DIGITAL IDENTITY

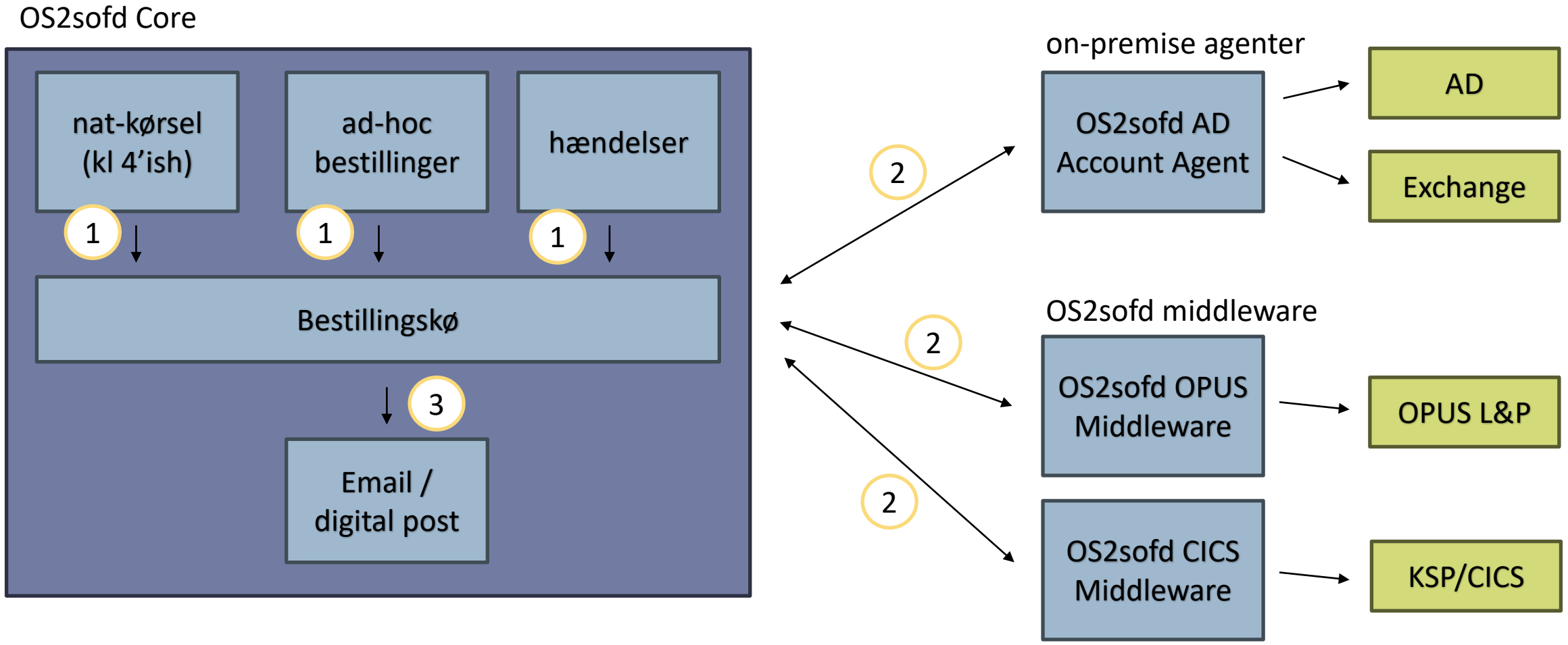
OS2sofd IdM

Agenda

- Overordnet flow IdM
- Overordnet flow AD vedligehold
- Konfiguration af IdM i OS2sofd
- Lokal opsætning (IdM)
- Lokal opsætning (AD vedligehold)
- En plan

