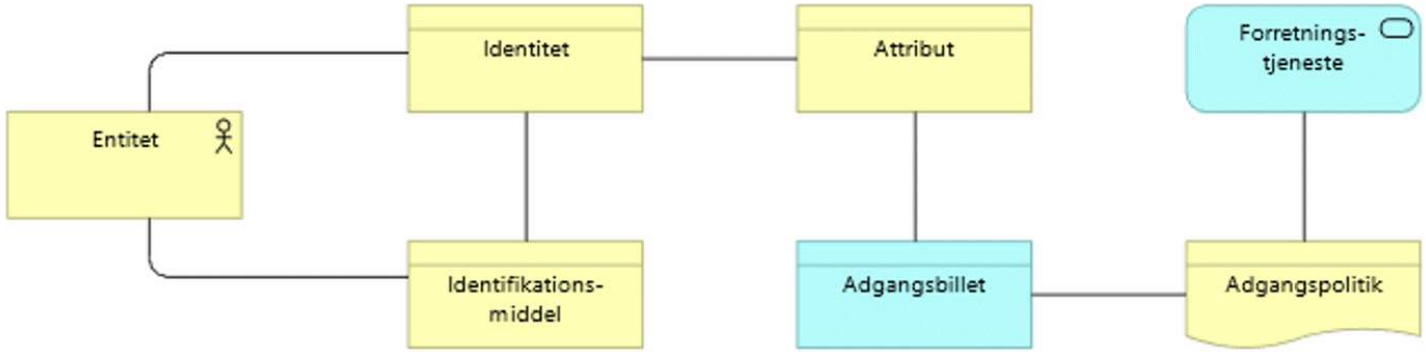
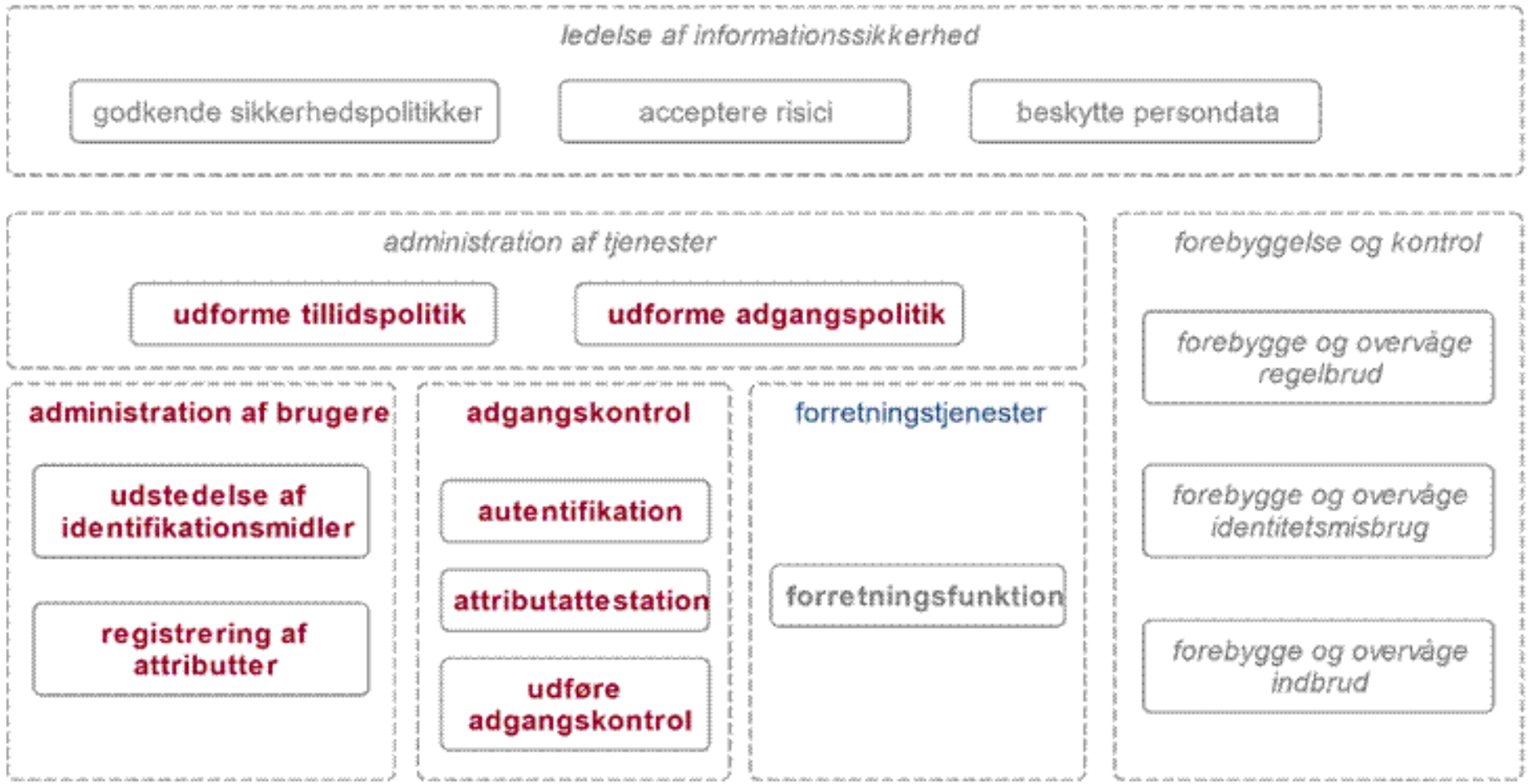
Arkitekturvinkler på
brugerstyring i kommunerne

Hvad er brugerstyring?

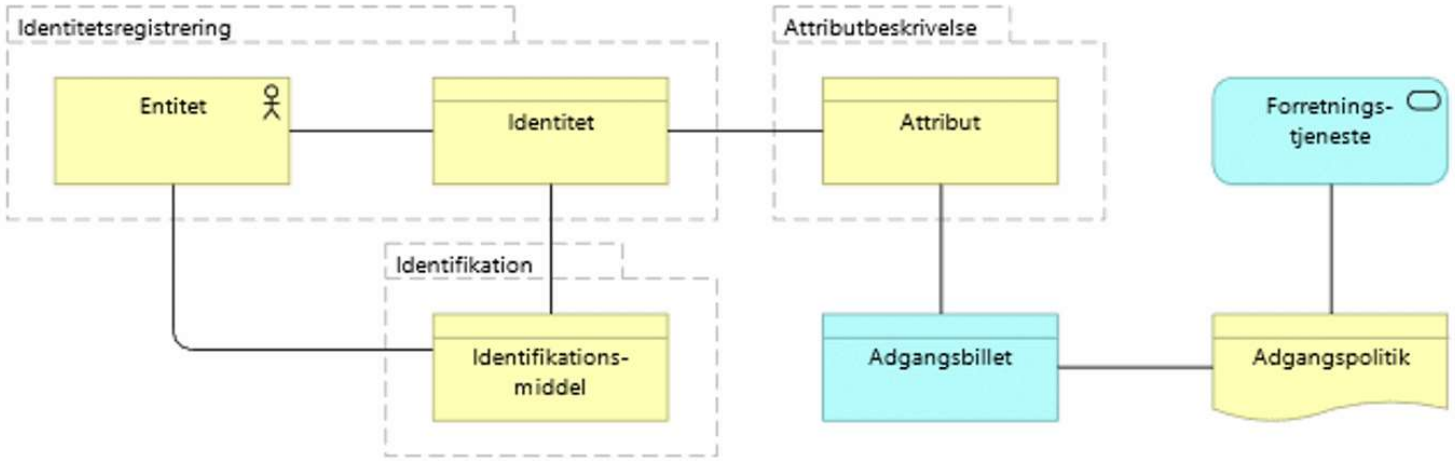
- Administration og kontrol af **brugere, identifikationsmidler og adgang til forretningstjenester**.
- Det sikres, at de rette brugere og systemer får adgang til de rette it-systemer og data, og at alle andre afvises.
- Brugerstyring er en **forudsætning for it-sikkerhed**




ledelse af informationssikkerhed
godkende sikkerhedspolitikker
acceptere risici
beskytte persondata
administration af tjenester
udforme tillidspolitik
udforme adgangspolitik
forebyggelse og kontrol
forebygge og overvåge regelbrud
forebygge og overvåge identitetsmisbrug
forebygge og overvåge indbrud
administration af brugere
udstedelse af identifikationsmidler
registrering af attributter
adgangskontrol
autentifikation
attributattestation
udføre adgangskontrol
forretningstjenester
forretningsfunktion

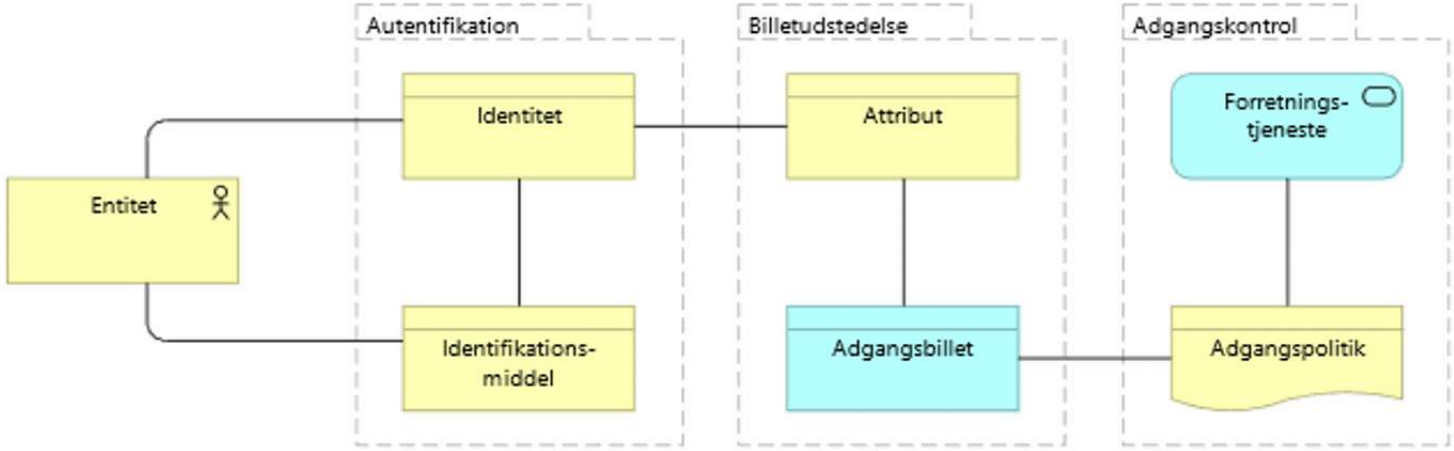
Brugerstyringsprocesser

- **Administration**
  - Registrering og udstedelse af identifikationsmidler
  - Registrering af attributter



