



IT- og Telestyrelsen

Ministeriet for Videnskab
Teknologi og Udvikling

Anbefaling vedrørende brug af RBAC standard til rollebaseret adgangskontrol

Kolofon:

OIO Referencemodel for tværgående brugerstyring

Denne anbefaling kan frit anvendes af alle. Citeres der fra anbefalingen i andre publikationer skal der angives korrekt kildehenvisning.

Forslag til anbefalinger for tværgående brugerstyring udarbejdes af IT- og Telestyrelsen, IT-strategisk kontor, som sekretariat for OIO It-Arkitekturkomiteen.

Kontaktperson:

It-Arkitekt Søren Peter Nielsen, email: spn@itst.dk
Telefon 2567 0783 (direkte)

It-Arkitekt Anders Dalsgaard, email: ada@itst.dk
Telefon 3337 9106 (direkte)

Ministeriet for Videnskab, Teknologi og Udvikling

IT- og Telestyrelsen

IT-strategisk kontor

Holsteinsgade 63

DK-2100 København Ø

Telf. +45 35 45 00 00

Fax. +45 35 45 00 10

<http://www.itst.dk>

itst@itst.dk

1	Indledning.....	5
1.1	Opsummering.....	5
1.2	Formål.....	5
1.3	Baggrund for anbefalingerne.....	6
1.4	Anvendelsesområde.....	7
2	Anbefalinger for rollebaseret adgangskontrol.....	8
2.1	Introduktion til rollebaseret adgangskontrol.....	8
2.2	RBAC standarden.....	9
3	Anbefalinger vedrørende brug af rollebaseret adgangskontrol.....	13
4	Implementering af rollebaseret adgangskontrol.....	15
5	Oversatte RBAC begreber.....	16
6	Appendiks A - Yderligere information.....	16

1 Indledning

1.1 Opsummering

Dette dokument indeholder følgende anbefalinger:

- Det anbefales, at adgangsrettigheder baseres på roller og regler, således at rettigheder kun behøver at blive administreret for individuelle brugere i situationer, hvor roller og regler ikke kan anvendes.
- Det anbefales, at der for systemer til administration af rollebaserede rettigheder stilles mindstekrav om, at de skal overholde RBAC¹-kernens definitioner og krav i RBAC-standarden.
- Det anbefales, at der ved anskaffelse eller udvikling stilles et mindstekrav om, at it-systemer, hvor det er relevant, skal understøtte rollebaseret adgangskontrol som beskrevet i RBAC-kernen af RBAC-standarden.

Baggrunden for disse anbefalinger er primært, at de kan medvirke til at nedbringe omkostninger ved administration af brugerrettigheder, forbedre sikkerheden og give basis for yderligere automatisering af it-brugerunderstøttelse og administration af rettigheder i eksterne systemer.

I kapitel 1 beskrives formål, baggrund og anvendelsesområde for anbefalingerne.

Kapitel 2 giver dels generel introduktion til rollebaseret adgangskontrol såvel som en introduktion til RBAC-standarden samt de ovenfor nævnte anbefalinger.

Anbefalinger i dette dokument vedrører ikke, hvorledes de enkelte roller defineres. I kapitel 3 nævnes, at et fremtidigt diskussionsdokument vil omhandle mulige tilgange til implementering af roller. Der diskuteres kort i kapitlet udfordringer i forbindelse med definition af tværgående roller.

1.2 Formål

Formålet med denne anbefaling er følgende:

- Medvirke til en mere effektiv, mere sikker, mere fleksibel administration af rettigheder i it-systemer ved hjælp af rollebaseret adgangskontrol
- Definere fælles begreber som forudsætning for fælles sprog og fælles tilgangsmåde i forhold til rollebaseret adgangskontrol
- Definere en anbefaling om mindstekrav til it-systemer, der understøtter og anvender rollebaseret adgangskontrol
- Skabe en af de grundlæggende byggesten for løsninger, der automatiserer tildeling, vedligeholdelse og fratagelse af ressourcer og adgangsrettigheder for it-brugere (også kaldet provisioneringsløsninger)

For god ordens skyld skal der også fremhæves nogle punkter, som ikke er formålet med denne anbefaling med henblik på at undgå misforståelser.