Overordnet flow IdM

Overordnet flow IdM



Overordnet IdM flow

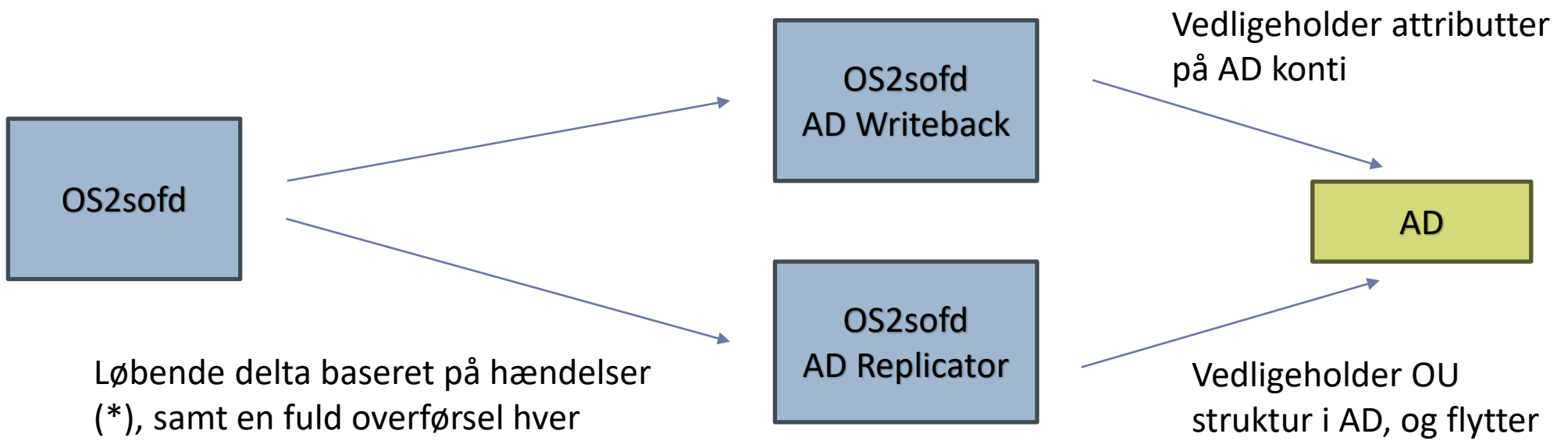
1 – danne ordre
På baggrund af enten natlige kørsler, brugerdrevne ”kliks” eller organisatoriske hændelser, dannes der ordre vedrørende oprettelse/nedlæggelse af it-konti (AD, Exchange, CICS & OPUS)

2 – afvikle ordre
Forskellige agenter håndterer ordrene. AD agenten kører on-premise, og sender status tilbage til OS2sofd

3 – kommunikere om afviklede ordre
OS2sofd kommunikerer omkring resultatet (fx Digital Post til medarbejderen, email til lederen, osv)

Overordnet flow AD vedligehold

Overordnet flow AD vedligehold



Løbende delta baseret på hændelser (*), samt en fuld overførsel hver morgen (5'ish)

* Ikke alle data-ændringer skaber hændelser, så fuld kørsel er nødvendig

Overordnet flow AD vedligehold

De to services (Writeback og Replicator) kan installeres uafhængigt af hinanden, og man vælger selv hvilke attributter der skal vedligeholdes (Writeback) og hvilke dele af organisationen i OS2sofd som skal skrives til AD (Replicator).

IdM processerne fra tidligere kan udfylde initielle attributter på AD konti på oprettelsestidspunkt, men laver ikke løbende vedligehold – dette håndteres af disse to services.

Bemærk man kan installere disse services uafhængigt af hinanden (som nævnt), men også uafhængigt af IdM processerne.