Brugerstyringsprocesser

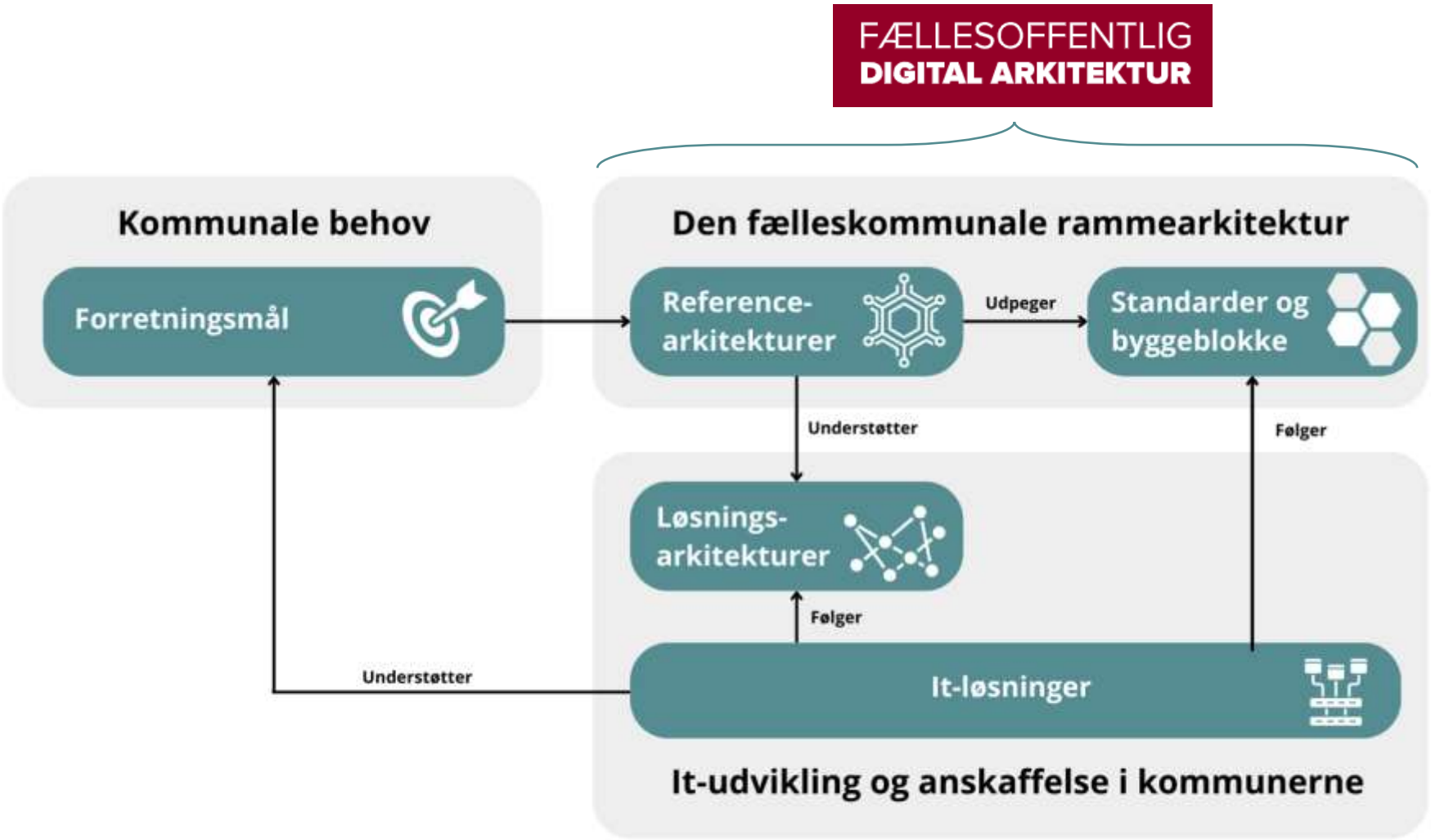
- **Adgangskontrol**
  - Autentifikation
  - Attributattestation
  - Udførelse af adgangskontrol




Sammenhængende it
Byg til genbrug og forandring
Flere leverandører
Data som værdiskabende ressource
Tillid og sikkerhed

Tillid og sikkerhed

- Kommunale it-løsninger bygges således, at borgere og virksomheder har tillid til, at deres data er korrekte, **og at de behandles og opbevares, så de er sikret mod misbrug og utilsigtet adgang eller anvendelse. Data beskyttes ensartet på tværs af it-løsninger.**


FÆLLESOFFENTLIG
DIGITAL ARKITEKTUR
Kommunale behov
Forretningsmål
Den fælleskommunale rammearkitektur
Reference-arkitekturer
Udpeger
Standarder og byggeblokke
Understøtter
Følger
Løsnings-arkitekturer
Følger
Understøtter
It-løsninger
It-udvikling og anskaffelse i kommunerne

Fællesoffentlig strategi

- Med henblik på at støtte myndighederne i at udvikle it-løsninger, der øger myndighederne **evne til at sikre fortrolighed, integritet, tilgængelighed og robusthed** af systemer og -tjenester,
- udarbejdes en **fællesoffentlig arkitektur for informationssikkerhed** bestående af principper, standarder, fælleskomponenter og vejledninger.

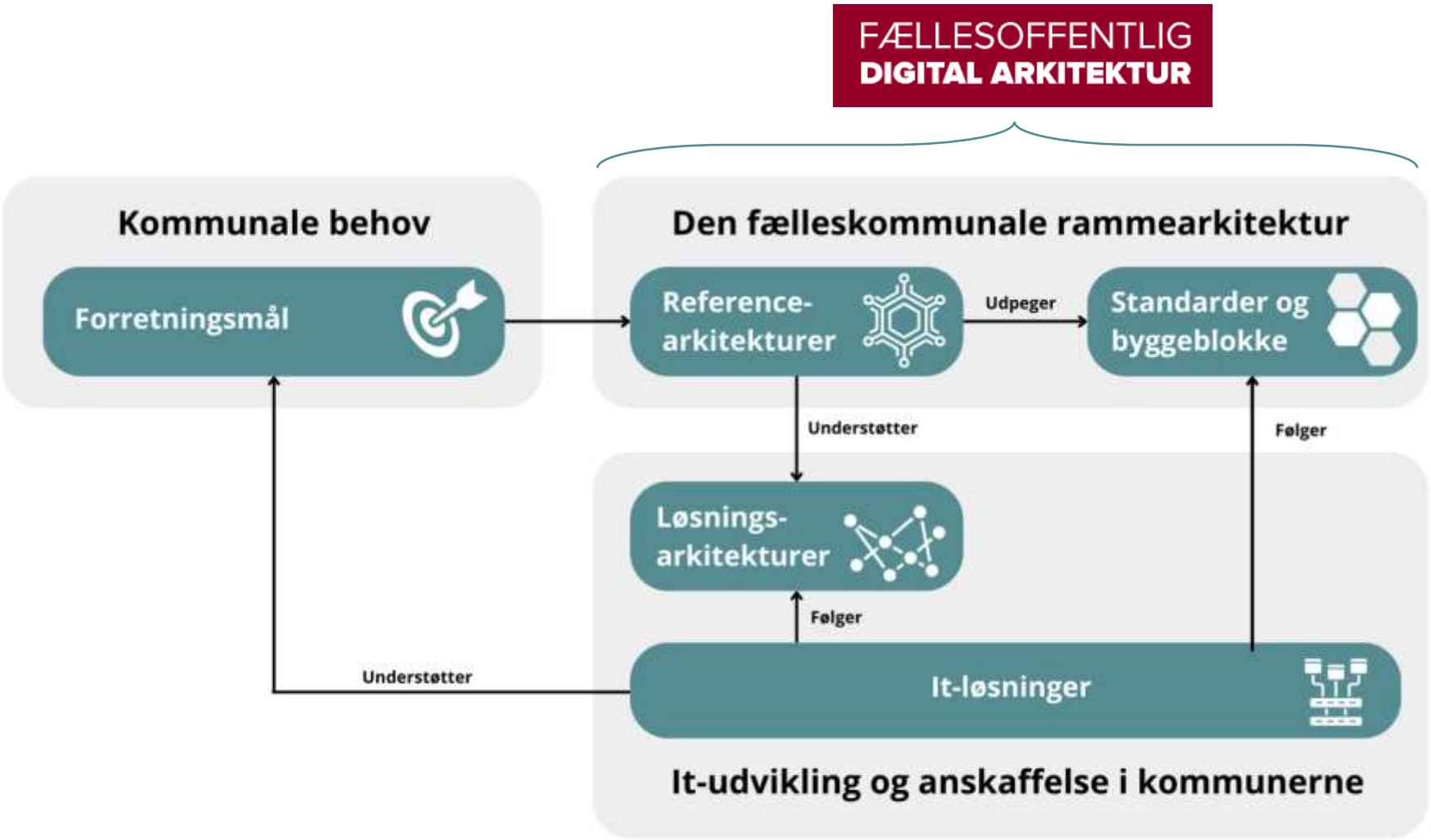
Referencearkitektur for brugerstyring

- Der er de senere år etableret **en række fælles løsninger for brugerstyring** i samarbejde mellem forskellige offentlige parter.
- Disse løsninger sikrer **sammenhæng inden for afgrænsede områder**, men der er fortsat mulighed for at forbedre den **overordnede fællesoffentlig digitale sammenhæng** i initiativer og løsninger.
- Formålet med referencearkitekturen er således at målrette og strukturere brugerstyringen i det offentlige for at skabe sammenhængende, effektive, sikre og brugervenlige løsninger **på tværs af domæner, nationalt og transnationalt**.

https://rammearkitektur.kl.dk/indhold-i-rammearkitekturen/referencearkitekturer/faellesoffentlige-referencearkitekturer/brugerstyring

Principper for brugerstyring

1. Brugerne oplever en **relevant og sammenhængende** adgangsstyring.
2. Brugerstyringsløsninger respekterer brugernes **privatliv**.
3. Tjenesteudbyder har ansvaret for at **adgangspolitikken håndhæves**.
4. Brugerstyring er **adskilt fra forretningstjenester**.
5. Brugerstyring realiseres via **løst koblede og standardiserede tillidstjenester**.
6. Tjenesteudbydere indgår i **føderationer**.


FÆLLESOFFENTLIG
DIGITAL ARKITEKTUR
Kommunale behov
Forretningsmål
Den fælleskommunale rammearkitektur
Reference-arkitekturer
Udpeger
Standarder og byggeblokke
Understøtter
Følger
Løsnings-arkitekturer
Følger
Understøtter
It-løsninger
It-udvikling og anskaffelse i kommunerne

Rammearkitekturens sikkerhedsmodel

Fælleskommunal Adgangsstyring for brugere håndterer både, hvilke medarbejdere der kan logge ind i et it-system, og hvilken adgang medarbejderne får til it-systemets data og funktionalitet.

Fælleskommunal Adgangsstyring for brugere er baseret på:

1. en **fødereret model**, der betyder, at brugere oprettes, tildeles adgang og autentificeres lokalt hos de enkelte kommuner
2. fællesoffentlige **standarder** i overensstemmelse med princip 8 for Rammearkitekturens sikkerhedsmodel, så det bliver muligt at *føderere* med **brugerstyringsløsninger på andre områder**.

Beskrivelse af sikkerhedsmodellen i Rammearkitekturen s. 4.

Rammearkitekturens sikkerhedsmodel

”Man kan på sigt også forestille sig, at nogle kommuner vil indkøbe **systemer til eget brug, der vil benytte rammearkitekturens model for adgangsstyring**. Disse systemer vil så også være brugervendte systemer i rammearkitekturens adgangsstyringsmodel.”

Rammearkitekturens sikkerhedsmodel

Fælleskommunal Adgangsstyring er udviklet i overensstemmelse med **princip 4 i fællesoffentlig referencearkitektur for brugerstyring**, der anbefaler, at

- brugerstyring er adskilt fra forretningstjenester
- og at etablering af brugerstyring i en selvstændig løsning er en forudsætning for, at medarbejdere kan opleve ***sammenhængende, effektive og sikre*** forløb på tværs af systemer.

Tekniske minimumsstandarder i kommuner 2023

Tekniske minimumsstandarder

- S6: **Administrative rettigheder** for brugere tildeles kun tidsbegrænset og med veldokumenterede behov.
- S10: **Autentifikation** til kommunens systemer over internettet skal anvende to-faktorlogin.
- S11: Alle platforme, hvor man **logger på med kommunens loginmidler**, må kun anvendes udenfor kommunens lokale netværk, hvis dette foregår vha. to-faktorlogin eller via en krypteret forbindelse til kommunens netværk.
- K7: Der skal være **adgangskontrol for fysisk adgang** til rum med følsomme oplysninger eller udstyr såsom servere, netværksudstyr, der håndterer intern trafik mv.
- K8: **Ekstern adgang til fx konsulenter** skal tildeles tidsbegrænset og kun til og med opgavens ophør. Den eksterne adgang skal kun inkludere adgang til relevante systemer til den konkrete opgaveløsning.
- K9: **Passwords** skal udformes, opdateres og opbevares i overensstemmelse med Center for Cybersikkerheds anbefalinger.

