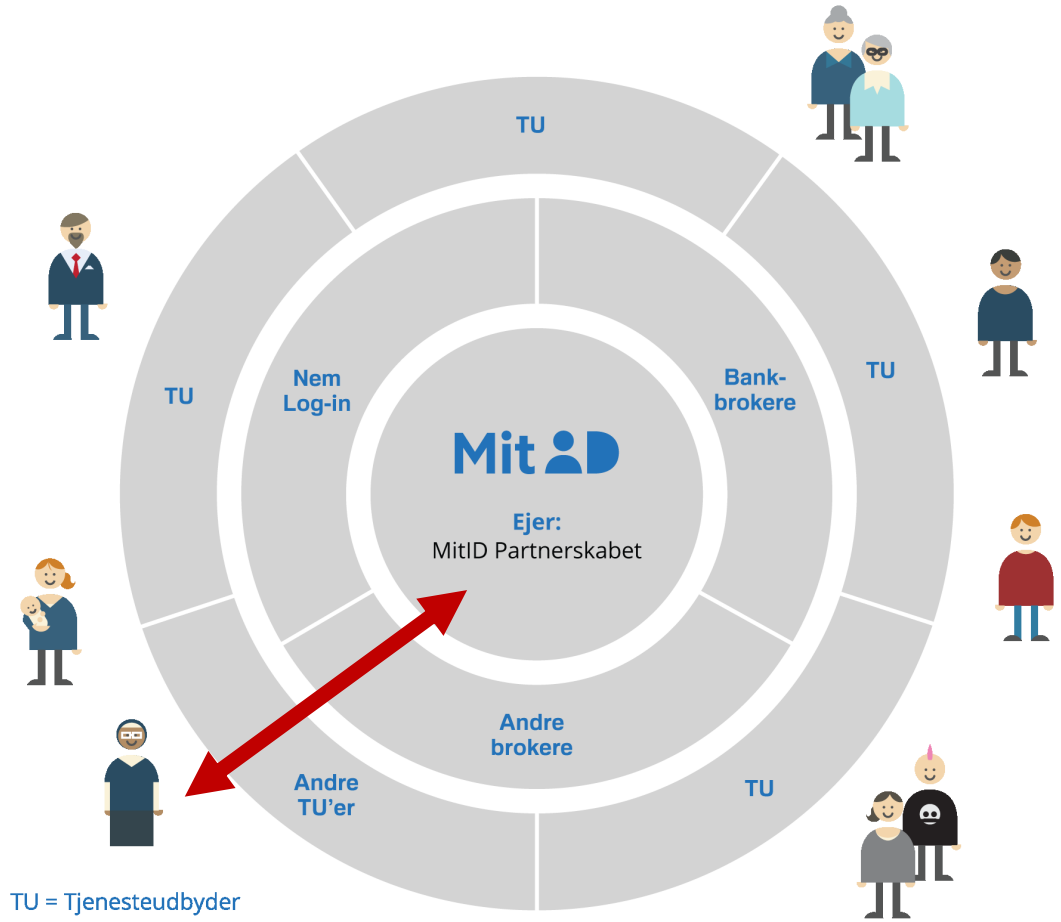
DIGITALISERINGSSTYRELSEN

Samfundskritisk infrastruktur

Slutbrugernes oplevelse afhænger af alle led

Broker er vigtig for brugeroplevelsen:

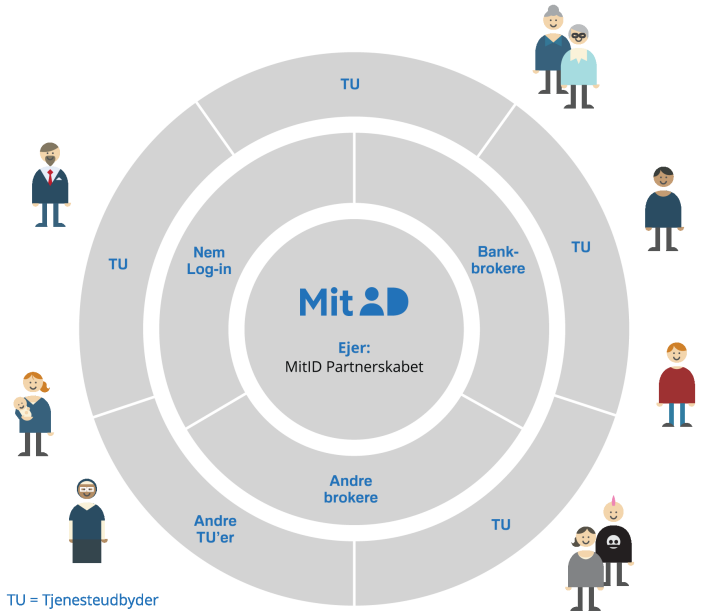
- Trygt
- Genkendeligt
- Effektivt i brug
- Tilgængeligt



Drift og support

Broker er vigtig for brugeroplevelsen:

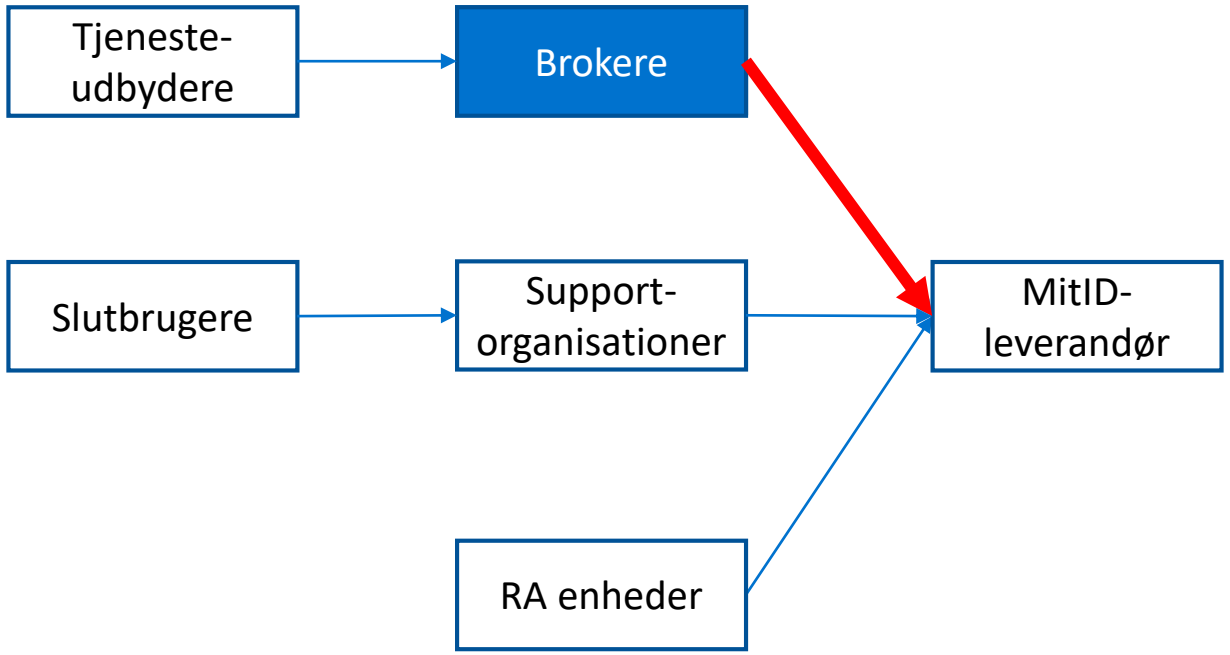
- Trygt
- Genkendeligt
- Effektivt i brug
- Tilgængeligt



Høje krav om tilgængelighed

- Krav om 24/7 tilgængelighed
- Serviceres døgnet rundt – ingen servicevinduer
- Robust driftssetup
  - Dimensionering
  - Kapacitetsstyring
  - Skalering