- Dette er ikke en anbefaling om, at al rettighedsstyring skal være rollebaseret. Det anbefales at anvende en kombination af roller og regelbaseret rettighedsstyring samt i specielle situationer at benytte styring af rettigheder for individuelle personer

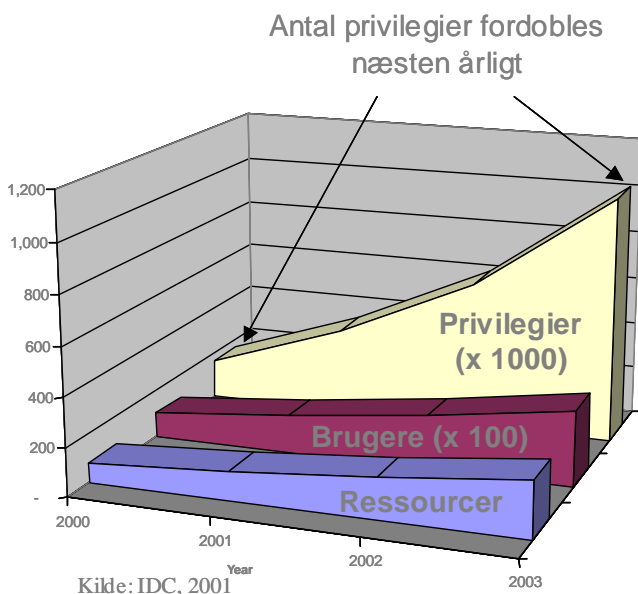
¹ RBAC er en forkortelse af det engelske udtryk *Role-Based Access Control*

- Dette er ikke en anbefaling om, at der skal defineres fælles roller for hele den offentlige sektor. I kapitel 3 diskuteres udfordringer i forbindelse med tværgående roller.
- Dette er ikke en anbefaling, som angiver implementeringsspecifikke anvisninger. Der anbefales en række mindstekrav for et rollebaseret adgangskontrolsystem. Disse vil skulle suppleres med en række andre krav i forhold til den enkelte organisations behov
- Denne anbefaling vedrører ikke definition af en metode til identifikation af roller. Anbefalingerne i dette dokument drejer sig om etablering af et fundament for anvendelse af rollebaseret adgangskontrol, men ikke om indhold af specifikke roller. Læs evt. mere i kapitel 3: 'Implementering af rollebaseret adgangskontrol'.

1.3 Baggrund for anbefalingerne

Med udviklingen indenfor digital forvaltning vokser antallet af it-privilegier, som den enkelte organisation skal styre. Samtidig sker der en vækst på brugersiden i forbindelse med, at flere ansatte i de enkelte organisationer bliver it-brugere. Denne udvikling forstærkes af kommunalreformen, der medfører en række om- og sammenlægninger af organisation og it-systemer, samt behov for en række nye it-løsninger.

Figur 1 illustrerer på basis af en undersøgelse af analysefirmaet IDC, hvorledes antallet af it-privilegier, der skal administreres, vokser meget hurtigere end antallet af it-brugere og it-ressourcer.



Figur 1. Estimeret vækst i privilegier i typiske firmaer. Kilde til figur: NIST²

Privilegier defineres i denne sammenhæng som kombinationen af it-ressourcer og rettighederne til at udføre handlinger eller operationer på dem.

Uden en struktureret tilgang til håndtering af tildeling, ændring og fjernelse af rettigheder for brugere, vil den enkelte organisation kunne få væsentlige administrative omkostninger. Der er også en fare for at sikkerhedsniveau vil lide, fx fordi at der ikke bliver fjernet rettigheder fra brugere, der forlader organisationen etc.

Indførelse af rollebaseret adgangskontrol kan medvirke til følgende:

² Kilde til figur: Præsentation fra National Institute of Standards and Technology (NIST): *Proposal for Fast-Tracking NIST Role-Based Access Control Standard* af David Ferraiolo - NIST, Rick Kuhn - NIST og Ravi Sandhu - George Mason University

- Mere struktureret administration af brugerrettigheder
- Mindskelse af den administrative byrde i forhold til en individ- eller gruppebaseret administration af rettigheder
- Bedre sikkerhed gennem bedre overblik over rettighedstilknytninger, f.eks. således, at det kan sikres, at alle rettigheder fjernes for personer, der har forladt organisationen

Roller kan også anvendes til automatisering af hele processen med at give en nyansat de adgange, som vedkommende har brug for. En sådan automatiseret proces betyder normalt, at nye medarbejdere hurtigere kan arbejde med fuld produktivitet.

For at kunne høste de ovennævnte fordele skal organisationen dels have løsninger til administration af rettigheder, it-løsningernes privilegier skal kunne tilknyttes roller, og organisationen skal definere hvilke roller, der er relevante i forhold til organisationens arbejdsgange.

Anbefalingerne i dette dokument vedrører definition af grundlæggende begreber samt en række mindstekrav til funktionalitet i forbindelse med administration af rollebaseret adgangskontrol og til de it-løsninger, der stiller privilegier til rådighed. Anbefalingerne skal være en hjælp til etablering af fundamentet for rollebaseret adgangskontrol.

1.4 Anvendelsesområde

Anbefalingerne i dette dokument retter sig generelt mod it-systemer, som anvendes til digital forvaltning.

Det vigtige er først og fremmest selve konceptet i, at brugeres tilknytning til it-privilegier ikke foretages direkte, men at roller anvendes til abstraktion og konsolidering af en brugers adgang til de enkelte it-ressourcer eller objekter.