Gevinster

Det sikrer sikkerhed, privatliv og tillid, sammenhæng og effektivitet, fordi:

- Det giver større **brugervenlighed**, når samme digitale identitet kan benyttes til flere tjenester, med mulighed for adgangsstyring på tværs af løsninger og domæner.
- **Brugeradministrationen effektiviseres**, idet brugerne ikke skal vedligeholdes flere steder og det øger sandsynligheden for korrekt oprydning i brugere og rettigheder.
- Det giver mindre overlap og dublering, når brugerstyring kan anvendes til mange tjenester, hvilket **sparer penge ved udvikling og drift** af applikationerne og resulterer i **mere effektive løsninger**.
- **Sikkerheden øges** når brugerstyring foregår i dedikerede tjenester, hvor fokus er på brugerstyring.

Målbillede for sammenhængende brugerstyring

Problem

Når kommunale medarbejdere bruger it-systemer i hverdagen, logger de på via en af flere brugerstyringsløsninger.

- Føderationer sænker barren for at udbyde og anvende tjenester for tjenesteudbydere og kommuner inden for den enkelte føderation ved at udstille disse **fælles tjenester til brugerstyring**.
- Et stigende behov for **adgang på tværs af domæner og fagområder**, så brugervenligheden øges for medarbejderne, potentialer og besparelser realiseres, og sikkerheden øges på tværs.

Referencearkitektur for brugerstyring

- Endelig vurderes det, at der kan blive behov for **yderligere vejledning og standarder for kommunikation mellem føderationer**, når erfaringerne med interføderation udbredes et eksempel kunne være best practice for billetomveksling.

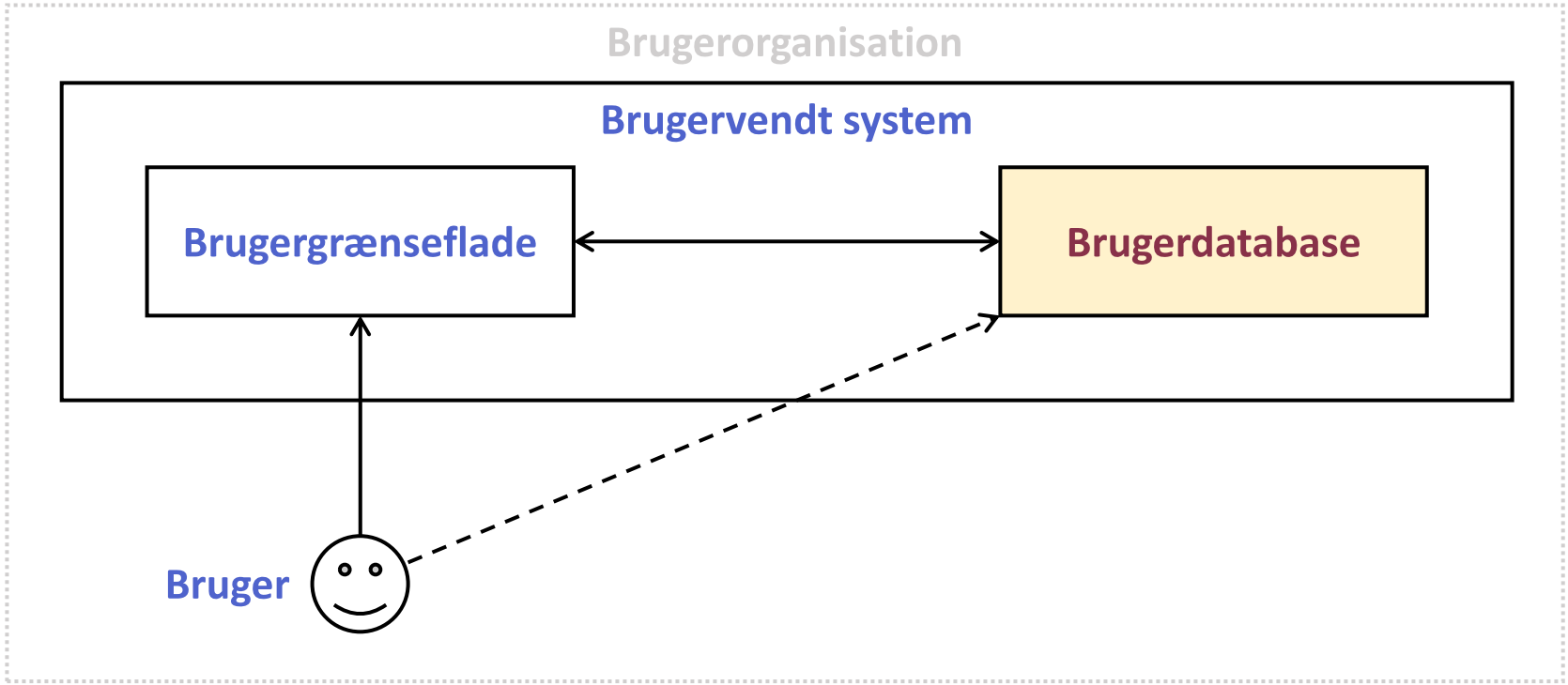
Fem mønstre for brugerstyring

1. Forretningstjeneste med egen autentifikationstjeneste
2. Delt, intern autentifikationstjeneste
3. Føderation med central autentifikationstjeneste
4. Fælles domænebroker for decentrale autentifikationstjenester
5. Interføderation mellem domæner

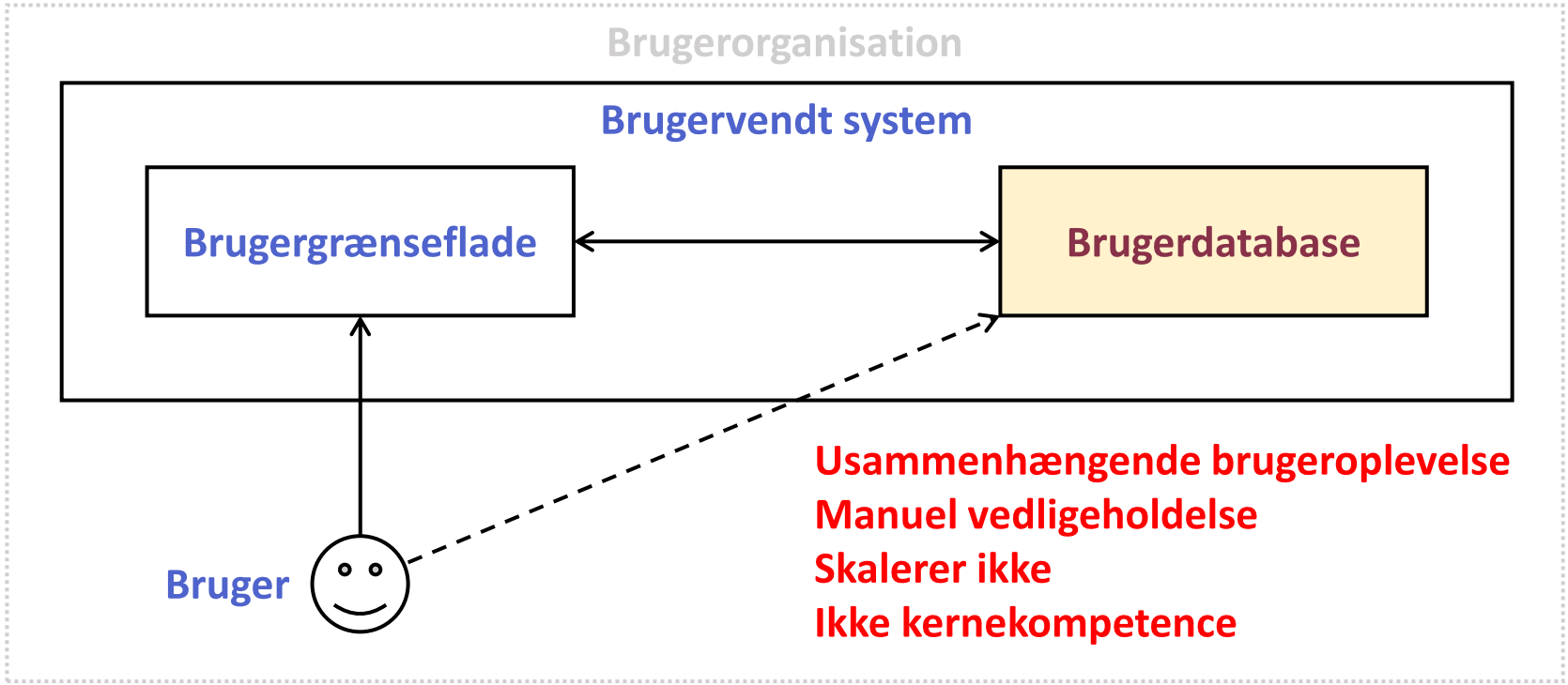
Fem mønstre for brugerstyring

1. ”Monolitten” – legacy
2. Funktionsadskillelse – inden for egen organisation
3. Fælles brugerstyring – fx MitID Erhverv
4. Broker på et domæne – Rammearkitekturens sikkerhedsmodel
5. Interføderation – sammenhængende brugerstyring på tværs

