

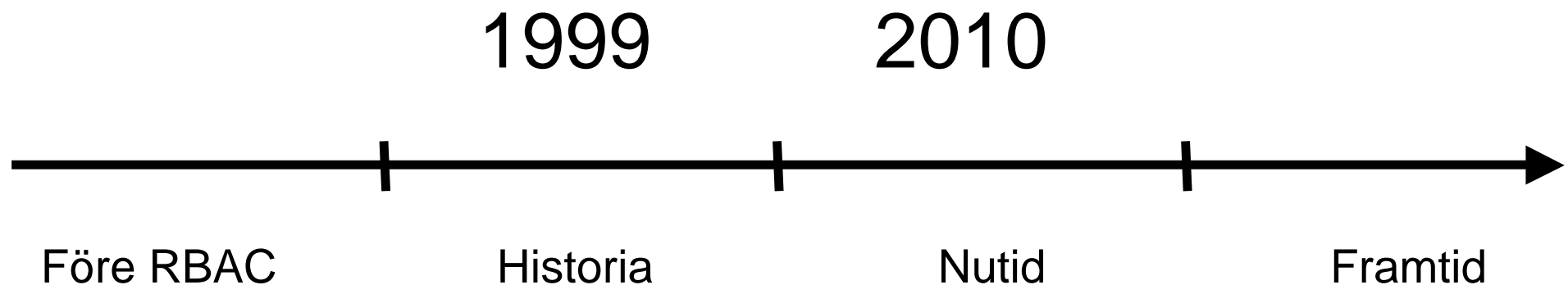
skandia :

Rollbaserad behörighet på Skandia

Om mig

- På Skandia sedan 2002
- Tidigare på Mijada och Icon Medialab
 - delvis som konsult på Skandia
- Arbetat med IT Säkerhetsarkitektur, lösningar för behörighet och säker elektronisk kommunikation

- Skandias arbete med behörighet
- Teknik
- Processer
- Erfarenheter



1999

2010

Före RBAC

Historia

Nutid

Framtid

- Behörighet baseras på ACL (Access Control List)
- Litar på behörighetskontroll i stordatorn
 - RACF
 - Egenutvecklade behörighetskontroller
- Egenutvecklade behörighetssystem i våra applikationer utanför stordatorn