Derudover kan anbefalingerne også anvendes:

- Som framework for leverandører
- Som basis for at beskrive arkitekturspecifikke API'er
- Som grundlag for videreudvikling af rollebaserede adgangskontrolssystemer og teknologier – tekniske standarder.
- Som grundlag for kravspecifikationer

Anbefalingerne baserer sig på en standard, der retter sig mod *personers* anvendelse af it-systemer, men der er principielt ikke noget i vejen for, at en given rolle-indehaver, som anvender et it-system, også kan være en automatiseret klient (eller web service).

Anbefalingerne retter sig mod rollebaseret adgangskontrol indenfor en enkelt organisation. Se kapitel 3 for en diskussion vedrørende anvendelse af roller på tværs af organisationer.

Roller kan anvendes til at afgøre, hvilke handlinger en bruger må udføre i et it-system. Roller kan for sig selv ikke anvendes til at afgøre med hvilket formål, brugeren udfører denne handling. Dette er især relevant i forbindelse med personfølsomme data, hvor adgang kun skal gives til brugere, der har et validt formål med handlingen. Dette kan f.eks. et krav om, at en læge kun må se følsomme dele af en elektronisk patient journal, hvis vedkommende læge har patienten i lægelig behandling. I sådanne tilfælde må der anvendes en kombination af roller og regler.

2 Anbefalinger for rollebaseret adgangskontrol

2.1 Introduktion til rollebaseret adgangskontrol

Ved hjælp af adgangskontrol bestemmes konkret en brugers³ tilladelse til at gøre (eller ikke at gøre) en specifik ting. Dette sker normalt ved fysisk eller systembaseret adgangskontrol.

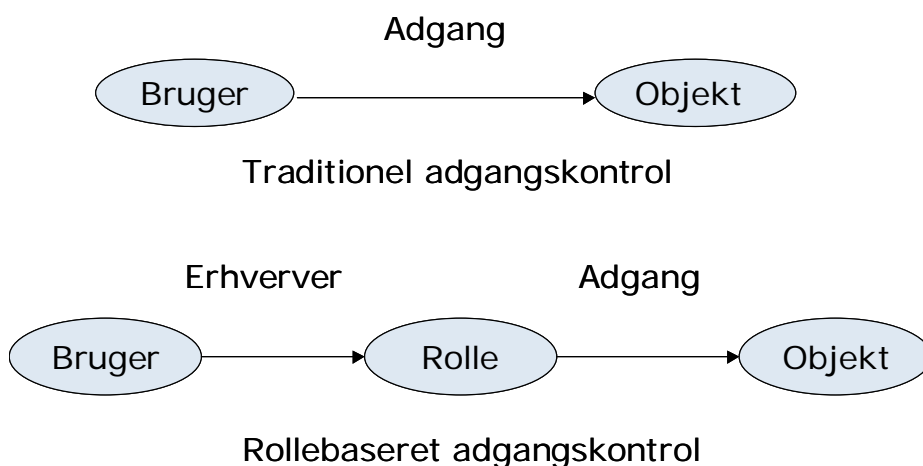
Når adgangskontrollen er it-baseret, kan det angives, hvilken person, rolle eller proces, der må få adgang til en given system-ressource, såvel som hvilken type af adgang, der er tale om (læse, skrive, slette, etc.)

Med Rollebaseret adgangskontrol (RBAC) gives adgang på basis af roller, som brugerne tildeles i deres organisation.

Privilegier tilknyttes roller, og roller tilknyttes brugere.

I denne forbindelse defineres et privilegium som kombinationen af et objekt (fx et dokument) og en handling, der kan udføres på objektet (som fx *Udskriv*). Objektet kan være abstrakt, som f.eks. en forretningsproces, hvor handlingen kan være *udfør*, *observer* og lignende.

Forskellen på adgangskontrol, hvor privilegier tilknyttes direkte til brugeren eller en gruppe af brugere, og rollebaseret adgangskontrol, hvor der anvendes en rolle til at forbinde bruger og privilegier, er illustreret i den følgende figur:



Figur 2. Traditionel / rollebaseret adgangskontrol.

Rollebaseret adgangskontrol kan bruges til at styre rettigheder, der muliggør:

- Komplekse politikker for tildeling af rettigheder.
- Reduktion i antallet af fejl i administration af rettigheder.
- Reduktion i omkostningerne ved administration af rettigheder.

Politikker for tildeling af rettigheder afspejles i kombinationen af følgende komponenter i rollebaseret adgangskontrol:

- Rolle-Privilegium relationer
- Rolle-Rolle relationer

³ Bruger kan i denne sammenhæng være person eller it-system/service

- Bruger-Rolle relationer

Disse komponenter bestemmer tilsammen, hvorvidt en specifik bruger får adgang til en bestemt systemressource.

