# ADEventService

20130820/SDE

## Indledning

Microsoft Active Directory (AD) er for mange virksomheder en central infrastruktur komponent for administration af virksomhedens IT-brugere, IT-grupper (grupper af brugere), organisatoriske enheder og andre IT-nære ressourcer. Herunder benyttes AD også til at vedligeholde IT-brugernes autorisationer til IT fagsystemer og andre IT-ressourcer via ADs koncept for sikkerhedsgrupper.

Således også i Gentofte Kommune (GK), som med omkring 6500 brugere, 500 organisatoriske enheder og ca. 300 fagsystemer anvender AD i udstrækt grad til at vedligeholde stamoplysninger omkring disse entiteter.

Det er således AD der sidder i førersædet (såkaldt autoritativ kilde) når det drejer sig om vedligeholdelse af brugere, organisatoriske enheder og roller/rettigheder. I AD termer kaldes disse entiteter også for *AD objekter*.

Mange IT-fagsystemer benytter sig også af et koncept om brugere, organisatoriske enheder (afdelinger), roller/rettigheder osv for at kunne understøtte den opgave de er udviklet til.

Det siger sig selv, at det er ikke er videre hensigtmæssigt, at skulle genindtaste oplysninger omkring brugere, enheder, osv i IT-fagsystemet, når de allerede findes i AD’et. Dels er der tale om en ekstra manuel opgave og dels er der risiko for inkonsistens mellem de systemer, som håndterer den slags oplysninger.

***Derfor er det en stående målsætning for GK, at IT-fagsystemer der opererer med brugere, enheder og roller/rettigheder kan anvende/spejle de entiteter fra AD der allerede er oprettet og som løbende oprettes, ændres og nedlægges, men vel og mærke, uden manuel intervention.***

## Integration med AD

Der findes en del teknologier og API’er for integration med AD.

Leverandører er i udgangspunktet fri til at vælge den teknologi de foretrækker for integration af eget fagsystem til AD, men under forudsætning af, at den integration der udvikles understøtter følgende overordnede krav:

1. Integrationen omfatter alle 3 typer af AD entiteter, dvs brugere, organisatoriske enheder (OU) og AD sikkerhedsgrupper
2. Ændringer til entiteter afspejles i realtid eller næsten realtid i fagsystemets kopi af de(n) tilsvarende entitet(er). I særlige tilfælde, kan afspejling af ændringer i AD til fagsystemet accepteres med en større forsinkelse.
3. Alle operationer der er lovlige at udføre på entiteter i AD, afspejles ”loyalt” i det tilsvarende entiteter i fagsystemet. Fx er det en forventning at objekter, der slettes fra AD – også slettes fra fagsystemet, mv.
4. Integration kan ske uden AD skema udvidelse.

Mere detaljeret tager brugeradministration af fagsystemer afsæt i følgende principper:

1. Brugere der allerede er oprettet på GKs IT-platform, skal ***ikke*** oprettes igen (ifm implementering af nyt IT-system), men afspejles automatisk ved passende integrations mekanisme i fagsystemet. Tilsvarende for organisatoriske enheder. Eventuelt for roller (AD sikkerhedsgrupper).
2. Nye oprettelser, ændringer til (herunder flytninger) og sletninger af brugere og organisatoriske enheder, afspejles 100% i fagsystemer ***uden manuel interaktion***.
3. Nye oprettelser, ændringer til (herunder flytninger) og sletninger af brugere og organisatoriske enheder, afspejles 100% i fagsystemer ***med det samme*** (nær realtid).
4. Rollebaseret autorisationsstyring administreres i udgangspunktet i AD (via AD sikkerhedsgrupper) – ***ikke*** i fagsystemet. Hvis fagsystemtets funktion er afhængigt af, at der kan administreres roller (og tildeling af roller til brugere) i fagsystemet, skal der etableres integration til AD, så fagsystemets administration skrives igennem til AD.
5. Rettighedstildeling til funktioner, data og andre IT-ressourcer tildeles altid til en given bruger via AD gruppe medlemskab. Mao – det skal være muligt alene ved konsultation af AD, at afgøre hvilke rettigheder der er tilknyttet en specifik bruger eller gruppe af brugere.
6. Administration af brugere, brugeres adgang til fagsystemer og brugernes rettigheder i fagsystemet skal kunne ske alene med udgangspunkt i AD (altså uden kendskab til fagsystemets administrative grænseflade).
7. Rettigheder kan tildeles via indirekte AD gruppe medlemskab (grupper i grupper i grupper i ...).
8. Løsninger der integrerer med AD understøtter SSO. Det vil sige at brugeren ikke skal logge eksplicit ind i fagsystemet, hvis brugeren allerede via oprettelse i AD og medlemskab af passende fagsystem specifikke rettighedsgrupper, kan anvende fagsystemet uden yderligere tiltag (selvfølgelig først når brugeren er autentificeret ved login på Windows skrivebord – eller tilsvarende).

xxx

Hvem har udviklet

Hvem ejer

Målgruppe for dette dokument

Virkemåde

Installation

3. parts integration