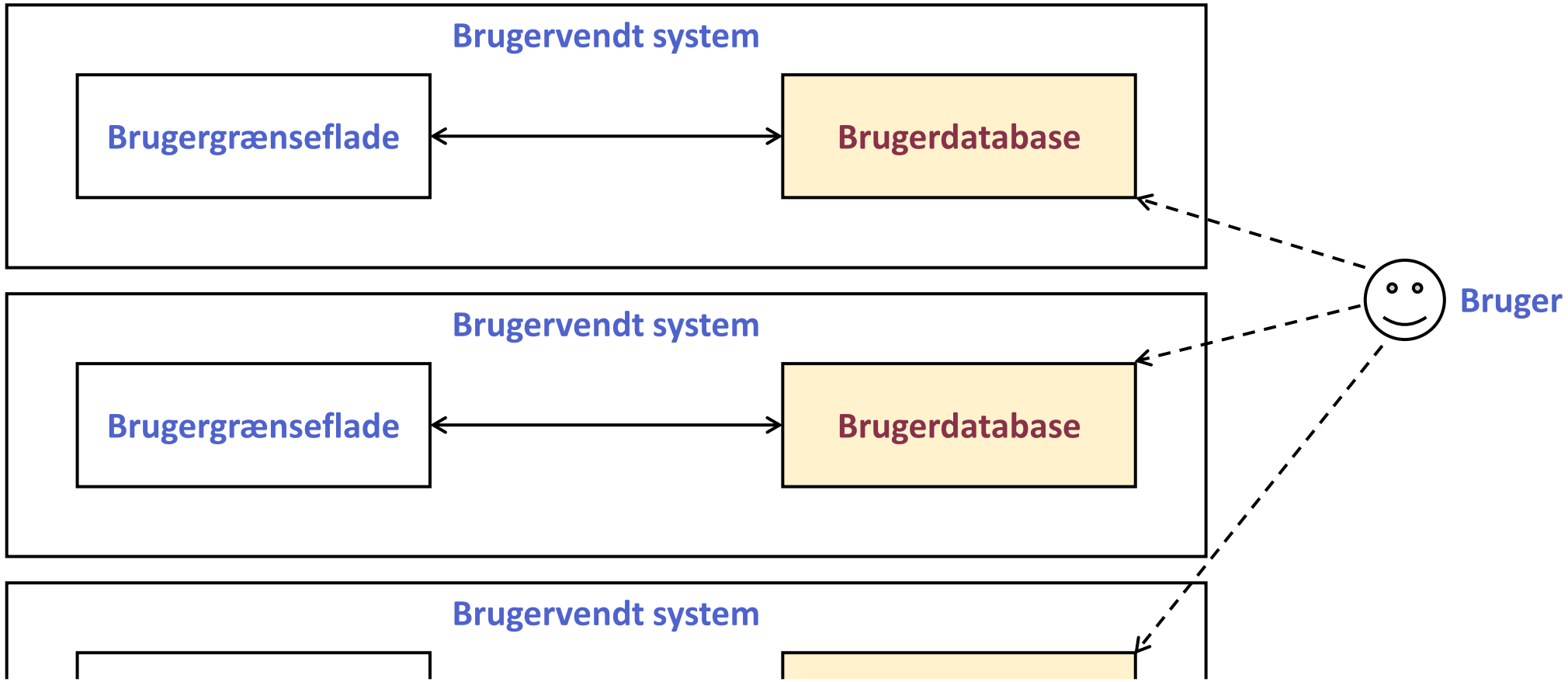
Mønster 1: Monolitisk arkitektur



Mønster 1: Monolitisk arkitektur

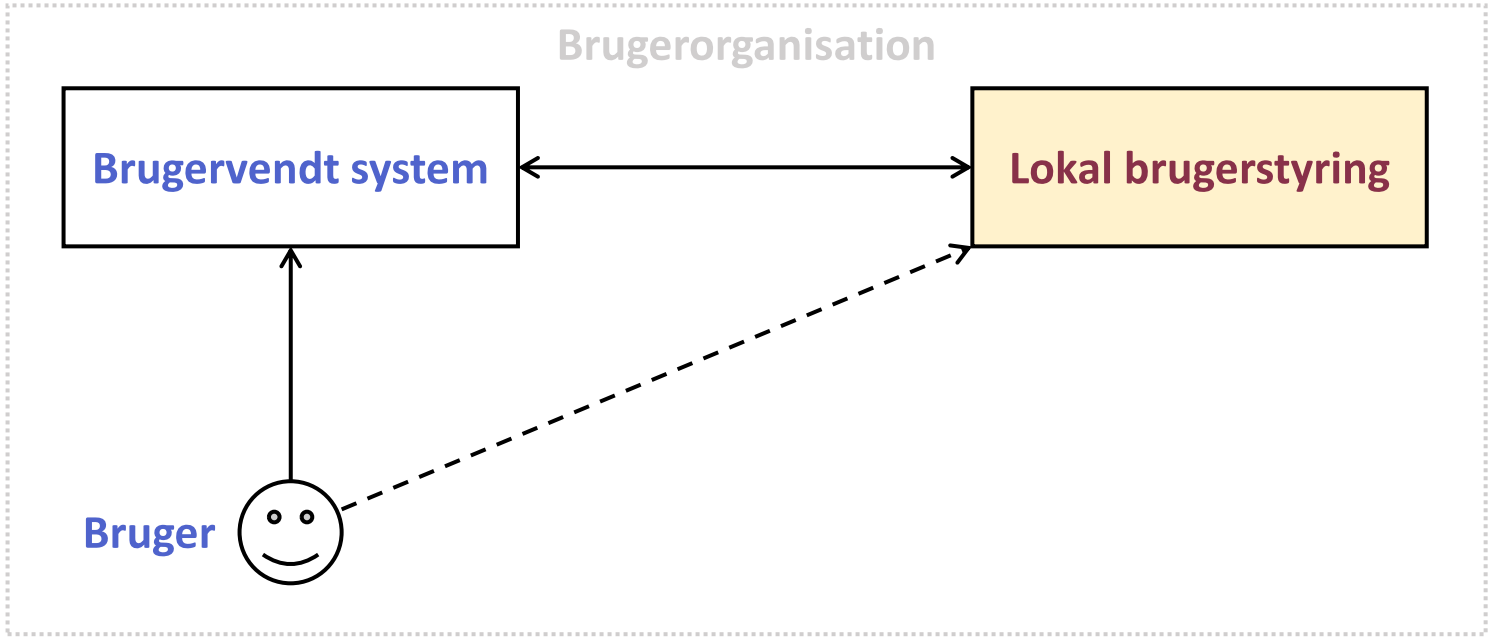


Mønster 1: Monolitisk arkitektur

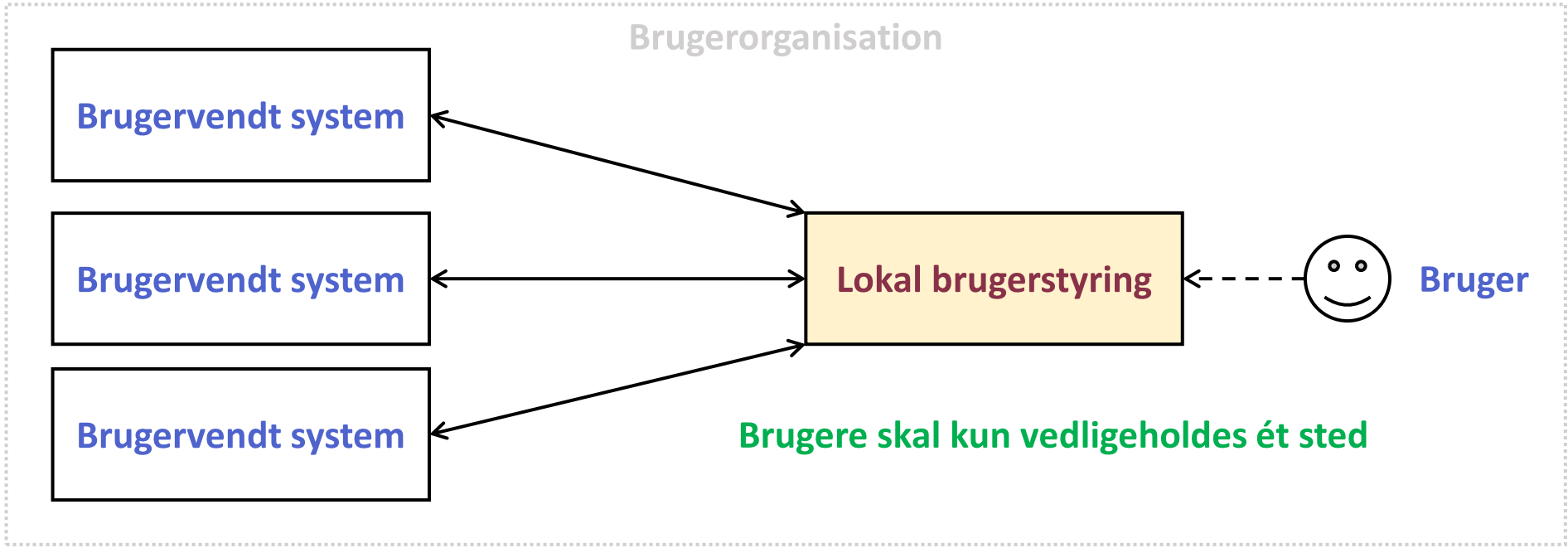


...