Rollebaserede komponenter kan konfigureres direkte af systemejeren eller indirekte af andre brugere med passende roller, som de er delegeret til af systemejeren.

Den adgangspolitik, som håndhæves i et specifikt system, er mængden af forskellige rollebaserede komponenter (og eventuelle regler) som foreskrevet af systemejeren

Evnen til fleksibelt at ændre i adgangspolitikken ved hjælp af konfiguration og uden kode-ændringer, er en væsentlig fordel ved rollebaseret adgangskontrol.

Rollebaseret adgangskontrol understøtter tre velkendte sikkerhedsprincipper:

- Mindste rettighed/Laveste autorisation (Engelsk: Least Privilege)
- Funktionsadskillelse (Engelsk: Separation of duties)
- Abstraktion af data (Engelsk: Data Abstraction)

Mindste rettighed understøttes, fordi rollebaseret adgangskontrol kan konfigureres således, at *kun* de nødvendige rettigheder, for at en rolleindehaver kan udføre en given opgave, tilknyttes rollen.

Funktionsadskillelse opnås ved at sikre, at flere roller, som gensidigt udelukker hinanden, er nødvendige for at gennemføre en sensitiv opgave (som fx at anvise penge til udbetaling og efterfølgende godkende udbetalingen).

Abstraktion af data opnås ved at anvende abstrakte privilegier, som f.eks. *Kreditering af konto*.

I hvor høj grad abstraktion af data er mulig afgøres af mulighederne i den konkrete implementering af rollebaseret adgangskontrol.

Det er ikke realistisk at betragte rollebaseret adgangskontrol som en enkelt model. Der er tale om et spektrum af modeller inden for rollebaseret adgangskontrol.

Én model vil enten fravælge eller inkludere for meget, og den vil således kun repræsentere en delmængde af de forskellige muligheder og teknologier, som rollebaseret adgangskontrol giver mulighed for.

For at kunne få en afgrænsning af forskellige modeller og fælles taksonomi (navngivning af begreber) har American National Standards Institute (ANSI) vedtaget en standard vedrørende RBAC. Standarden er foreslået af National Institute of Standards and Technology (NIST) i USA.

Anbefalingerne i dette dokument vedrører dele af denne standard, hvorfor hovedpunkterne i standarden gennemgås i næste afsnit.

2.2 RBAC standarden

ANSI's standard vedrørende rollebaseret adgangskontrol hedder formelt *American National Standard ANSI INCITS 359-2004*, men benævnes herefter blot som RBAC-standard⁴.

Dette afsnit vil give en kort ikke-normativ introduktion til indhold og struktur i standarden, men det anbefales, at læseren anskaffer og orienterer sig selv direkte i RBAC-standard (eller det udkast NIST publicerede som forslag til standard⁵).

⁴ Selve standarden kan købes online for et relativt lille beløb. Per 1. august 2005 kunne en PDF-version af RBAC-standard købes online på http://www.techstreet.com/cgi-bin/detail?product_id=1151353 til en pris af 18 dollar.

RBAC-standarden består af to dele:

- RBAC-modeller
- Funktionel specifikation med krav til RBAC-systemer

I den del der vedrører RBAC-modeller, defineres først basale RBAC-elementer som bruger, rolle, privilegier, operationer og objekter samt relationer som typer og funktioner, der er inkluderet i standarden.

Herved defineres en afgrænsning af, hvilke elementer standarden vedrører. Disse elementer har fået en konsistent navngivning, som kan anvendes ved beskrivelserne af funktionalitet.

Herefter gennemgås de følgende fire komponenter, som RBAC modellerne er sammensat af

- RBAC-kernen
- Hierarkisk RBAC
- Statisk funktionsadskillelse
- Dynamisk funktionsadskillelse

Komponenterne og de forskellige modeller for RBAC, som opstår ved kombinationer af disse komponenter, gennemgås kort i det følgende.

2.2.1 RBAC-kernen

Kernen i RBAC-standarden beskriver det essentielle i rollebaseret adgangskontrol: At brugere tilknyttes til roller, samt at brugere opnår rettigheder ved at være rolleindehavere.

RBAC-kernen inkluderer også et krav om, at bruger-til-rolle-tilknytninger samt privilegium-til-rolle-tilknytning kan være mange-til-mange.

Et andet krav er, at muligheden for bruger-rolle-review, hvor det skal være muligt at se alle roller tilknyttet en given bruger såvel som alle brugere tilknyttet en given rolle.