Brokeren vil få support fra MitID-leverandøren



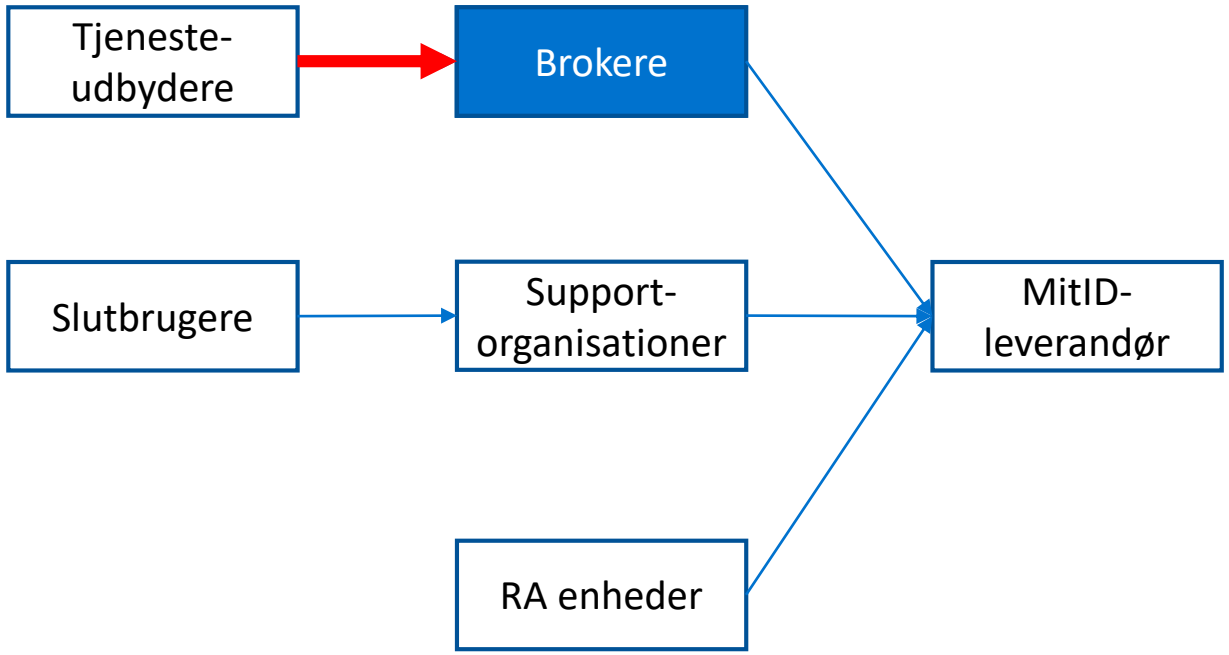
Brokerpakke

- Codex og UX scheme
- Dokumentation
- Implementeringsvejledning
- Referenceimplementering
- Kodeeksempler
- Testsystem og testdata