1999

2010

Före RBAC

Historia

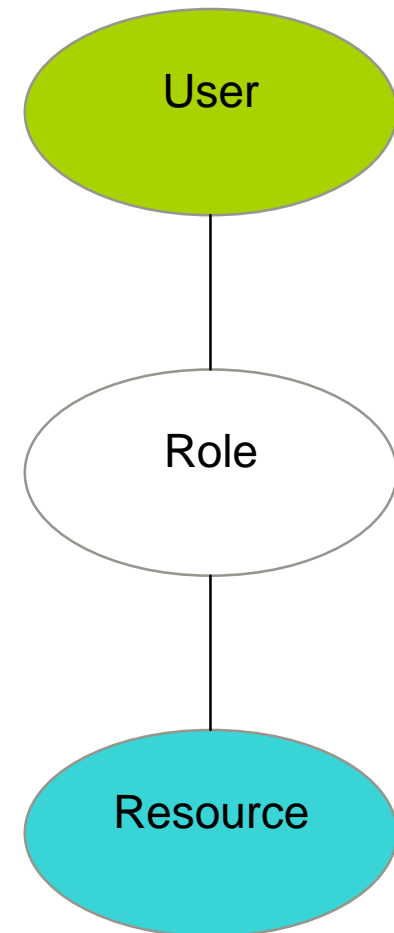
Nutid

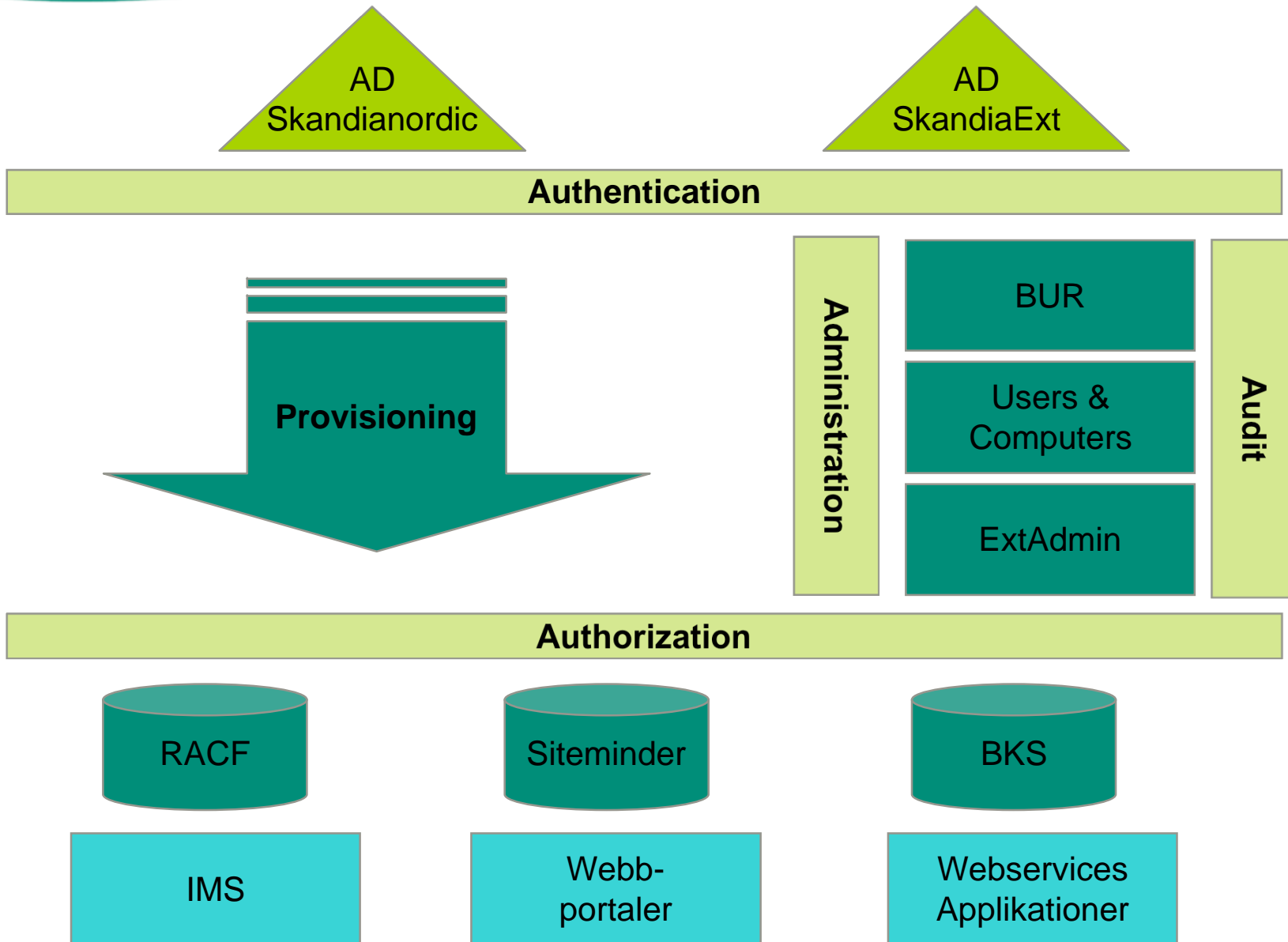
Framtid

- 1999 påbörjas ett projekt för behörighet
- RBAC (Role Based Access Control)
 - Behörigheten baseras på roller
- Centralt behörighetsregelverk
 - stöd för applikationer i stordator, klienter och andra servrar

Skandias stöd för behörighet enligt RBAC

- Kallat BKS (Behörighets Kontroll System)
- Är ett stöd för system som reglerar åtkomst till sina resurser
- Erbjuder
 - central administration av användarnas roller
 - API för åtkomst av användares resurser
 - provisioning till system med eget lokalt regelverk





Övergången till BKS

- Nya, egenutvecklade applikationer använde BKS
- Befintliga stordatorsystem gick gradvis över
- Integration av 3:e partsprodukter
- Integrationen av system pågår alltjämt..