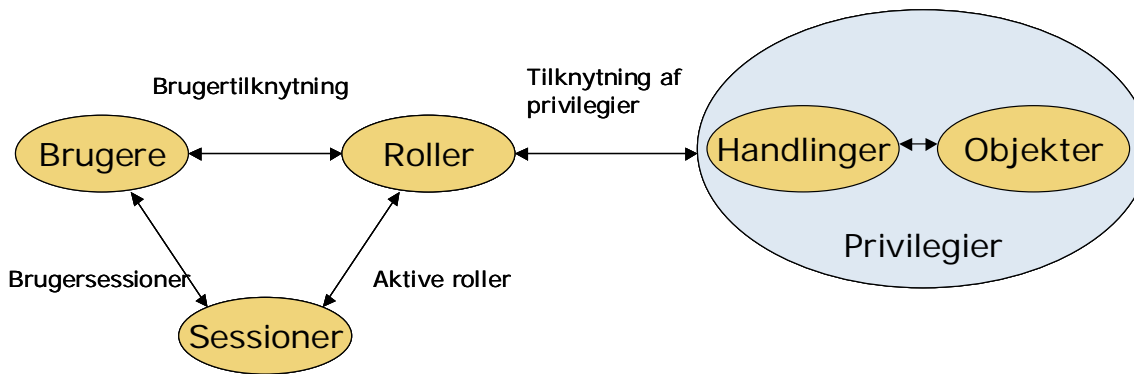
Et tilsvarende krav om privilegium-rolle-review, med muligheden for at se hvilke roller, der er tilknyttet et givent privilegium, kategoriseres i standarden som en avanceret review-mulighed og er valgfri i RBAC-kernen.

RBAC-kernen indfører også konceptet med brugersessioner, hvilket muliggør selektiv aktivering/deaktivering af roller for brugere.

Endelig kræver RBAC-kernen også, at brugere skal være i stand til at udnytte flere rollers privilegier samtidigt.

RBAC-kernen er en komponent, der kan kombineres til forskellige modeller sammen med andre komponenter, men den definerer også den basale model for RBAC, som illustreret i den følgende figur:

⁵ Dette forslag kan i skrivende stund fx hentes på <http://www.va.gov/rbac/docs/rbacstandard-ansit.pdf>



Figur 3. RBAC-kernen - den basale model for RBAC

Et privilegie kan betragtes som retten til at udføre en handling på/med et objekt. Til hvert objekt findes en mængde tilladte handlinger. En rolle består af tilknyttede privilegier. Et privilegie peger på den eller de roller, der anvender privilegiet. Brugere er tilknyttet roller, som tilsvarende peger på tilknyttede brugere. Brugere tilgår it-systemer via sessioner, som har en bruger tilknyttet. Til en session knyttes aktive roller, hvilket igen styrer brugernes rettigheder. Roller peger på aktive tilknyttede sessioner.

Nogle karakteristika for RBAC-kernen, som det er værd at nævne i forbindelse med figuren, er:

- Mange-til-mange relationer mellem individuelle brugere og privilegier.
- En session er en mapning mellem en bruger og et aktiveret delmængde af brugerens tildelte roller.
- Bruger/rolle relationer kan defineres uafhængigt af rolle/privilegium relationer.
- Privilegier er system/service-afhængige.

Som en opsummering kan det kort siges, at RBAC-kernen drejer sig om fælles begreber og definitioner af funktionalitet i forhold til, at individuelle brugere tilknyttes roller, samt at privilegier tilknyttes til roller.

2.2.2 Hierarkisk RBAC

Hierarkisk RBAC vil kun blive kort berørt. For en komplet oversigt over det fulde indhold i denne komponent henvises til selve standarden.

Hierarkisk RBAC stiller krav om, at roller skal kunne arve privilegium-rolle tilknytninger i flere led.

Der er følgende typer af rolle-hierarkier

- Generelt hierarkisk RBAC. Denne type giver blandt andet mulighed for, at en rolle kan nedarve privilegier fra flere roller.
- Begrænset hierarkisk RBAC. Denne type retter sig mod systemer med begrænsninger, der betyder, at generelt hierarkisk RBAC ikke kan understøttes. Typisk er her tale om hierarkier, der er struktureret som træer eller omvendte træer.

Anvendelse af hierarkier giver teoretisk set en mulighed for mere effektiv administration, fordi privilegier, som store grupper af brugere skal have adgang til, kan administreres ved etablering af fælles overordnede roller. Mere specifikke privilegium-tilknytninger kan så ske til roller, der nedarver de generelle privilegium-tilknytninger fra en overordnet rolle.

2.2.3 Statisk funktionsadskillelse

Statisk funktionsadskillelse anvendes til at håndhæve politikker for imødegåelse af interessekonflikter. I et rollebaseret adgangssystem kan en interessekonflikt opstå ved, at en bruger gennem tilknyttede roller opnår to eller flere privilegier, som er i konflikt med hinanden.

Med statisk funktionsadskillelse beskrives roller, som ikke må tilknyttes til den samme bruger. Et eksempel er, at en rolle, der tillader anvisning af en udbetaling, og en rolle, der tillader godkendelse af en udbetaling, ikke må tilknyttes samme bruger.