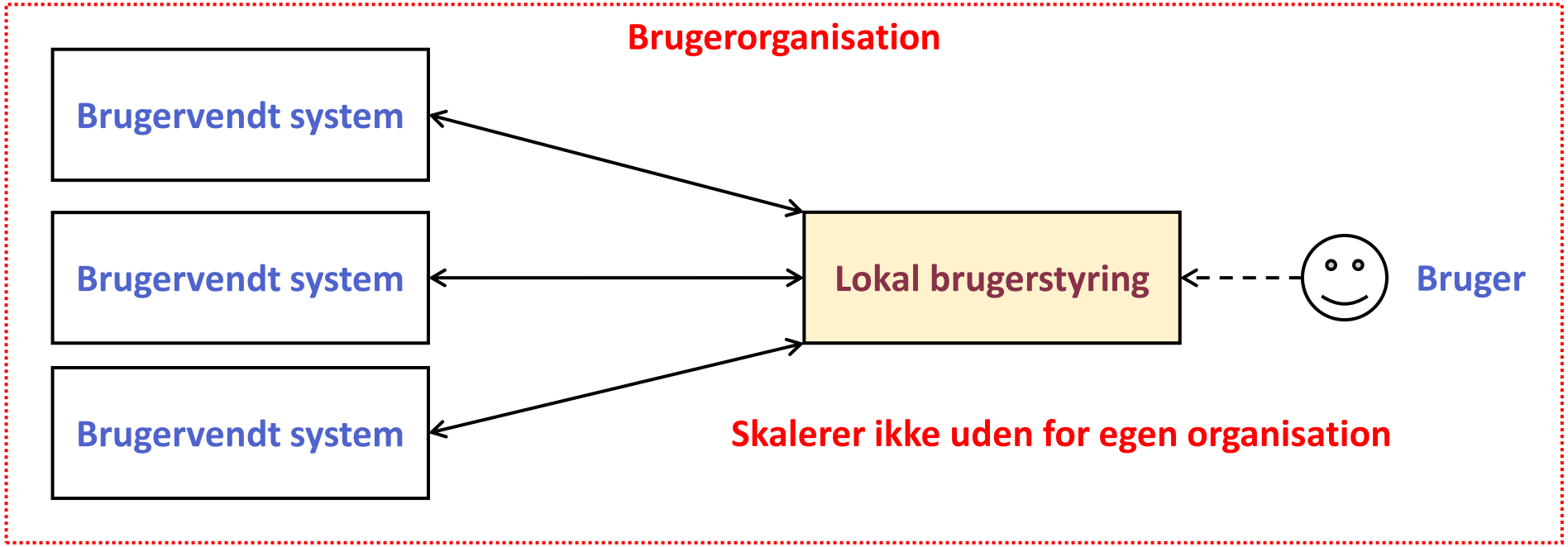
Mønster 2: Funktionsadskillelse



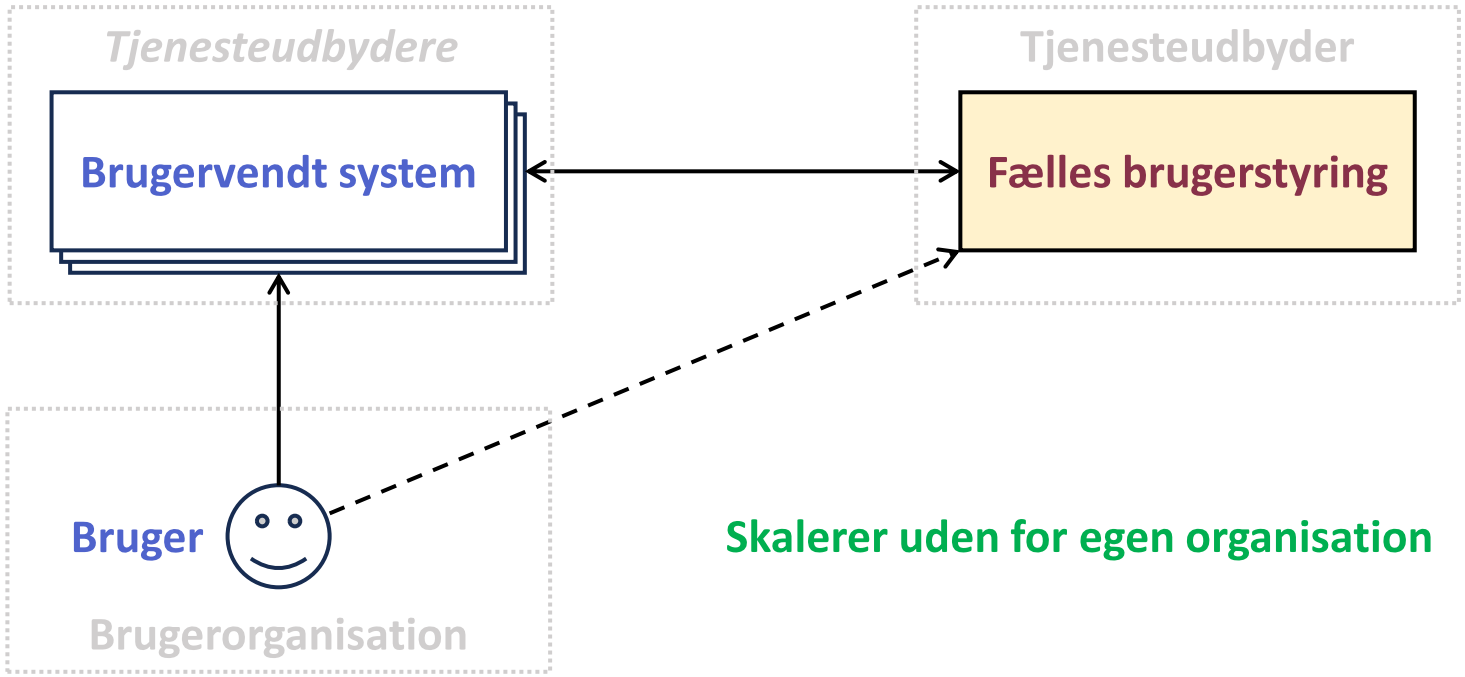
Mønster 2: Funktionsadskillelse



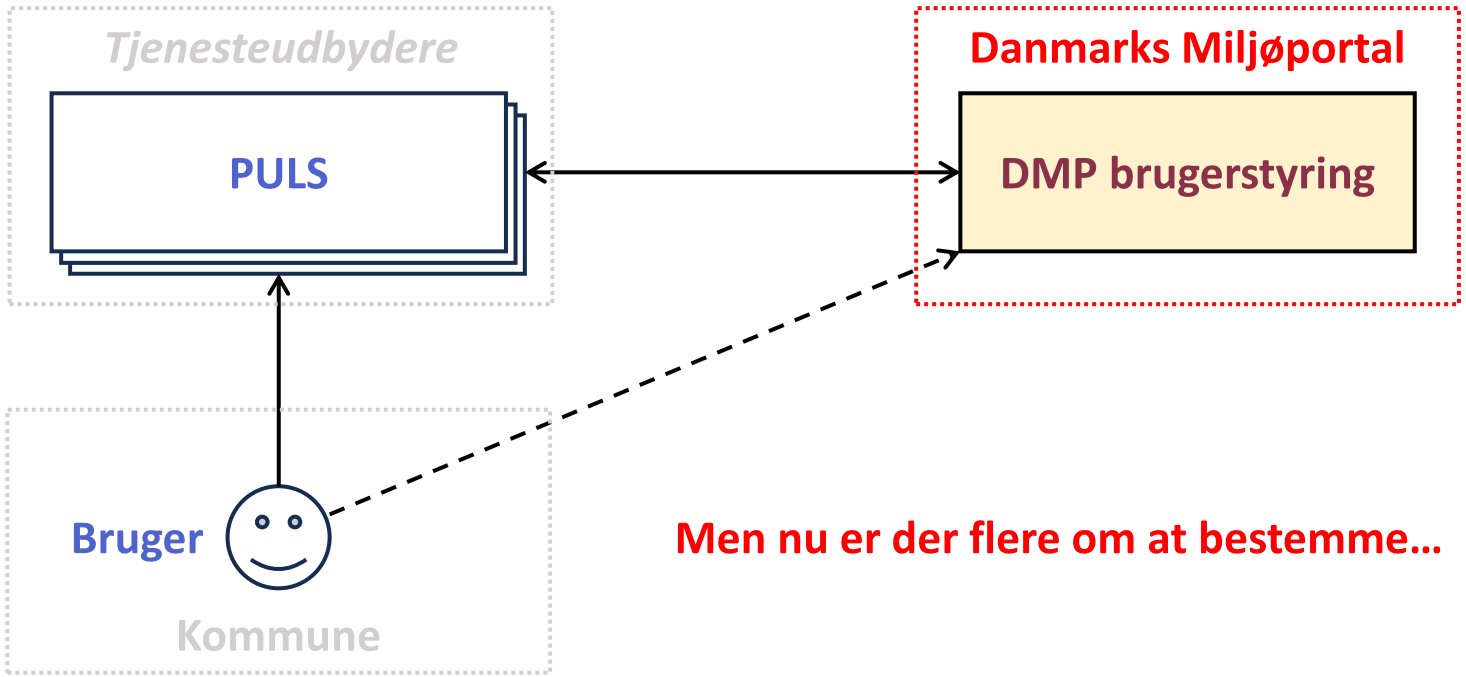
Mønster 2: Funktionsadskillelse



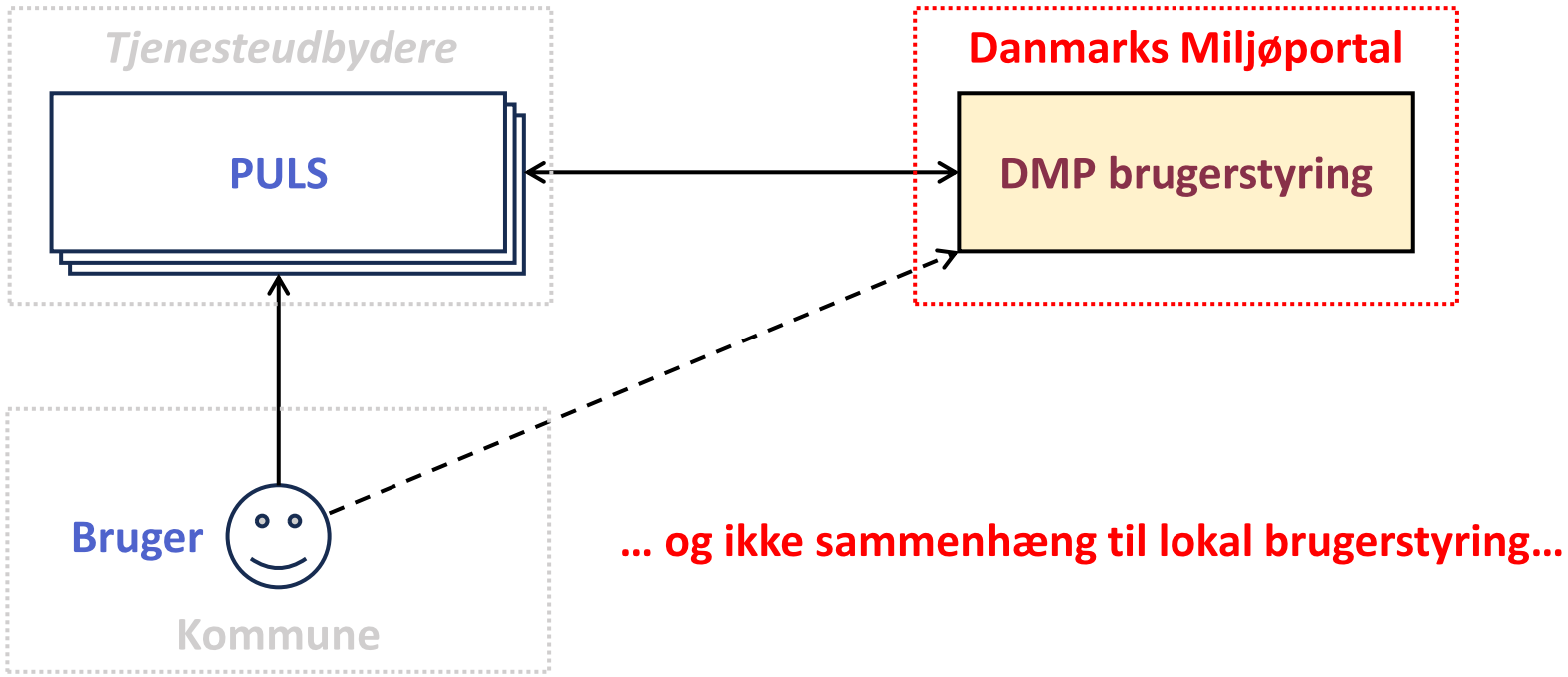
Mønster 3: Fælles brugerstyring



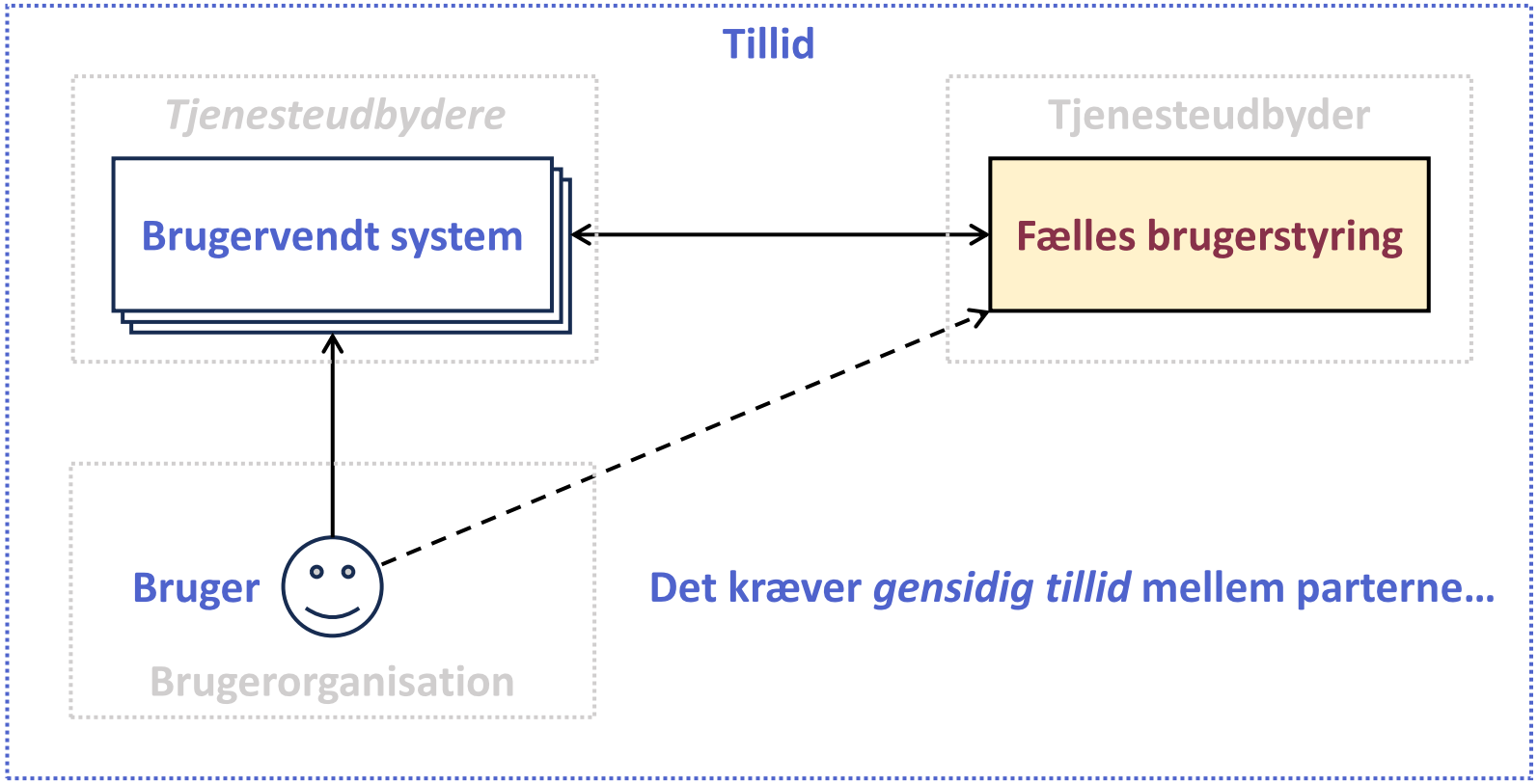
Mønster 3: Fx Danmarks Miljøportal



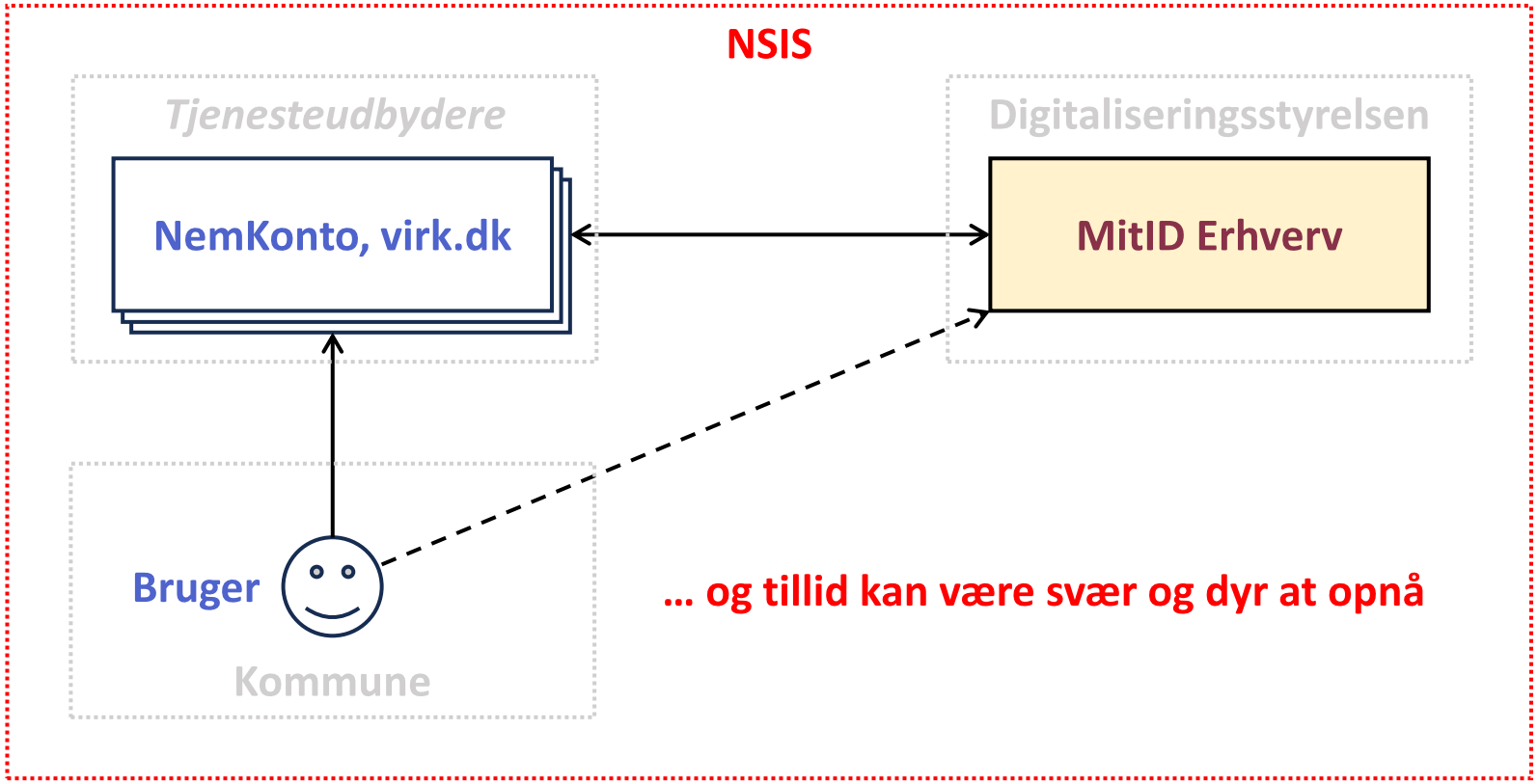