Konfiguration af IdM i OS2sofd

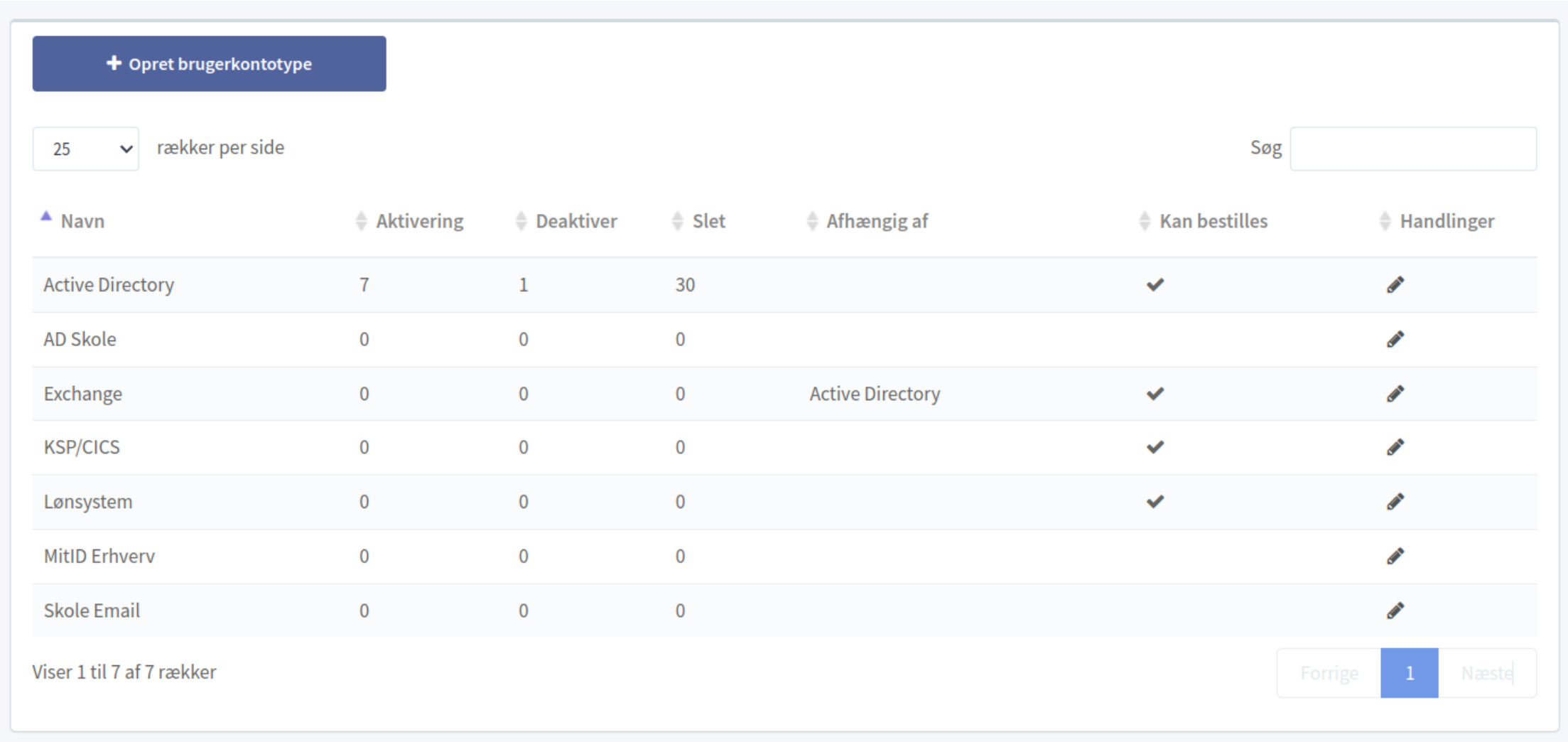
Konfiguration af IdM i OS2sofd

I OS2sofd skal man gennem 3 punkter i forbindelse med opsætningen af IdM processerne.