På grund af forskelligheder i definitionen af statisk funktionsadskillelse i forhold til RBAC-kernen og hierarkisk RBAC definerer standarden krav til statisk funktionsadskillelse for både RBAC-kernen og hierarkisk RBAC.

2.2.4 Dynamisk funktionsadskillelse

Dynamisk funktionsadskillelse drejer sig om at undgå interessekonflikter. Forskellen i forhold til statisk funktionsadskillelse ligger i, hvor der sker en begrænsning af, hvilke kombinationer af roller en bruger kan have.

Med dynamisk funktionsadskillelse er det i forbindelse med brugerens tilknytning af roller i en brugersession, at begrænsningen af, hvilke roller der samtidigt kan aktiveres for en bruger, håndhæves.

Det tidligere eksempel under statisk funktionsadskillelse, hvor en bruger ikke både måtte være tilknyttet roller til anvisning af udbetaling og godkendelse af udbetaling, vil ofte være for ufleksibelt, fordi behovet blot er, at brugeren ikke må godkende udbetalinger, som vedkommende selv har anvist til udbetaling. Med dynamisk funktionsadskillelse er det muligt at lade brugeren være tilknyttet begge roller, men lægge den begrænsning, at rollerne ikke må aktiveres samtidigt i en brugersession.

2.2.5 Funktionel specifikation

Den anden del af RBAC-standardens definerer den funktionalitet, som kræves af systemer for at leve op til RBAC-standardens.

Kravene falder i tre kategorier:

- Administrative handlinger – definerer krav til administrativ grænseflade med et tilhørende sæt af semantiske begreber, som giver evnen til at oprette, nedlægge og vedligeholde RBAC-elementer og RBAC-relationer.
- Administrativ revision – definerer krav til administrativ grænseflade med et tilhørende sæt semantiske begreber, som giver evnen til at foretage forespørgsler på RBAC-elementer og RBAC-relationer.
- Funktionalitet på systemniveau – definerer systemegenskaber til oprettelse af brugersession, herunder aktivering/deaktivering af roller, håndhævelse af begrænsninger på rolle-aktivering og udregning af en afgang.

Efter denne korte gennemgang af RBAC-standardens vil næste afsnit omhandle de konkrete danske fællesoffentlige anbefalinger vedrørende rollebaseret adgangskontrol.

3 anbefalinger vedrørende brug af rollebaseret adgangskontrol

Følgende anbefales i forhold til anvendelse af rollebaseret adgangskontrol:

- Det anbefales, at adgangsrettigheder baseres på roller og regler, således at rettigheder kun behøver at blive administreret for individuelle brugere i situationer, hvor roller og regler ikke kan anvendes⁶.
- Det anbefales, at der for systemer til administration af rollebaserede rettigheder stilles mindstekrav om, at de skal overholde RBAC-kernens definitioner og krav i RBAC-standarden.
- Det anbefales, at der ved anskaffelse eller udvikling stilles et mindstekrav om, at it-systemer, hvor det er relevant, skal understøtte rollebaseret adgangskontrol, som beskrevet i RBAC-kernen af RBAC-standarden⁷.

3.1.1 Bemærkninger i forhold til anbefalingerne

Det er vigtigt at bemærke, at disse anbefalinger relaterer sig til en række krav, der er defineret i RBAC-standarden, og som alle kunder og alle leverandører dermed har et fælles referencepunkt til. Det betyder ikke, at de anbefalede krav også anbefales som tilstrækkelige for at få en velfungerende løsning af opgaven med rolleadgangsstyring.

En organisation har i forbindelse med indførelse og anvendelse af rollebaseret adgangskontrol en række behov, hvoraf nogle kan adresseres ved hjælp af generelle krav, og andre måske er specifikke i forhold til den enkelte organisation. Ved at opfylde de ovenfor anbefalede krav i RBAC-standarden forventes det, at man kan dække en *del-mængde* af de generelle krav til rollebaserede adgangskontrolløsninger, som en organisation måtte have. Det kan således ikke tages som forudsætning, at løsninger, der overholder RBAC-standarden, også opfylder en organisations konkrete forretningsbehov, uden at der stilles yderligere krav til løsningen.

Anbefalingerne inkluderer ikke anvendelse af hierarkisk RBAC. Dette betyder ikke direkte, at hierarkisk RBAC frarådes. Teoretisk set rummer det administrative fordele i forhold til blot at anvende RBAC-kernen. Imidlertid har det ikke været muligt at identificere organisationer, hvor hierarkisk RBAC anvendes med succes. Der kendes dog til erfaringer med anvendelse af hierarkisk rettighedsadministration fra både udlandet og fra en større dansk offentlig institution. Disse erfaringer peger på praktiske problemer i forbindelse med indførelse og vedligehold af rolle-hierarkier i en organisationsstruktur, som ikke er meget statisk.

