

Er rolle basert tilgangskontroll tilstrekkelig for å realisere en prosessdrevet SOA?

Hva er en rolle egentlig?

Erfaringsmessig er rollebegrepet benyttet til veldig enkel saksbehandling og brukt som en autorisasjonsmekanisme ift. tildeling av rettigheter til IT systemer, filområder og filer. En rolle i vanlig IT forstand ofte representerer en gruppe med ansatte i en organisasjon som skal ha de samme IT autorisasjoner f.eks. applikasjons- og filtilganger. Dette kalles for rollebasert tilgangskontroll (RBAC). En rolle synes å inneha en egenskap av felles tilhørighet f.eks. alle selgere, alle innkjøpere, alle hjertekirurger osv. Det er vanskelig ut fra rollen til en ansatt å identifisere hvilken organisatorisk tilhørighet den ansatte har, f.eks. hvilken stilling den har, hvilken avdeling den tilhører, hvem man rapporterer til osv. Dette er egenskaper som er viktige å ha oversikt over når man skal flytte informasjon og oppgaver langs forskjellige organisatoriske akser.



Organisasjonen er også en viktig dimensjon til en arbeidsprosess!

Arbeidsprosesser utføres av mennesker og maskiner i koordinert samhandling. Mennesker er som regel ansatt i en organisasjon som består av en struktur av enheter og stillinger. Prosessoperasjonalisering bør dermed gjøres med utgangspunkt i at arbeidsprosessens oppgaver kan automatisk tildeles langs flere organisatoriske akser. Aksene behøver ikke nødvendigvis å følge organisasjonshierarkiet. Det bør derfor være mulig å rute oppgaver både horisontalt, vertikalt, dynamisk og i tidsdimensjonen til enheter, ansatte og systemer i en virksomhet, avhengig av hvilke styrings- og koordineringsbehov arbeidsprosessene skal dekke. Ut fra det perspektivet synes rollebegrepet man er vant til og anvender i IT i dag å være utilstrekkelig for realisering av en prosessdrevet, tjenestorientert arkitektur.

Utfordring 1

Oppgaveruting i reelle arbeidsprosesser

Det er ofte behov for å tildele arbeidsprosessens oppgaver fortløpende ift. en organisatorisk kontekst f.eks. til en gitt enhet i en organisasjon, team eller spesifikk ansatt. Rollebegrepet i seg selv blir for snevert fordi en rolle er tverr-organisatorisk per definisjon. Det er ikke så vanskelig å tildele en oppgave til en ansatt i en gitt rolle i en ren rollemodell, men det er vanskeligere å eskalere opp-

gaven til den ansattes leder dersom fristen for gjennomføringen av oppgaven er passert. Hvem er den ansattes leder i en ren rollemodell? Er det en ansatt i stilling som Administrerende Direktør eller er det de ansatte i rollen som Salgssjef? I så tilfelle hvem av de ansatte i rollen som Salgssjef i en organisasjon med flere Salgssjefer, er den ansattes leder for en gitt arbeidsprosess?

Utfordring 2

Rollebegrepets begrensninger

Da rollebegrepet per definisjon impliserer homogenitet, blir det unaturlig at en rolle består av andre roller f.eks. at rollen Salgssjefer består av Hjertekirurger, Radiologer og Resepsjonister. Det er også unaturlig å bruke rollebegrepet som byggekloss for å definere et organisasjonshierarki, da det som inngår i en organisasjonsenhet er stillinger, andre enheter, roller (team) og grupper som igjen kan bestå av alle "rolletyper".

En annen mulig begrensning ved begrepet rolle, er knyttet til tverr-organisatorisk samhandling i situasjoner der man har behov for å angi en tidsbegrenset rolle for en gitt arbeidsprosesskontekst f.eks. en behandlende lege på AMK sentral forespør sykehus på hjemstedet om å få utlevert pasientjournal til en kritisk skadd pasient. Akkurat der og da har legen rollen som behandlende lege i en tidsbegrenset periode. Legen oppgir disse opplysninger på forespørsel til sykehuset Utleveringsstedet må evaluere disse

opplysningene før utlevering av pasientjournalen kan finne sted. Utfordringen med rollebegrepet i dette tilfellet, er at det ikke endres dynamisk som en følge av kontekst og en tidsbegrenset oppgave som utføres i en arbeidsprosess.