Definition av resurser

- Definieras vid nyutveckling eller förvaltning av applikationer
- Ägs av Systemägare eller motsvarande
 - definierar vilka roller som ska ha åtkomst till resurserna
- Typer av resurser
 - Egenutvecklad funktionalitet
 - tolkas av applikationen som begränsar åtkomst
 - kan representera olika typer av funktionalitet (webservices, cobol-program etc.)
 - flexibel
 - IMS
 - URL

Utveckling och förvaltning av roller

- Rollägare med ansvar för specifika roller
 - definierar vilka användare som får rollerna
- Behörighetsforum
 - IT och verksamheten tillsammans
 - Ansvariga med mandat att ta beslut i verksamheten
 - Definierar vilka roller som ska finnas
- Gradvis definition av roller - ingen "Big Bang"

Process för tilldelning av roller

- Anställd
 - kan ansöka om behörighet
- Chefer
 - kan ansöka om behörighet
 - godkänner ansökan
- Rollägare
 - godkänner tilldelning av behörighet
- Behörighetsadministratör
 - tilldelar efter godkännande roller till användaren
- BKS
 - ger åtkomst till resurser i alla integrerade system

1999

2010

Före RBAC

Historia

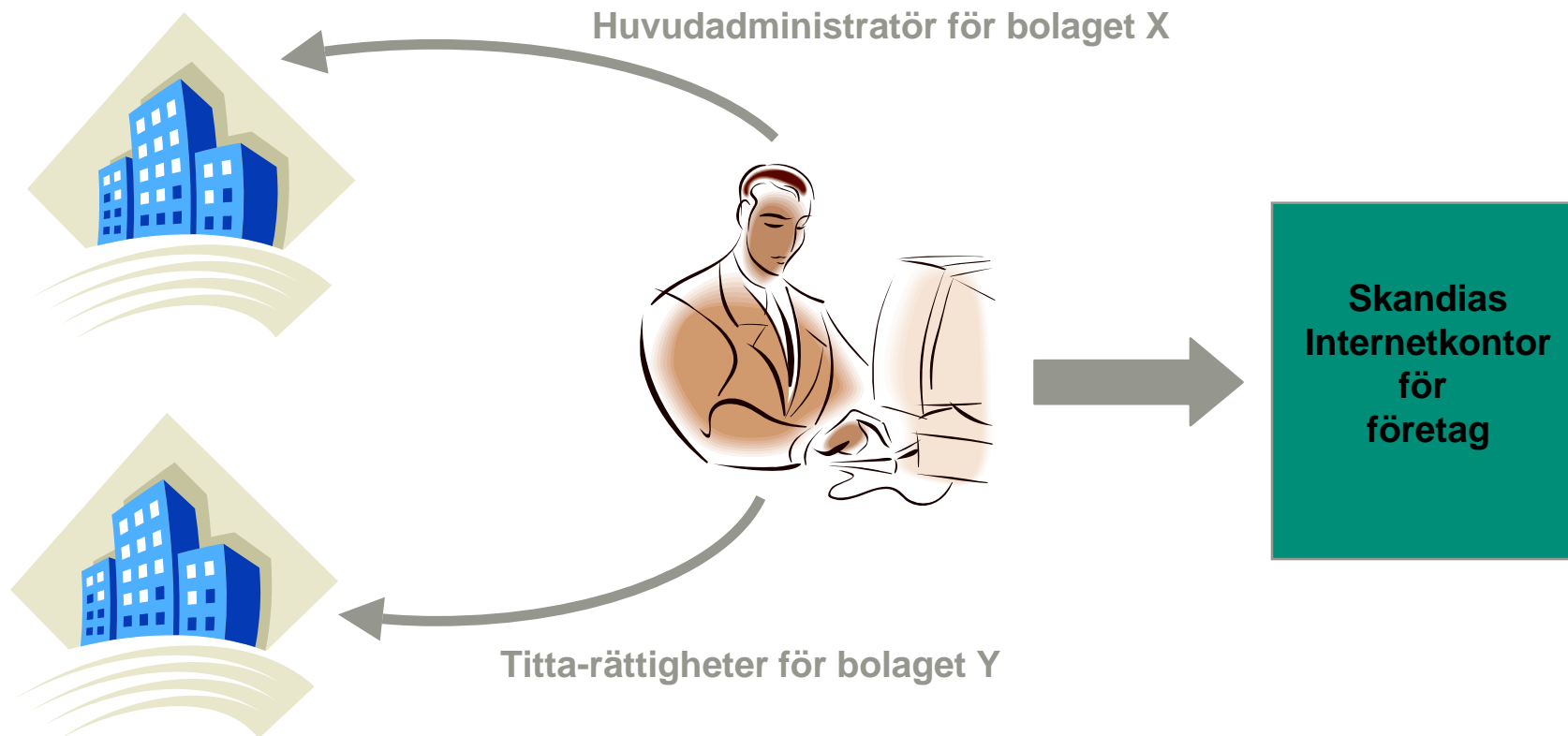
Nutid

Framtid

- Förvaltning av verktyg vi utvecklat
- Ökade krav ställs från
 - revision & compliance
 - bättre uppföljning och spårbarhet
 - verksamheten
 - bättre workflow för IM
 - kunder, samarbetspartner och leverantörer
 - högre granularitet
 - större flexibilitet
- Leverantörerna och produkterna har utvecklats

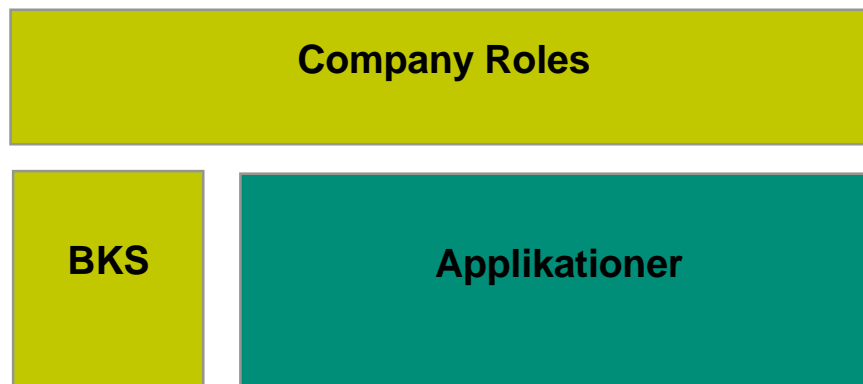
Krav från externa parter

- Erbjuder åtkomst av tjänster hos Skandias system
- Användare ska kunna ha olika roller i olika sammanhang



Krav från externa parter

- Behöver återanvända befintliga applikationer och tjänster