Teknisk support

- Servicedesk og ITSM vil være indgang

Forventninger til brokerens support til TU



Brokere skal supportere tjenesteudbydere

- Der forventes et serviceniveau, som afspejler MitID-leverandørens

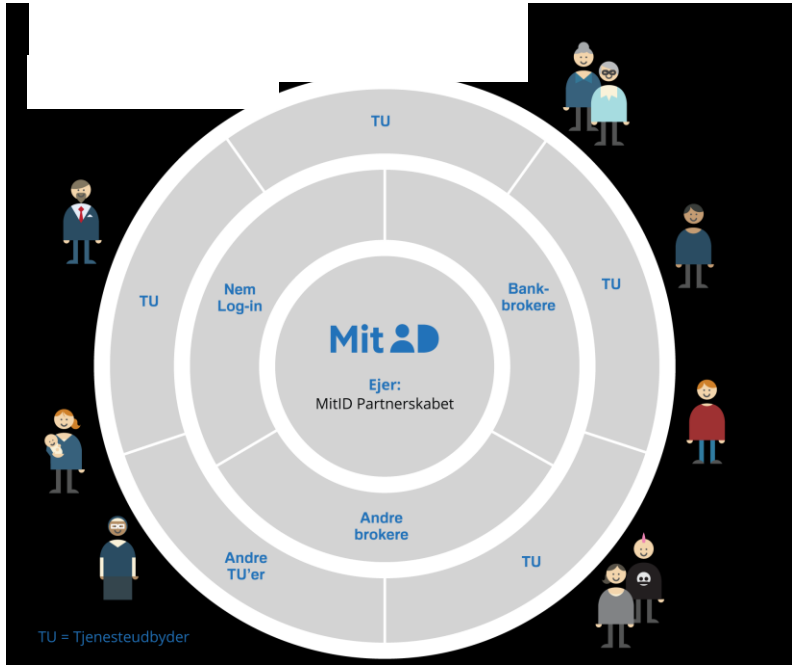
MitID-leverandørens serviceniveau

- Service desk for teknisk support
- ITSM stilles til rådighed
- Åbningstid hverdage kl. 05-20
- Besvarelse af henvendelser inden for 2 minutter
- Løsningstid < 3 timer

Sikkerhed

Broker er vigtig for brugeroplevelsen:

- Trygt
- Genkendeligt
- Effektivt i brug
- Tilgængeligt



MitID-leverandøren står på mål for sikkerheden

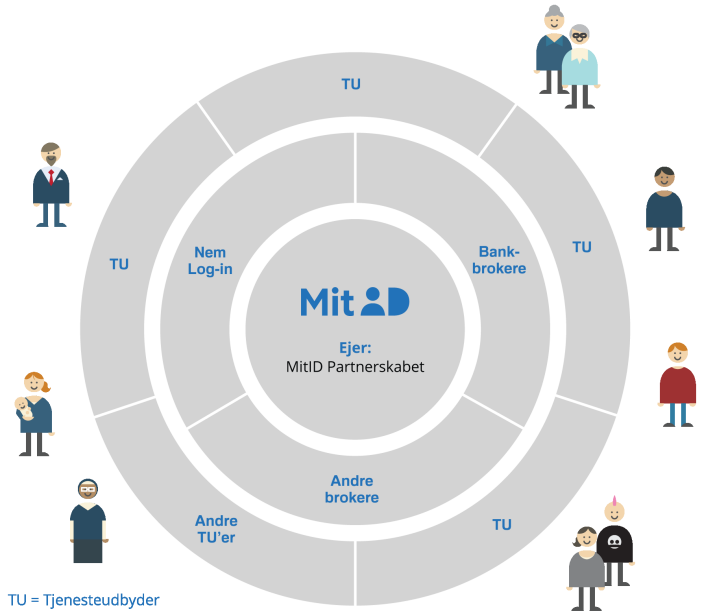
- Anvender en systematisk proces for gennemgang af risici og sårbarheder jf. ISO27001
- Evaluerer og optimerer kontinuerligt MitID's sikkerhed
  - Fysisk sikkerhed
  - Sikkerhed i infrastrukturen
  - Sikker softwareudvikling
- Overvåger MitID, drifts- og sikkerhedsmæssigt
- Indsamler efterretninger om aktuelle trusler
- Håndterer alle potentielle trusler til enhver tid

Omfatter også brokeren

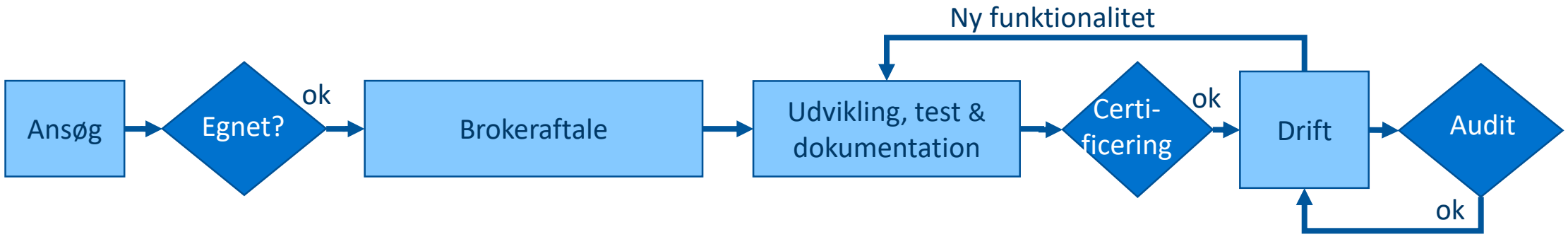
Proces for at blive broker

Broker er vigtig for brugeroplevelsen:

- Trygt
- Genkendeligt
- Effektivt i brug
- Tilgængeligt



Proces for brokere



Grundlag for certificering af brokere

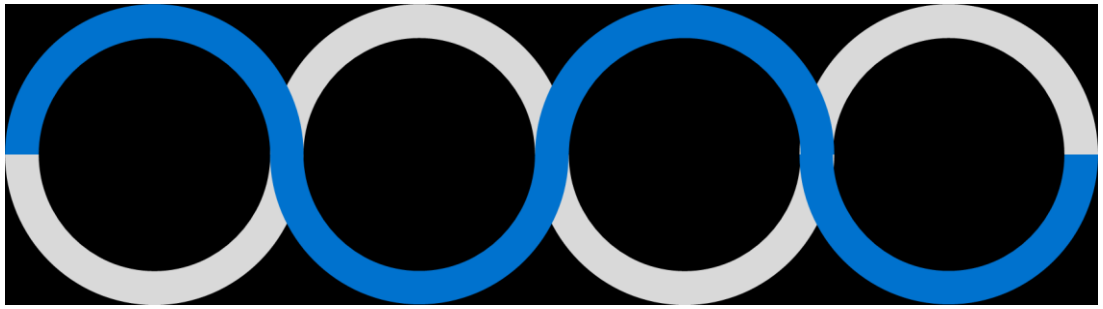
Sikkerhedskrav – Codex

Regulering af sikkerhedsaspekter for brokere:

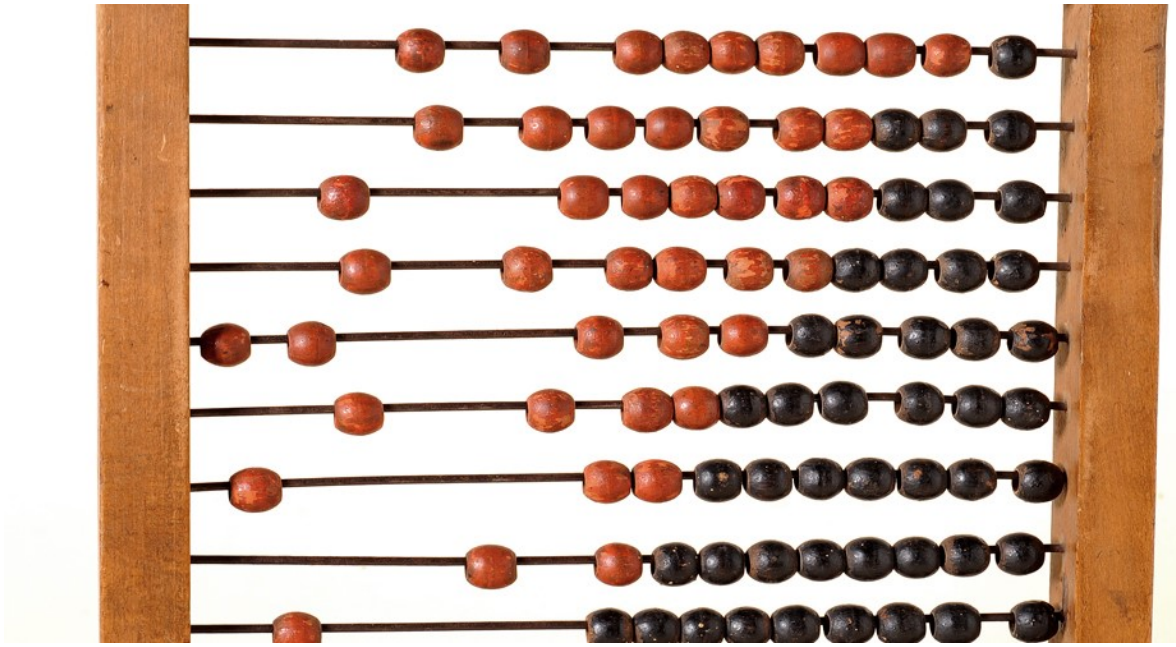
1. Basiscertificering:
   Informationssikkerhed
2. Integration:
   Brokerens integration til MitID for hver anvendelsesmodel