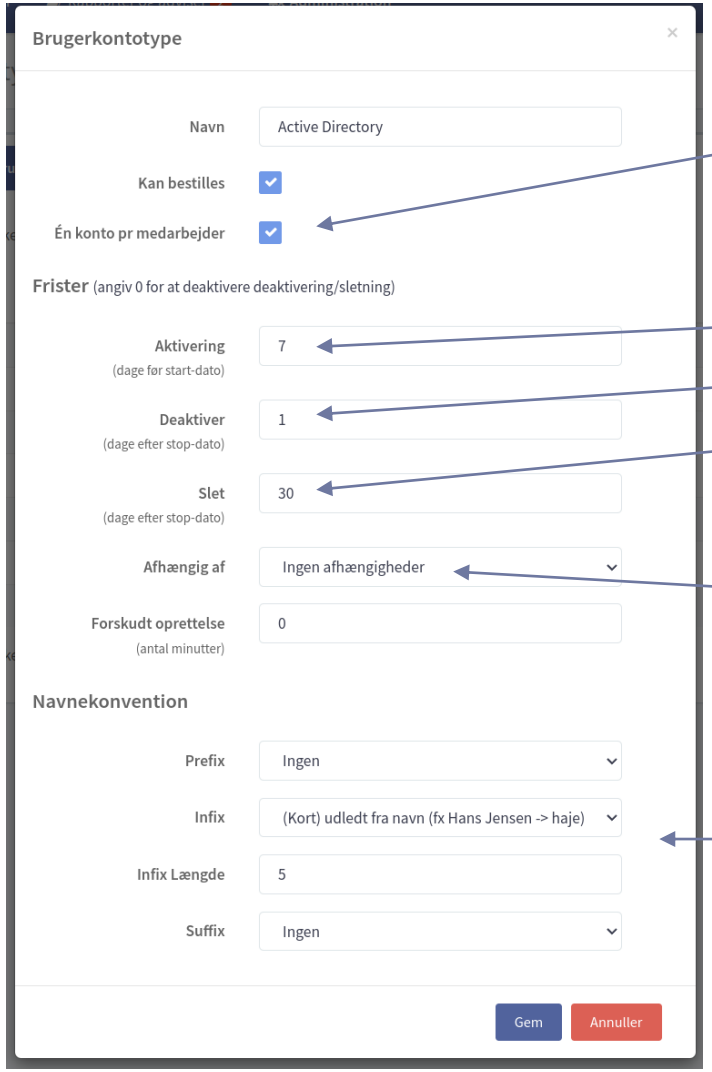
- Opsætning af tidsfrister og navnestandard for brugerkonti
- Opsætning af bestillingsregler på enheder/stillinger
- Opsætning af kommunikation (email og digital post)

Disse er illustreret på følgende slides

Opsætning af tidsfrister og navnestandard



Opsætning af tidsfrister og navnestandard



Får man **én konto** i kommunen, eller får man en konto **per ansættelse**.