Mønster 3: Fx Danmarks Miljøportal



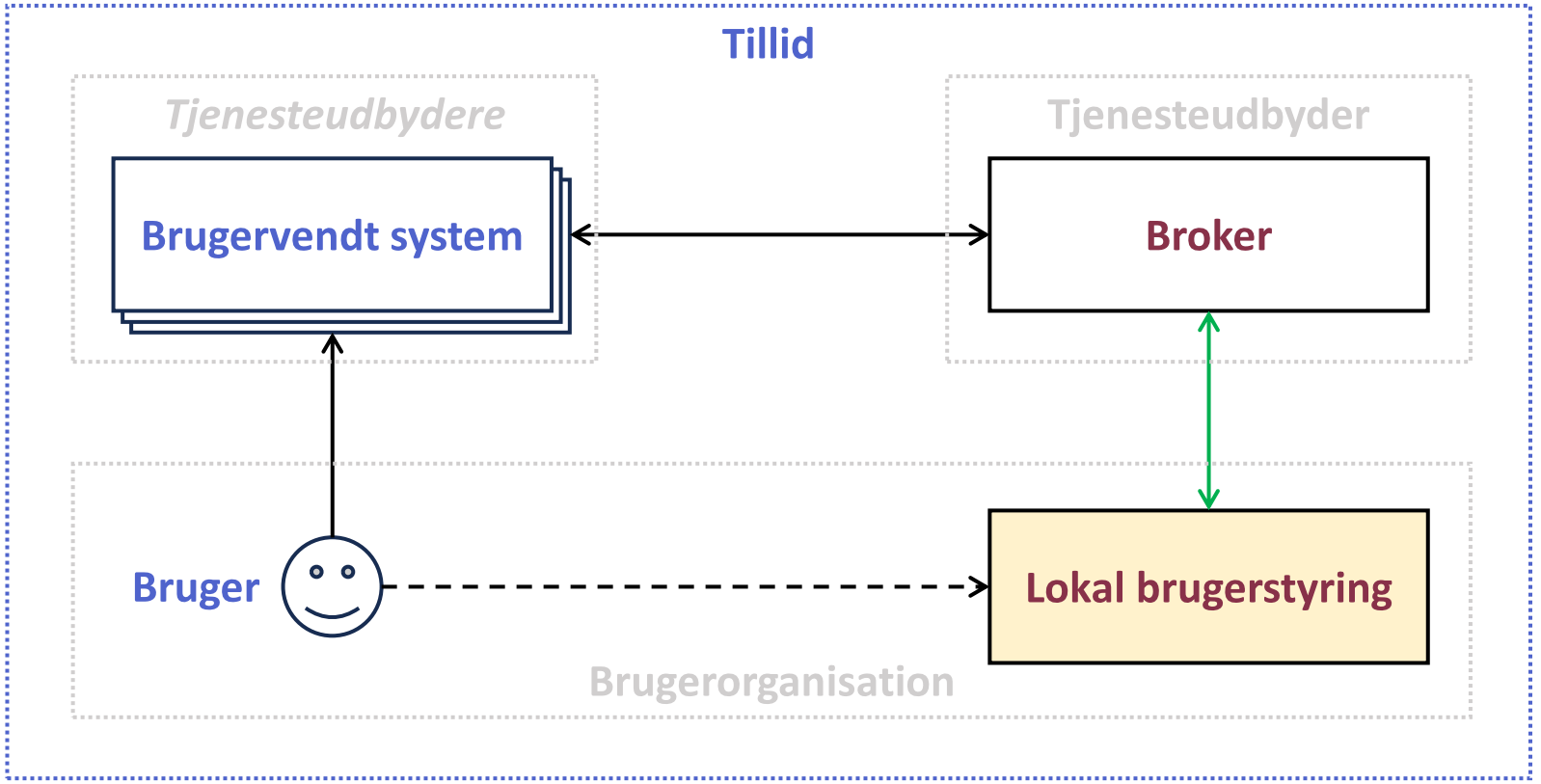
Mønster 3: Fælles brugerstyring



Mønster 3: Fx MitID Erhverv

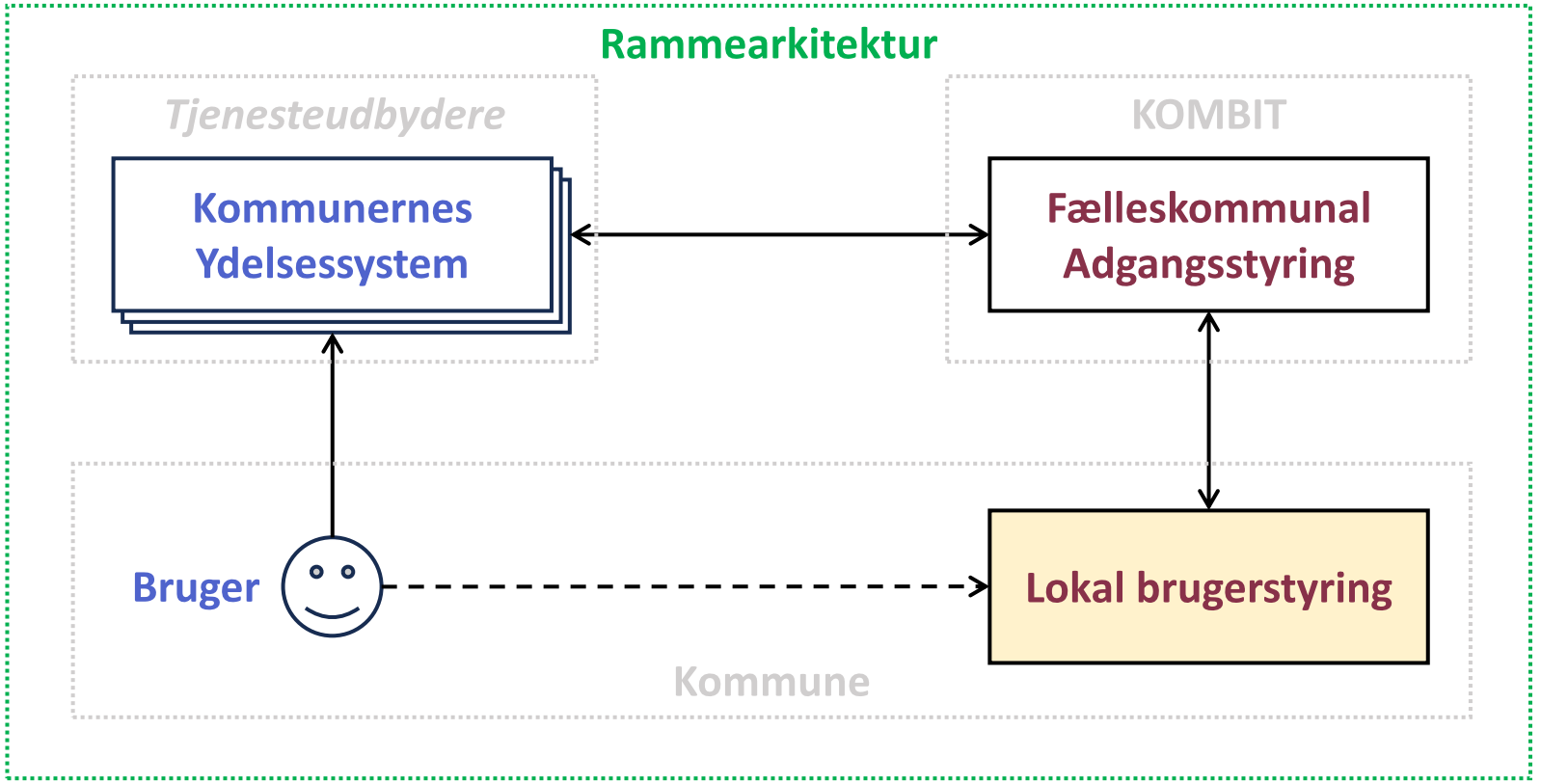


Mønster 4: Broker på et *domæne*



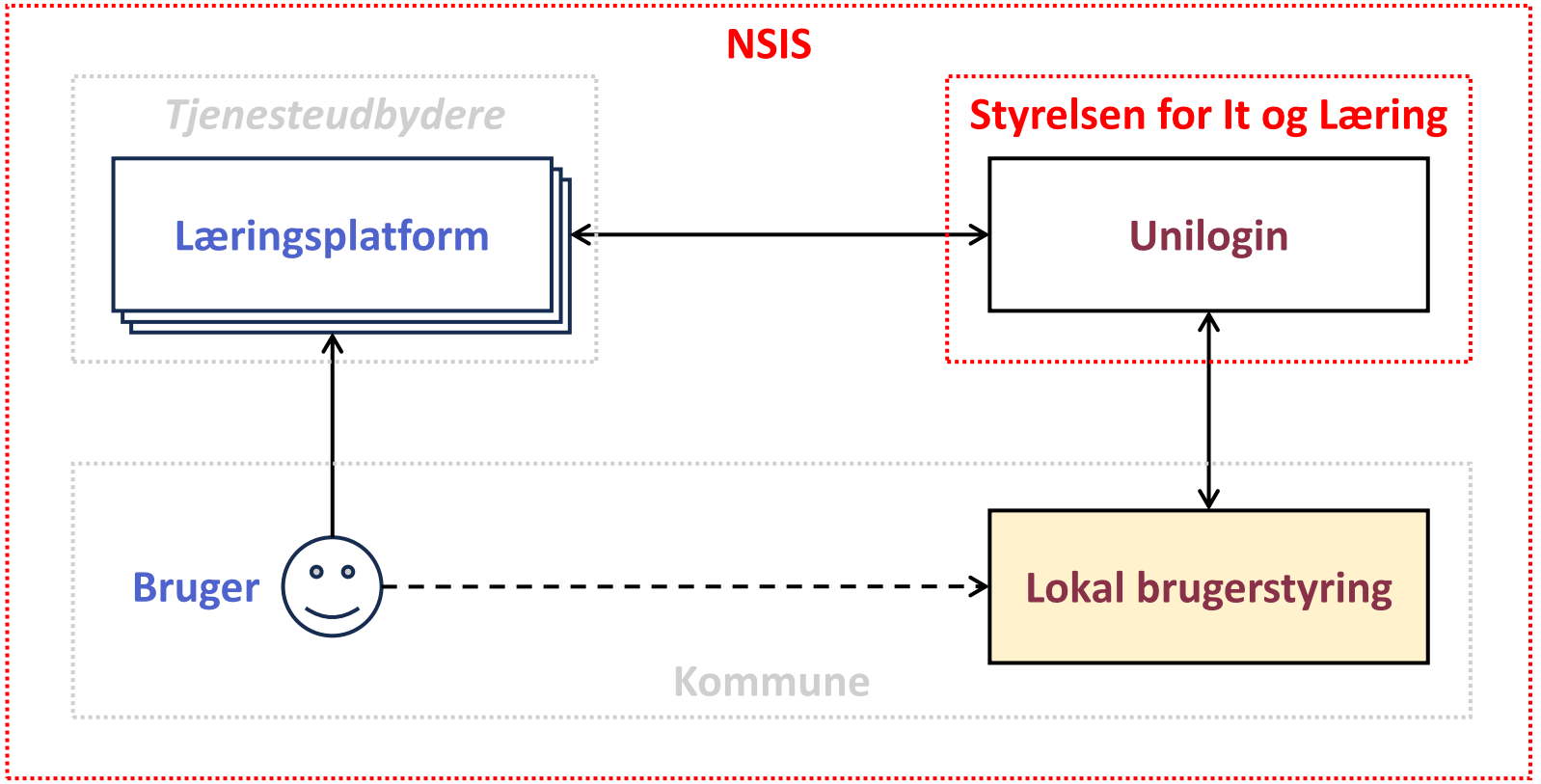
Der er skabt sammenhæng til den lokale brugerstyring…

Mønster 4: Fx FK Adgangsstyring



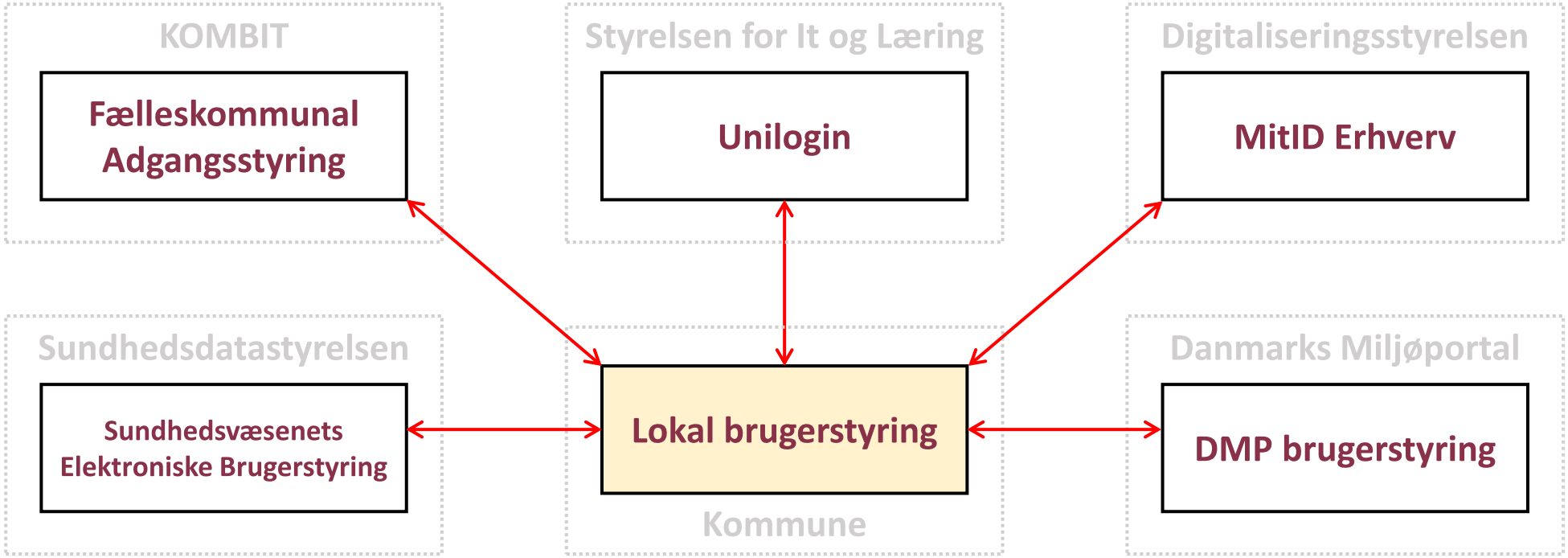