De ovenstående anbefalinger inkluderer heller ikke dynamisk funktionsadskillelse, selv om dette så absolut ses som anbefalelsesværdigt. Det skyldes, at det ikke er klart i hvor høj grad de tilgængelige produkter, der understøtter RBAC-kernen, også kan understøtte dynamisk funktionsadskillelse. Inkludering af dynamisk funktionsadskillelse, som krav kunne måske betyde en væsentlig reduktion i antallet af produkter, der kan vælges imellem.

3.1.2 Interoperabilitet og portabilitet

RBAC-standarden er konceptuel. Det betyder, at den kan anvendes i opbygningen af det rettighedsadministrative apparat hos en organisation og til at stille krav til it-løsninger. RBAC-standarden sikrer ikke i sig selv interoperabilitet og portabilitet. Til disse formål skal den kombineres med andre standarder, som f.eks. SAML, XACML og SPML såvel som en begrebsmodel for udveksling af rolle-

⁶ Et eksempel, hvor administration af rettigheder for individuelle brugere er nødvendig, kan være en sag, hvor det er sagens omstændigheder, der afgør, hvilke personer, som skal arbejde med den..

⁷ RBAC-kernen i RBAC-standarden og de krav, der afledes heraf, er beskrevet i afsnit 5.1 *Core RBAC*, kapitel 5 *RBAC Reference Model*, såvel som i afsnit 6.1 *Core RBAC*, kapitel 6 *RBAC System and Administrative Functional Specification* af American National Standard ANSI INCITS 359-2004.

information. Til trods for disse udeståender er den klare anbefaling stadig at indføre rollebaseret adgangskontrol. Anbefalingen begrundes af de administrative fordele, bedre sikkerhed og den fleksibilitet, som den enkelte organisation forventes at kunne opnå med anvendelse af roller, selvom det kun er koncepterne, der er standardiserede.

4 Implementering af rollebaseret adgangskontrol

Etableringen af en it-infrastruktur, der kan understøtte anvendelsen, er kun en del af indførelsen af rollebaseret adgangskontrol. En anden del er selve identifikationen af, hvilke roller og privilegie-tilknytninger, det giver mening af have i en organisation. RBAC-standarden beskæftiger sig ikke med dette.

Der er ikke etableret en bred praksis for identifikation af roller indenfor en organisation. Derfor indeholder dette dokument heller ingen decideret anbefalet metode til identifikation af roller. Der findes dog eksempler på, hvordan andre organisationer har gjort samt forslag til metodiske tilgange til at identificere roller indenfor en enkelt organisation. Videnskabsministeriet vil på et senere tidspunkt udsende et diskussionspapir i høring vedrørende dette i forbindelse med udbygningen af rammerne under OIO Referencemodel for tværgående brugerstyring.

Det er naturligvis også interessant at kunne anvende roller i forbindelse med tværgående løsninger. Det er et område, som der findes endnu mindre praksis for. Muligheder og overvejelser i forbindelse med at indføre og anvende tværgående roller vil kort blive diskuteret i det følgende afsnit.

4.1.1 Muligheden for at anvende tværgående roller

I forbindelse med interoperabilitet er det interessant at se på, om der kan defineres roller, som er gyldige på tværs af organisationer. Dette giver, at en bruger med en given rolle kan få adgang til data/transaktioner i flere forskellige organisationer. Dette er måske muligt for en rolle som *Borger*, men herudover ses det på nuværende tidspunkt som en ikke-mulig opgave på grund af en række forskelligheder imellem organisationer som fx i definition og navngivning af begreber, organisationsform, granularitet og gruppering af privilegier i tekniske løsninger med mere. Indenfor sektorområder med stor homogenitet, som fx sundhedsområdet, er det måske muligt at indføre fælles roller. Forudsætningen for roller, som kan anvendes fælles på tværs af organisationer er et stort begrebsdefinitionsarbejde og deraf følgende tilretninger i funktionsbeskrivelserne for de personer, som skal have tværgående roller tilknyttet.

Eksempelvis skulle man forvente, at en rolle som sygeplejerske godt kunne udnævnes til en fælles rolle, som sundhedsorganisationer vil lægge den samme betydning i. Imidlertid er der i dag nogle steder, hvor en sygeplejerske også har ordinationsret (ret til at tildele medicin), men sygeplejersker andre steder ikke har denne tilladelse. Her er en konflikt ved definition af en tværgående rolle. Skal rollen sygeplejerske have ordinationsret eller ej? Og i hvilket omfang påvirkes det daglige arbejde, behov for uddannelse etc. hvis en gruppe sygeplejersker, der i dag ikke har ordinationsret, skal have denne beføjelse som resultat af, at der skal anvendes ens roller på tværs af organisationer?