Hvor mange dage før første arbejdsdag oprettes kontoen

Hvor mange dage efter sidste arbejdsdag (*) deaktiveres kontoen

Hvor mange dage efter sidste arbejdsdag (*) slettes kontoen

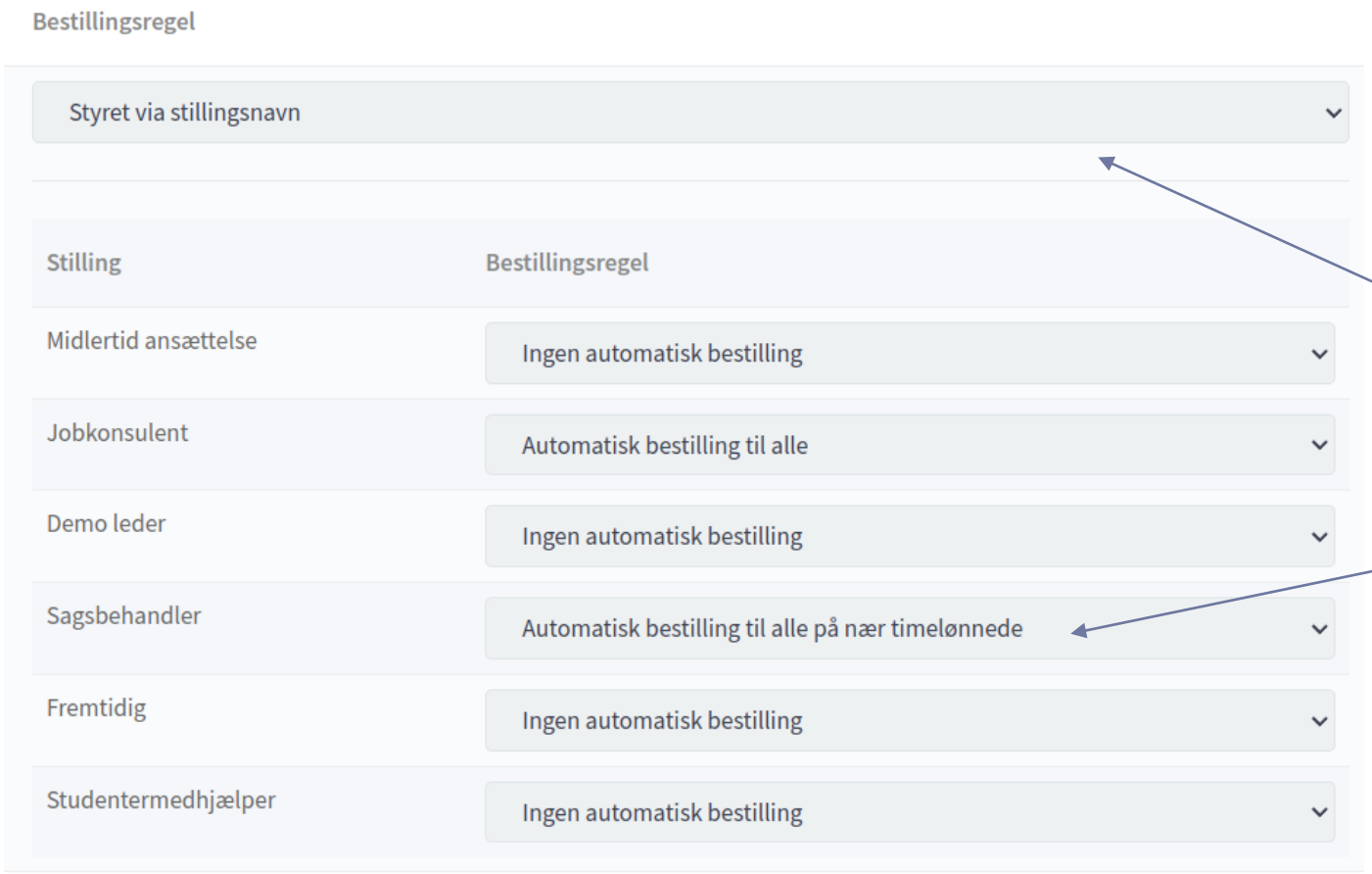
Kan man kun få kontoen hvis man har en anden konto først?

Hvordan dannes navnet på kontoen?

Opsætning af bestillingsregler

Opsætning udføres ”per enhed” – men reglerne kan nemt kopieres fra enhed til enhed