Utfordring 3

Rollehierarkier og grupper

Ofte benyttes roller i hierarkier som grunnlag for organisasjonsmodellen. Å bruke rollehierarkier kan forvanske organisasjonsmodelleringen, da man forsøker å bruke et og samme begrep til å modellere flere andre begreper som enheter, stillinger, grupper, osv. Hierarkiet av roller med relasjon til andre roller blir fort uoversiktlig, vanskelig å administrere og forstå. Ofte er det beste å kalle en spade en spade da det blir enklere å forstå, forklare og anvende.

I komplekse arbeidsprosesser har man ofte behov for å opprette grupper som består av forskjellige typer oppgavemottakere f.eks. personer, enheter, roller og andre grupper. Det som kan kjennetegne en gruppe er at den ikke er begrenset til en type oppgavemottaker, men kan brukes for å inneholde personer, stillinger, roller og organisasjonsenheter som oppgavemottakere. Tidligere forskning har også påvist andre svakheter ved RBAC modellen f.eks. relatert til delegering og retur av arbeidsoppgaver til og fra oppgavemottakerne (Wainer, J., Kumar, A., Barthelmess, P., 2007).

Utfordring 4

Prosesstilgang

I en prosessdrevet SOA verden er det nødvendig å kunne tildele tilgang til prosesser på forskjellige nivå f.eks. man bør kunne angi "hvem" som har lov til å initiere nye arbeidsprosesser. Man må også kunne involvere de forskjellige delene av organisasjonen i prosessene ut fra deres organisatoriske tilhørighet, stilling, rolle og organisatoriske relasjoner. Prosesstilgangen bør kunne endres raskt og uten spesiell IT kompetanse eller henvendelser til brukerstøtte. Slike krav indikerer at det er nødvendig at organisasjonsmodellen er integrert med, men løskoblet fra brukerkatalogen der brukerprofilene ligger lagret. En begrunnelse for dette følger i påfølgende avsnitt.

Utfordring 5

IT organisasjonens beskyttelse av brukerkatalogen

IT funksjonen i en virksomhet vil ofte velge å operasjonalisere organisasjonsmodellen og autorisasjoner ut fra sitt ståsted f.eks.

tilganger til applikasjoner vha. en katalogtjeneste som Active Directory. Det kan være nødvendig at organisasjonsmodellen støtter flere perspektiver ikke begrenset til IT. Å modellere organisasjonen i en katalogtjeneste blir fort utilstrekkelig i en prosessverden pga flere forhold bl.a.:

- Tradisjonelle brukerkataloger er ofte ikke laget for å håndtere komplekse organisasjonsmodeller der man ikke nødvendigvis har en hierarkisk struktur.
- Begrepsapparatet i en katalogtjeneste er ikke tilpasset organisasjonsmodellerings- og arbeidsprosessbehovene da forvaltningsverktøyene henvender seg til IT tekniske ressurser som brukere.
- Endringer i brukerkatalogens struktur vil kunne ha negative konsekvenser for arbeidsprosesser dersom man ikke har løse koblinger mellom organisasjonsmodellen som forretningen forholder seg til og brukerkatalogen som IT forholder seg til.
- Tradisjonelle brukerkataloger er vanskeligere å endre struktur og innhold i pga eierskapet som ligger hos IT funksjonen i organisasjonen.
- Tradisjonelle brukerkataloger brukes ofte til IT teknisk tilgang på applikasjons- og filsystemnivå og ikke til prosessstilganger.

Utfordring 6

Påstand basert autorisasjon

Tverr-organisatorisk samhandling vil sannsynligvis kreve en mer avansert form for autorisasjonsmodell som baseres på et dynamisk sett med attributter tilsendt tjenesteleverandøren med et standardisert sikkerhetsbevis. Autorisasjonen vil da kunne gis basert på en evaluering av de oppgitte påstandene i sikkerhetsbeviset mottatt fra konsumenten av tjenesten. En slik autorisasjonsmodell kan bygges vha av identitetsfödereringsløsninger og anvendelse av Security Assertion Markup Language (SAML).

Oppsummering

Denne artikkelen forsøker å beskrive en rekke svakheter ved RBAC modellen som gjør den lite egnet i nåværende form for håndtering av virksomhetens komplekse og skiftende tilgangsbehov i en prosessdrevet tjenesteorientert verden.

Artikkelen er skrevet av Jon Gupta, Rådgiver i Acando AS.
Opprinnelig publisert i ComputerWorld Norge.

KONTAKT

Tel: +47 93 00 10 00

E-post: acando@acando.no