UX Scheme

- Sikrer slutbrugers oplevelse af MitID på tværs af løsninger
- Krav til UX design for autentifikation, uafhængigt af anvendelsesmodel



Betaling



Principper for MitID-priser i forhold til brokere

- Brokere betaler en transaktionspris til MitID
- Samme pris for alle brokere
- Prisen er pr. transaktion (autentifikationsanmodning)
- Prisen består af
  - Autentifikationsanmodningspris (AAP)
  - Tillægspris for kerneklient
- Transaktionsprisen afhænger af den samlede transaktionsmængde i MitID
- Teknisk support er inkluderet (inden for rimelighedens grænser)

Fakturering

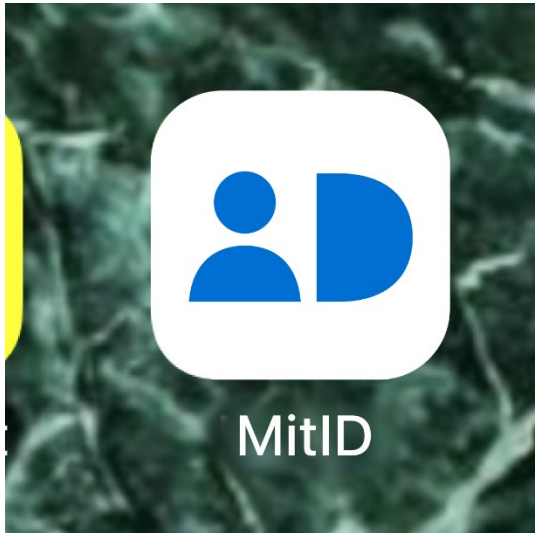
Dette bilag er et forenklet fakturaeksempel og indeholder ikke alle vederlagselementer, der skal faktureres.

Fakturaeksempel

Månedlig opkrævning til broker (Illustrativt eksempel)	Antal autentifkationsan modninger	Pris per enhed	Pris (t.kr.)
Samlet fakturering til broker i indeværende måned (maj måned)			-
Pris for transaktioner	-		-
Opgørelse af transaktioner per tjenesteudbyder			
Tjenesteudbyder		-	-
Udviklingspris		-	-
AAP		-	-
Tjenesteudbyder		-	-
Udviklingspris		-	-
AAP		-	-
Forventninger til efterregulering			
Forventet efterregulering for månedfaktura på baggrund af nyt forecast	-	-	-
Forventet samlet årlig efterregulering på tværs af alle Brokere beregnet på baggrund af fremskrivning af hidtidigt forbrug	-	-	-

MitID loginmidler
(udover bruger-id og adgangskode)