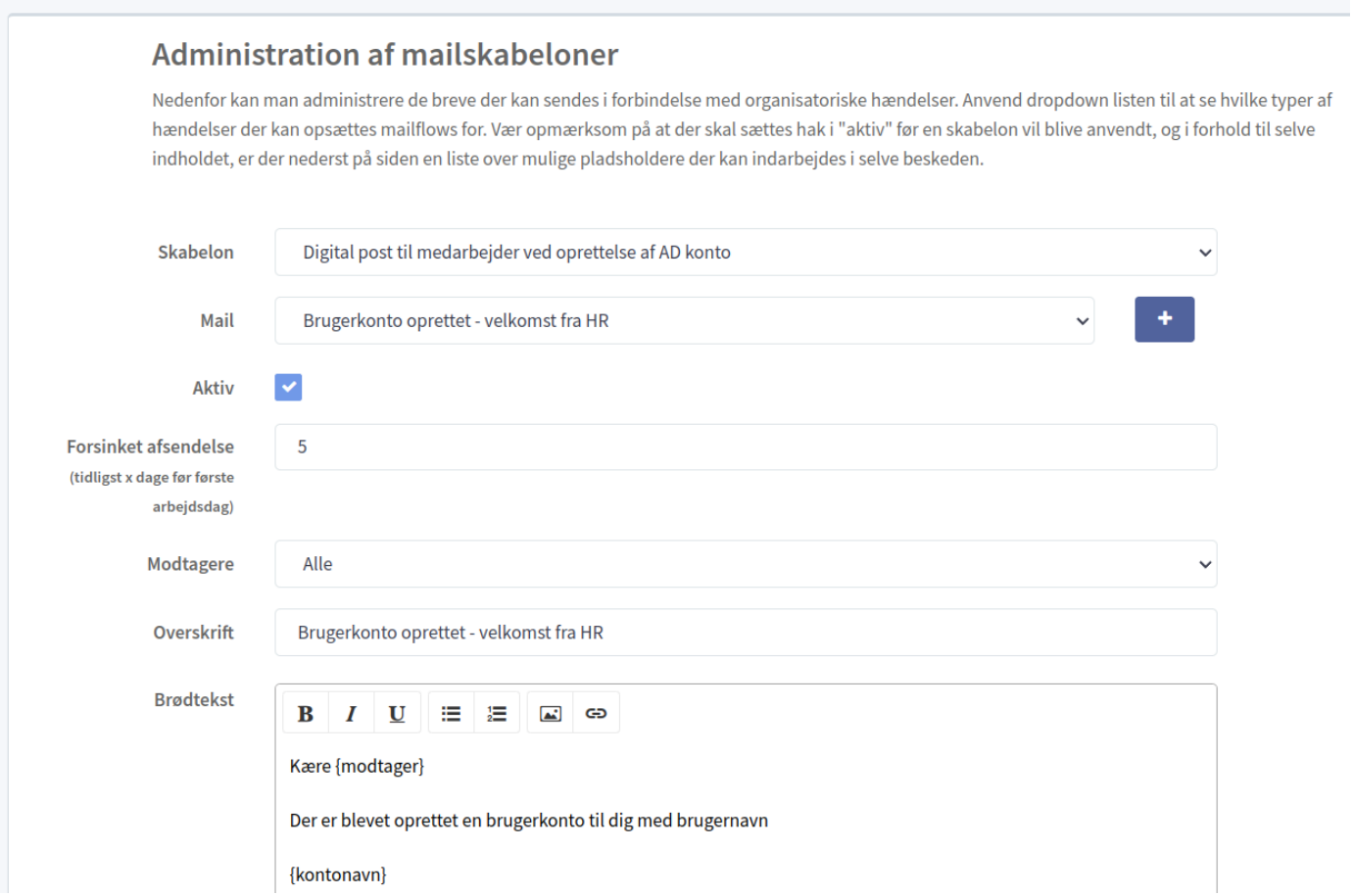
Opsætning af bestillingsregler



Reglerne kan fintunes helt ned på stillingsniveau.

Og man kan skelne mellem fastansatte og timelønnede

Opsætning af kommunikation



Mailskabeloner, som I kender dem fra OS2rollekatalog og andre systemer, kan opsættes til at kommunikere om IdM processerne.

- Digital Post til medarbejder ved oprettelse af AD konto
- Digital Post (eller mail) til medarbejder ved oprettelse af Exchange konto
- Mail til bestiller ved fejl på AD oprettelse
- Mail til leder ved oprettelse (eller spærring) af AD konto
- Mail til leder hvis der ligger bestilling på AD konto til godkendelse (*)

Lokal opsætning af IdM

Lokal opsætning af IdM

Lokalt er der én agent der skal installeres og konfigureres. Den håndterer både oprettelse, spærring og sletning af AD konti, samt tilsvarende operationer for Exchange.