... og det er typisk nemmere at opnå tillid inden for domænet...

Mønster 4: Fx Unilogin

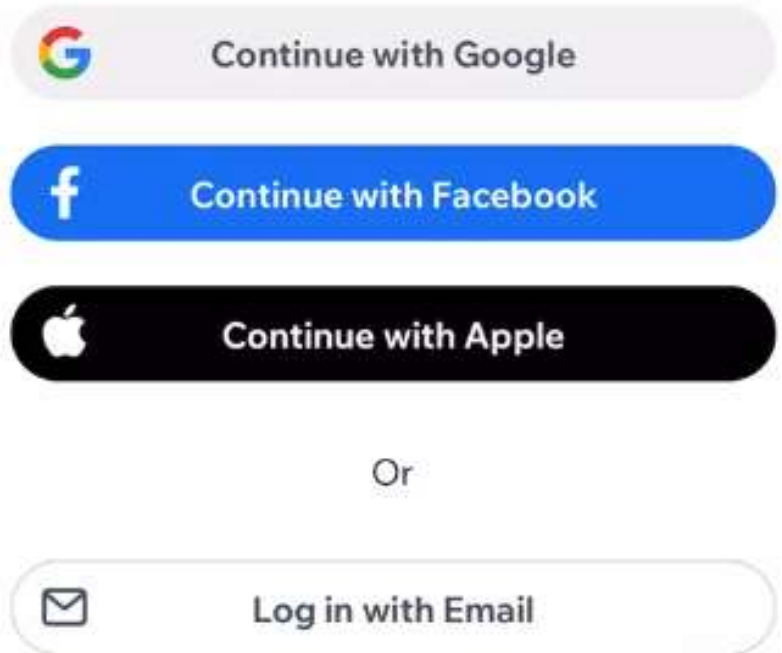


… men det kan stadig være et problem, at der er andre, der bestemmer…

Mønster 4: Eksempler på domæner



… og organisationen skal tilsluttes mange forskellige domænebrokere


Continue with Google
Continue with Facebook
Continue with Apple
Or
Log in with Email