Det er vurderingen, at der i dag kun indenfor få områder findes et begrebsapparat af et omfang, så det kan være en forudsætning for definition af fælles roller. Hertil kommer arbejdet med at definere de organiske og funktionsmæssige begrænsninger (primært i fleksibilitet), som den enkelte organisation skal acceptere for at kunne indgå i et samarbejde omkring fælles roller. Efterhånden, som der opbygges mere erfaring med implementering af roller i individuelle danske offentlige organisationer, vil der komme et bedre grundlag for at afgøre på hvilke måder, rolle bedst kan anvendes i tværgående sammenhænge.

En anden mulig for at anvende roller i forbindelse med rettighedsstyring i tværgående løsninger, som ikke direkte kræver, at alle involverede organisationer anvender samme roller, vil kort blive diskuteret. Denne tilgang forudsætter, at rollerne defineres som summen af en række attributter (som fx organisatorisk tilhørsforhold, emne/fagområde, uddannelse, certificering/akkreditering, stilling etc.). Sagt på en anden måde: En bestemt række attributter definerer en rolle. Disse attributter, som skal være defineret i forhold til et fælles begrebsapparat, kan overføres⁸ på tværs af organisationer. Den enkelte organisation kan så ud fra en række tilgængelige attributter mappe brugeren ind i en eller flere af sine egne roller (såfremt der er tilstrækkelig information i de attributter, der er til rådighed). I eksemplet med sygeplejerske-rollen ovenfor

⁸ Disse attributter kan meget vel være personfølsomme, hvorfor overførslen i sådanne tilfælde naturligvis skal være underlagt passende sikkerhedsforanstaltninger.

kan ordinationsret defineres som en attribut. Nogle organisationer vil kræve denne attribut for at mappe brugeren ind i en sygeplejerske-rolle, mens andre ikke vil have dette krav. Det er endnu ikke klart, i hvor høj grad opsplnitning af roller i attributter kan lade sig gøre i forbindelse med digital forvaltning. Et eksempel, hvor det er gennemført med succes, er den amerikanske flåde. Det må antages at danske offentlige organisationer har en større mangfoldighed, og ikke de samme muligheder for at skabe homogenitet, som den amerikanske flåde. Der kan næppe drages direkte konklusioner for danske offentlige forhold ud fra den amerikanske flådes erfaringer, men dette område vil blive yderligere undersøgt i forbindelse med udbygningen af med OIO Referencemodell for tværgående brugerstyring.

En tredje måde at anvende roller til tværgående løsninger på ses allerede i brug i dag. Her har hver organisation sine egne roller, og eksterne brugere tilknyttes disse roller – blot ikke dynamisk, men via en lokal administrator i hver ekstern organisation. Dette ses pragmatisk som en løsning, der for nuværende i mange tilfælde er det mest oplagte valg.

5 Oversatte RBAC begreber

Komponent (eng. component): Refererer i denne sammenhæng til en af de centrale dele af RBAC egenskaberne: kerne RBAC, hierarkisk RBAC, relationer vedrørende statisk funktionsadskillelse og relationer vedrørende dynamisk funktionsadskillelse.

Objekter (eng. objects): Refererer i denne sammenhæng til enhver systemressource, som kan blive genstand for adgangskontrol. F.eks. filer, printere, terminaler, databaseoptegnelser mm.

Handlinger eller *Aktiviteter* (eng. operations): Beskriver en eksekverbar instans af et program, som efter anmodning kan udføre en funktion for brugeren.

Privilegier eller *Tilladelser* (eng. permissions): Beskriver en accept af, at der kan udføres en handling i forhold til en eller flere RBAC beskyttede objekter.

Rolle (eng. role): En rolle er en jobfunktion inden for en organisationel kontekst, som indeholder en associeret semantik omkring den autoritet og det ansvar, som er givet til den bruger, som rollen er overdraget til.

Bruger (eng. user): Bruger henviser i denne sammenhæng alene til en person. Dette af hensyn til enkelheden i foreliggende dokument, da brugerbegrebet også kan udvides til at omfatte maskiner, netværk eller intelligente autonome aktører.

Brugertilknytning: (eng. User Assignment (UA))

Tilknytning af privilegier: (eng. Permission Assignment (PA))

6 Appendiks A - Yderligere information

Dette fællesoffentlige arbejde i forbindelse med tværgående brugerstyring er beskrevet på

<http://www.oio.dk/arkitektur/brugerstyring>

Information om nogle af de aktiviteter inden for it-sikkerhed, som Videnskabsministeriet varetager findes på

<http://www.oio.dk/sikkerhed>

Information vedrørende arbejdet med at implementere en fælles standard for styring af itsikkerhedsprocesser i staten findes på

<http://www.oio.dk/itsikkerhed/isis>