Vedrørende exchange er der 2 forskellige måder, afhængigt af at om det er Exchange on-premise eller Exchange Online (herunder også hybrid opsætningen)

Til alle operationer (opret, spær, slet) er der mulighed for at afvikle et **lokalt powershell** script, som køres EFTER operationen er udført. Dette bruges mest under oprettelse, og her kan man udføre ekstra tilpasninger, som oprettelse af ”drev”, tilpasning af standard-attributter på AD kontoen m.m.

Lokal opsætning af AD vedligehold

Lokal opsætning af Writeback

Her mapper man reelt data fra OS2sofd til AD via en mapningstabel – som er illustreret nedenfor. Der er et rigt mapningssprog at anvende til at flette data med.

```
<mappings>

    <!--simple eksempler. Hvis ingen punktum er angivet tager den bare attributterne fra Person objektet i SOFD-->
    <mapping sofd="firstname" ad="givenName" />
    <mapping sofd="surname" ad="sn" />

    <!--Eksempel på mapping hvor man vil have navnet på enheden i 4. niveau fra toppen med nedarvning -->
    <mapping sofd="affiliation.orgUnit.^4.name" ad="extensionAttribute3" />

    <!--Denne vil skrive "fornavn efternavn" i AD-->
    <mapping sofd="join(firstname,static( ),surname)" ad="extentionAttribute2" />

    <!--Eksempel på mapping hvor man vil have et tag fra enheden. -->
    <!--Første parameter angiver navnet på Tag (Office i eksemplet) -->
    <!--Anden parameter angiver om der skal anvendes nedarvning fra øvre enheder
        i hierarkiet (true eller false) -->
    <!--Tredje parameter angivet hvilken attribut på orgUnit der skal anvendes
        som defaultværdi, hvis tagget ikke selv har en værdi. Der kan angives null-->
    <mapping sofd="affiliation.orgUnit.tag[Office,true,name]" ad="physicalDeliveryOfficeName" />

    <!-- Eksempel på formattering af cpr med bindestreg-->
    <mapping sofd="cprformat(cpr)" ad="description" />

</mappings>
```

Lokal opsætning af Replicator

Der er 2 implementeringsmodeller for opsætningen af OS2sofd AD Replicator servicen.

Man kan enten tage udgangspunkt i en eksisterende AD struktur – her skal man udføre noget ”fodarbejde” inden man kan tænde, da alle enheder i den eksisterende struktur skal mappes til de enheder de matcher inde i OS2sofd. Ved første kørsel oprettes så de enheder der findes i OS2sofd, som ikke allerede findes i AD.

Man kan også vælge at lave en helt ny struktur i AD, som afspejler opsætningen i OS2sofd. Her slipper man for først at skulle mappe AD enheder med OS2sofd enheder, men tilgengæld får man en helt ny struktur, hvor man igen skal opsætte Group Policies m.m.

Overordnet flow IdM

En mulig rækkefølge at implementere i

- ❑ Tænde for automatisk spærring af AD konti når medarbejdere stopper
- ❑ Tænde for replikering af OU strukturen fra OS2sofd ned i AD
- ❑ Tænde for overførsel af bruger-attributter fra OS2sofd til AD
- ❑ Afdække ”den ideelle brugeroprettelse”
- ❑ Konfigurere IdM processer for oprettelse af AD og Exchange konti
- ❑ Konfigurere email skabeloner
- ❑ Konfigurere powershell til oprettelse af AD / Exchange, og udfør testoprettelser
- ❑ Opsætte bestillingsregler for 1-3 enheder (eller måske et helt center)
- ❑ Afprøve IdM flowet i en periode
- ❑ Opsætte bestillingsregler for alle enheder
- ❑ Konfigurere IdM processer for oprettelse og nedlæggelse af CICS og OPUS konti

DIGITAL IDENTITY

OS2sofd IdM