Loginvælger

Unilogin

Seneste login

Københavns Kommune

Andre muligheder

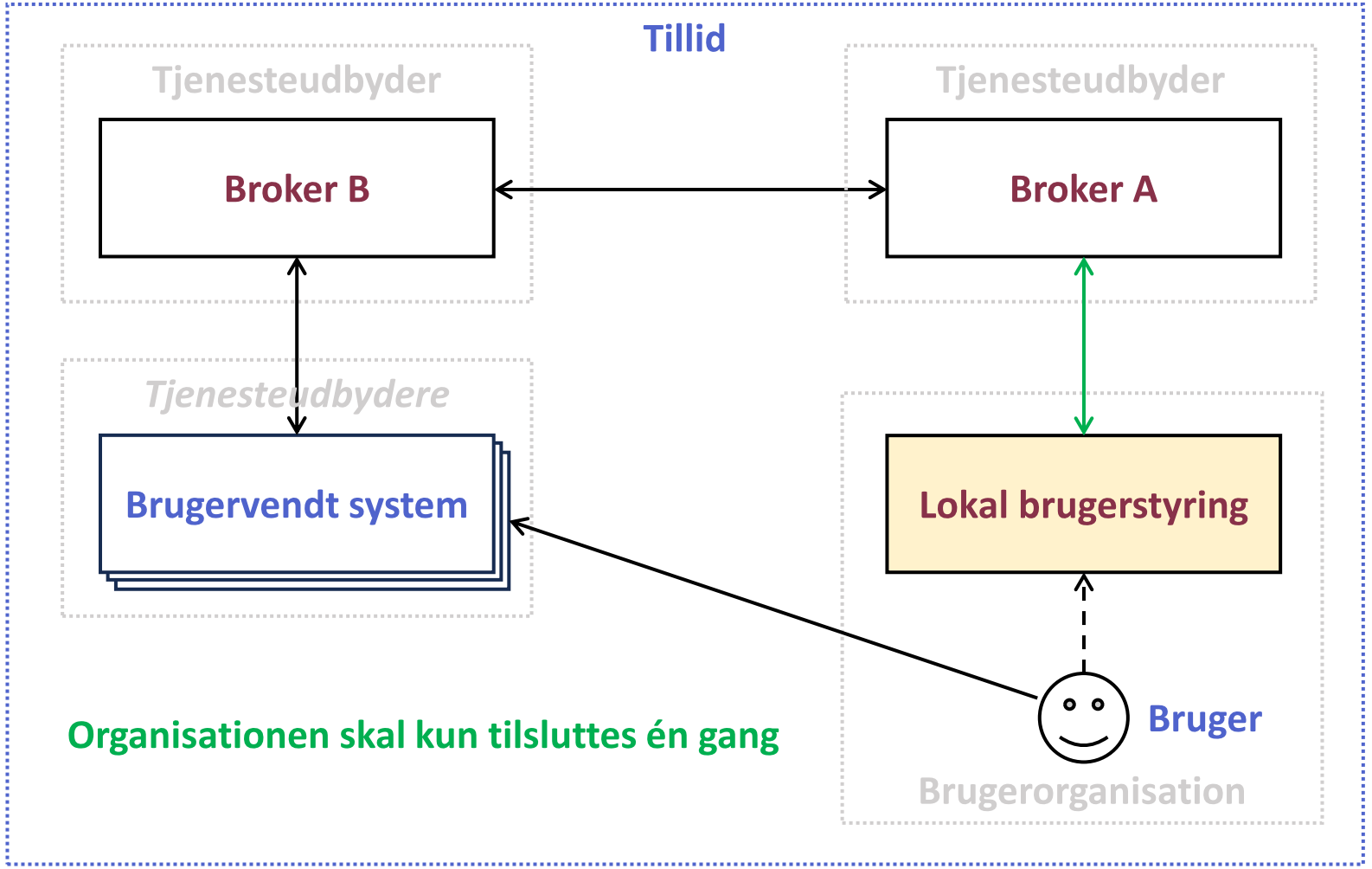
Unilogin

MitID

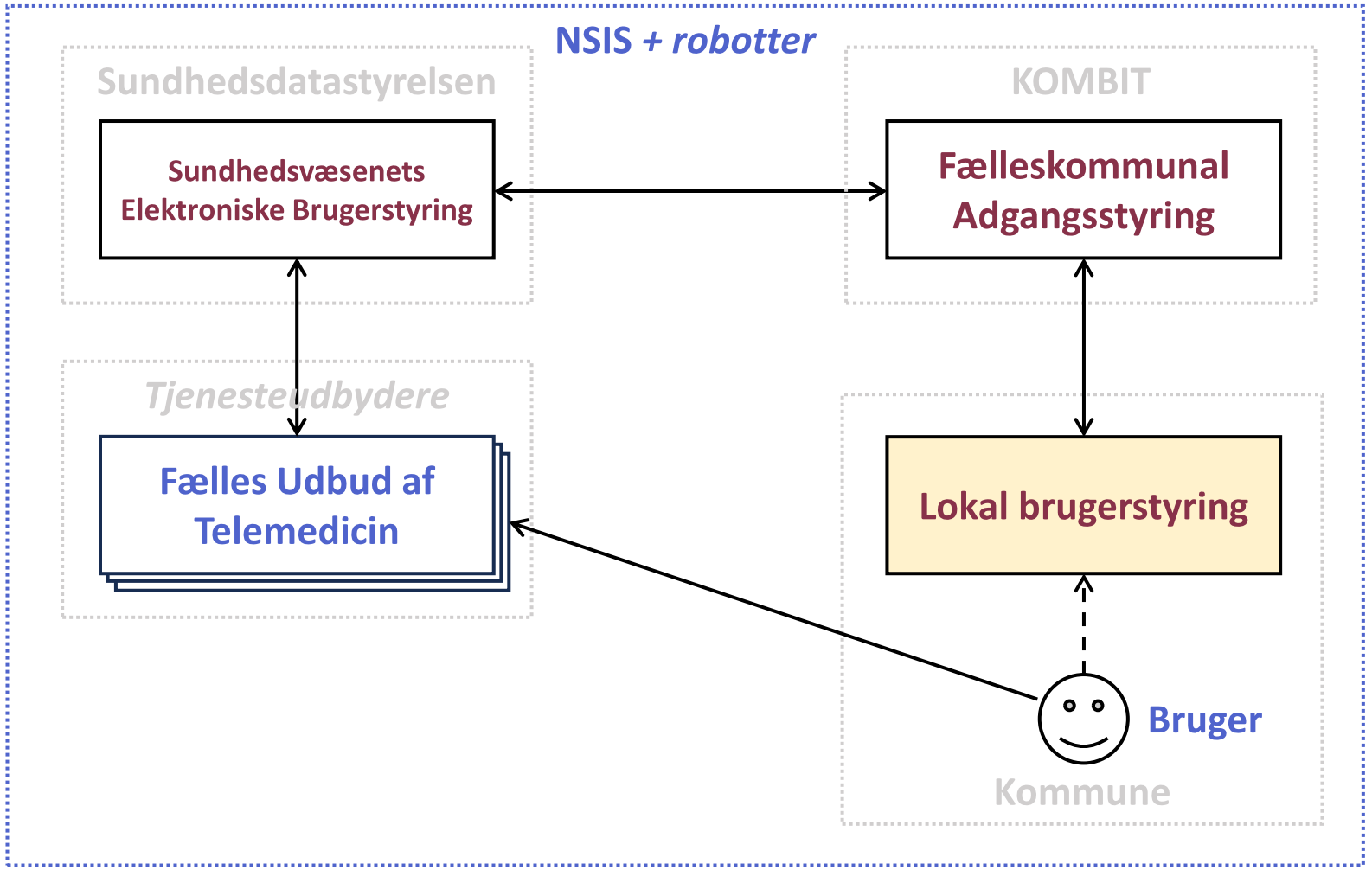
Lokalt login

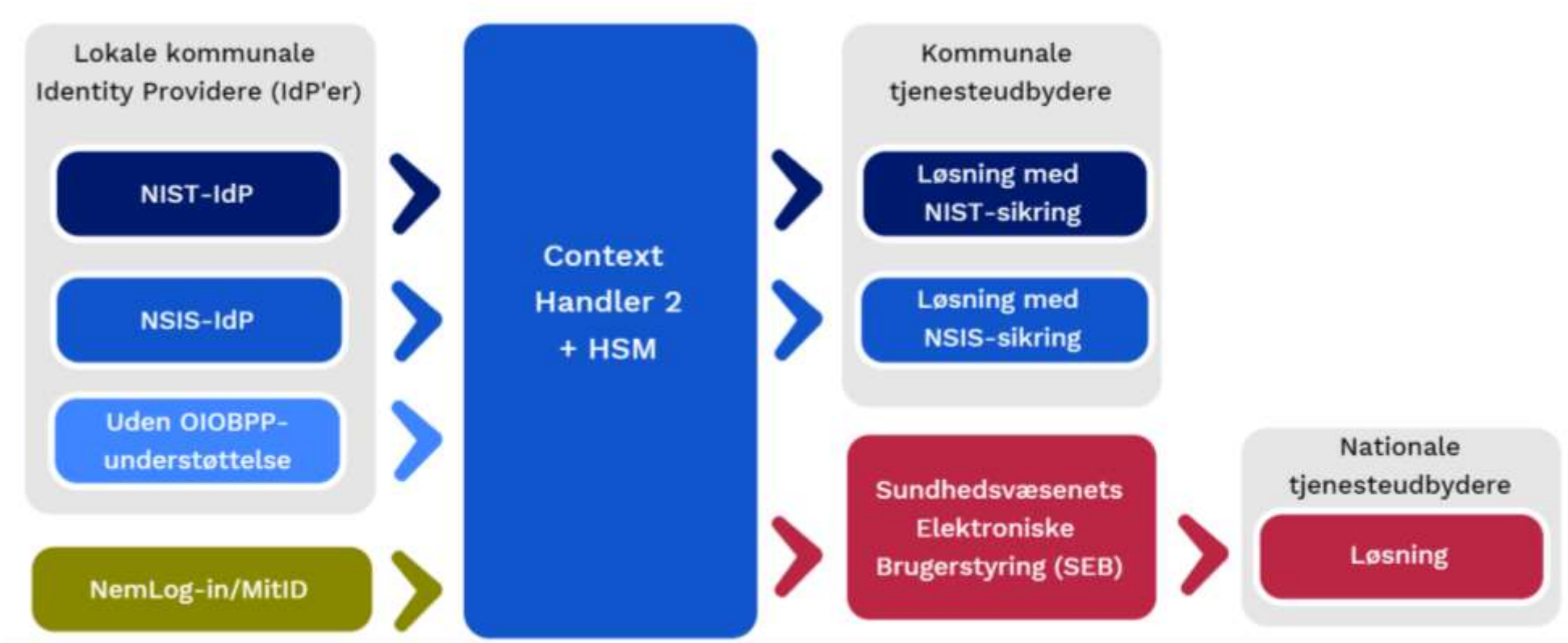
BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING

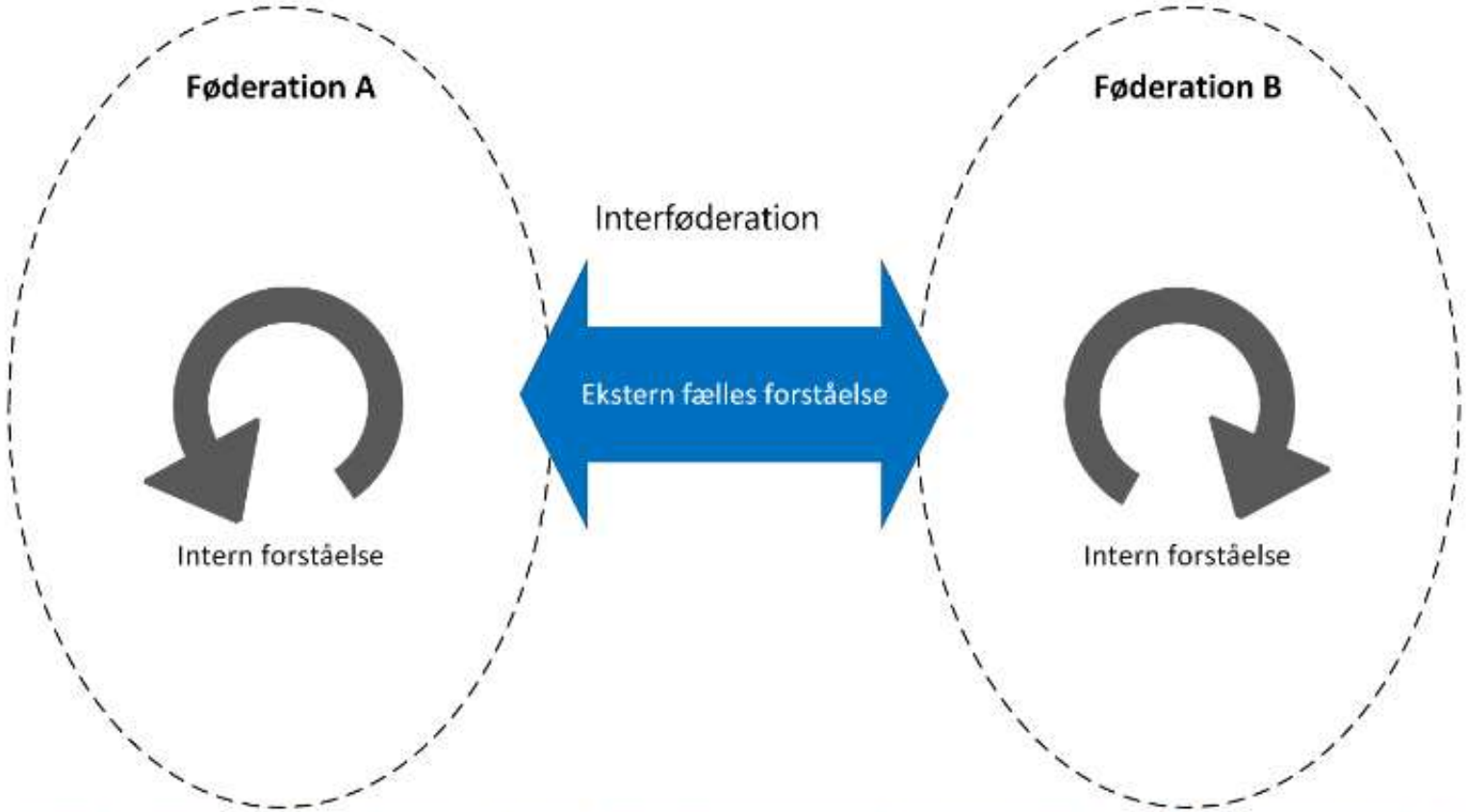
Mønster 5: Interføderation



Fx målbillede: *"FK ADG først"*




Lokale kommunale Identity Providere (IdP'er)
NIST-IdP
NSIS-IdP
Uden OIOBPP-understøttelse
NemLog-in/MitID
Context Handler 2 + HSM
Kommunale tjenesteudbydere
Løsning med NIST-sikring
Løsning med NSIS-sikring
Sundhedsvæsenets Elektroniske Brugerstyring (SEB)
Nationale tjenesteudbydere
Løsning



Figur 1: Intern vs. ekstern forståelse af tekniske og organisatoriske procedurer, specifikationer og standarder [modificeret efter Analyse2014, s. 23]

RAPPORT 2020

Målbillede for sammenhængende brugerstyring

Beskrivelse af tillidstjenester og tillidsrelationer

SUNDHEDSDATA-
STYRELSEN

Potentialer ved et målbillede?

Kommunerne risikerer at gå glip af nogle af de gevinster, der kan realiseres med de eksisterende brugerstyringsløsninger, som vi har investeret i sammen:

- større **brugervenlighed** for medarbejdere
- mere **effektive arbejdsgange** for administration af brugere og rettigheder
- øget **sikkerhed**
- billigere **vedligeholdelse og drift**

Potentialer ved et målbillede?

Med et fælles målbillede bliver KL og KOMBIT meget bedre rustet til at **varetage kommunernes interesser** over for andre offentlige og private aktører og håndtere nye udfordringer, der dukker op.

Samtidig får kommunerne et fælles udgangspunkt for at **stille krav til leverandørerne**.

I første omgang er der behov for at etablere fælleskommunal enighed om en **vision for sammenhængende brugerstyring**.

Visionen bør dernæst konkretiseres med brugsscenarier i en sådan grad at det bliver muligt for de forskellige aktører at handle i overensstemmelse med målbilledet. Det vil kræve **bred kommunal forankring**.