- Behörighet är implementerad enligt RBAC
- Stödsystem krävs



1999

2010

Före RBAC

Historia

Nutid

Framtid

- Uppfylla ökade krav
 - spårbarhet
 - workflow
 - uppföljning
 - fingranularitet
 - flexibilitet
- Bättre utnyttja de produkter som finns på marknaden

Flexibilitet och fingranularitet

- Finkorning styrning
 - enskilda avtal
 - attribut hos kundernas personal
- Flexibla regler
 - enklare kunna ändra i uppsatta regler
- "Company Roles" räcker inte
- ABAC (Attribute Based Access Control) med XACML (eXtensible Access Control Markup Language)

Uppföljning, workflow och uppföljning

- Spårbarhet
 - bättre möjlighet till audit för revision
- Workflow
 - effektivare och säkrare hantering för tilldelning av behörighet
- Uppföljning
 - säkrare borttag av identiteter och behörighet
- IAM-system från många leverantörer på marknaden

Utmaningar

- Svårt att få engagemang hos verksamheten
 - Att användarna har för lite behörighet = stort problem
 - Att användarna har för mycket behörighet = litet problem
"gör det inte ont gör man inget åt det"
- Olika delar av organisationen har olika behov under olika perioder
- Initiativ kommer från olika delar av bolaget
 - svårt att ena för finansiering

Tips inför "förhandling" med verksamheten..

- Riskerar kostsam förvaltning
- Risk för bedrägerier
- Riskerar brott mot interna och externa regelverk

Tips

- Hitta engagemanget hos verksamheten
 - Utse en General på verksamheten
- Se inte behörighet som ett tekniskt problem
- Bygg upp gradvis - ät elefanten i bitar

Avslutningsvis - Drivkrafter

- Högre effektivitet
- Sänkta kostnader
- Efterföljnad av regelverk

Något vi behöver lägga mer kraft på!

Tack för mig!
Frågor?

mats.andersson@skandia.se