MitID App



MitID Kodeviser

MitID Chip

Betalbart

MitID Kodeoplæser/Lydkode

Øvrige driftsydelser

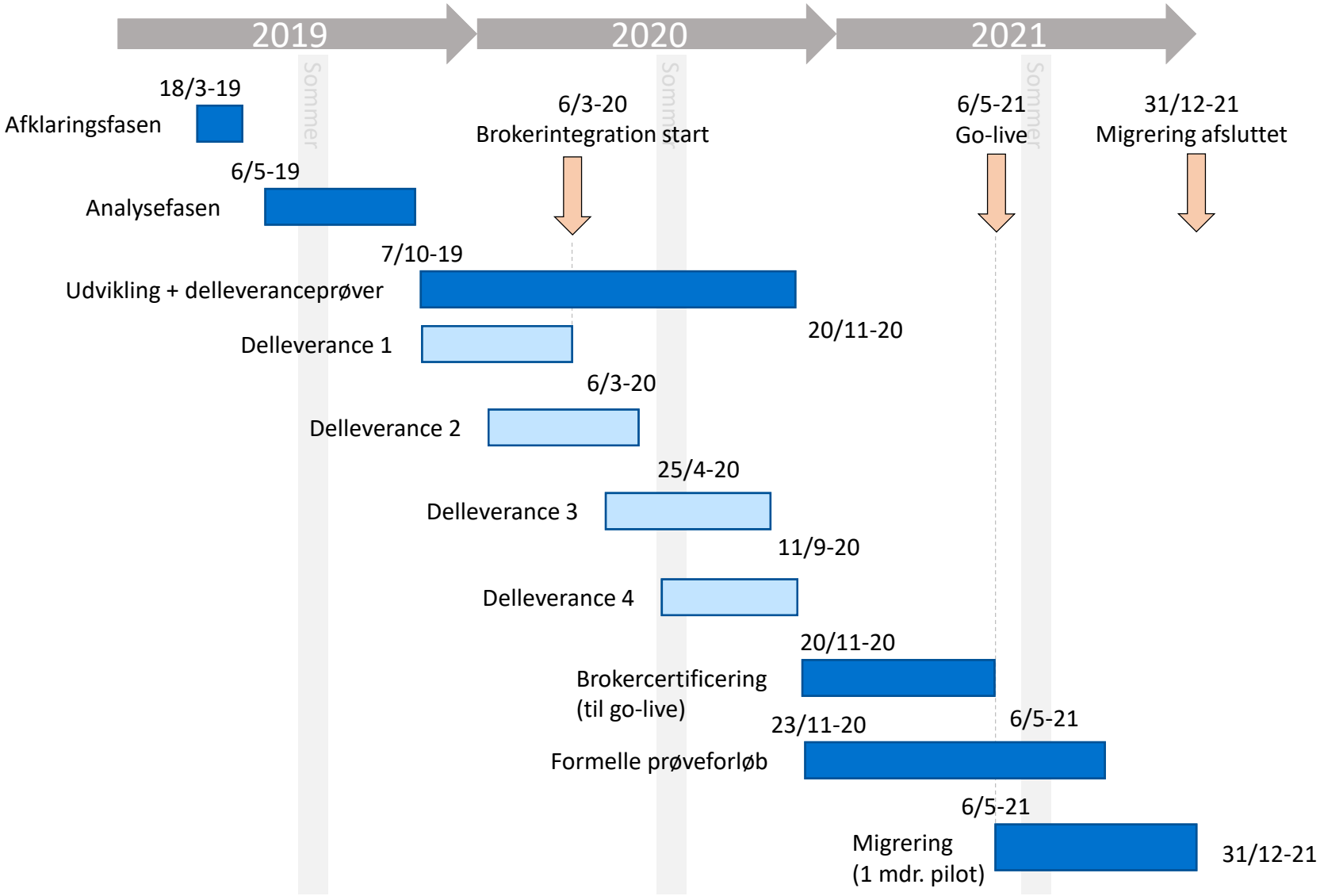
- Der vil være en udgift til certificering

Udviklingspris

- Tjenesteudbydere vil forventeligt blive opkrævet en udviklingspris pr. transaktion for deres forholdsvise forbrug af MitID

MitID's tidsplan

MitID's tidsplan – det store perspektiv



Næste skridt for interesserede brokere

Stadig interesseret i at blive broker?

- Nyt møde for brokere om priser
  - Vi indkalder snarest
- Dialog med tjenesteudbydere
  - Vi afholder møde for tjenesteudbydere ultimo 2019
  - I kan få en stand
  - Vi hjælper gerne, fx ved at reviewe jeres materiale
- Tag endelig fat i os

Mere information

- Mitid.dk, digst.dk, fida.dk
- Implementeringssitet:
  digst.dk/it-loesninger/implementeringssite
- Nyhedsbrev om MitID og NemLog-in:
  digst.dk/nyheder/nyhedsbreve
- Eller skriv til mitid@digst.dk

Tak for i dag