

# Identitetsføderering – en forutsetning for en vellykket SOA?

## Hva er identitetsføderering?

Den kinesiske muren var helt fram til 1700-tallet en sikkerhetsteknologi som holdt uvedkommende ute. I dag er uvedkommende på nettverket om man liker det eller ei. Gjenkjennelsen av- og tillitt til- identiteten til de som er på nettverket er en måte å avgjøre hvem som skal ha tilgang til tjenester. Identitetsføderering er et begrep som ofte brukes der man har behov for å utveksle godkjente identiteter for å få tilgang til en tjeneste og der tjenesteleverandøren stoler på autoriteten som har autentisert identiteten til konsumenten. Et hverdagslig eksempel er den globale "føderasjonen" av nasjoner som krever et gyldig pass som bevis på identiteten til den som ønsker adgang til et land. De fleste land stoler på passutstederen, men i noen tilfeller kreves også tilleggsopplysninger godkjent i forkant og synliggjort gjennom et visum for å få adgang til landet. Analogien gjelder også for sikker Web Service basert samhandling internt og mellom virksomheter.



## Utfordring 1

### Sikkerhet stopper tradisjonelt ved webserveren

Web Service arkitekturen medfører at det ikke lengre er tilstrekkelig å sikre kommunikasjonen mellom tjenestekonsumenten og tjenesteleverandøren. Web Service arkitekturen krever at man implementerer ende-til-ende sikkerhet da en Web Service selv kan være en Web Service konsument dvs. bruke tjenester levert av andre tjenesteleverandører. Arkitekturen krever dermed at identiteten til den opprinnelige konsumenten kan autentiseres, er portabel og kan spores gjennom alle tjenesteleverandørledd. Dette er spesielt viktig i helsesektoren som må ivareta et strengt sikkerhetsregelverk.

## Utfordring 2

### Forskjellige typer sikkerhetsprotokoller

Dessverre er det ofte slik at legitimasjon dvs. bevisførsel for identiteten man har i en virksomhet ikke er implementert iht. en standardisert protokoll som alltid virker på tvers av sikkerhetsdomener. For eksempel vil de virksomheter som benytter Active Directory ofte bruke et Kerberos token som legitimasjon på at brukeren er autentisert. Legitimasjonen utstedt fra egen organisasjon er som regel ikke tilstrekkelig dersom man ønsker å få tilgang til en tjeneste levert fra en annen organisasjon som har et annet sikkerhetsregime.

## Utfordring 3

### En felles brukerkatalog løser sikkerhetsutfordringen?

Tilsynelatende tror mange at etableringen av en felles katalogtjeneste i virksomheten (om det er mulig) vil løse sikkerhetsutfordringene ved intern og ekstern samhandling. Det er vanskelig å se hvordan etableringen av en felles brukerkatalog bidrar til sikker samhandling på tvers av organisasjons- og sikkerhetsgrenser, når sikkerhetsprotokollene som benyttes er ofte forskjellige og ikke kan benyttes med enkelhet på tvers av sikkerhetsdomener. Det er også svært vanskelig å se hvordan dette reelt sett kan oppnås når de fleste store organisasjoner ofte har et titalls systemer med egne autentiserings- og autorisasjonsmekanismer. Det er betimelig å stille spørsmål om etableringen av en felles brukerkatalog løser de riktige problemstillingene når man ønsker å anvende Web Services i et tverr-organisatorisk samhandlingsperspektiv. Det er også rimelig å spørre hvorvidt innføring av en felles katalogtjeneste bidrar til løsekoblinger mellom Web Service konsumentene og Web Service leverandørene.

## Utfordring 4

### En PKI løser sikkerhetsutfordringen?

En annen myte som synes å dominere IT tenkningen, er at etableringen av en "Public Key Infrastructure" (PKI) og anvendelse av digitale sertifikater alene løser sikkerhetsutfordringen ved

tværr-organisatorisk samhandling. En av hovedutfordringene med denne tilnærmingen, er at det er svak støtte for løsekoblinger mellom X509 som autentisert identitetsbevis og behovet for stor fleksibilitet ift autorisasjon hos tjenesteleverandøren. Autorisasjonsmodellen ved sertifikatbruk kan bare baseres på de opplysningene som ligger i sertifikatene. Det er vanskelig å propagere egendefinerte tilleggsopplysninger sammen med sertifikatet. Dette gir svakere fleksibilitet og færre muligheter for avanserte autorisasjonsmodeller. En annen utfordring ved anvendelse av en PKI i et Web Service perspektiv og som er en mulig større utfordring, er at man som tjenestekonsument stiller krav til tjenesteleverandør om å implementere en PKI eller visa versa. Dette øker forvaltningsomfanget i en SOA og begrenser skalerbarheten, da tjenesteleverandør må kunne kjenne igjen sertifikatet som blir sendt med forespørselen fra tjenestekonsumenten. Man bidrar til å forsterke en implisitt sterk binding mellom tjenestekonsumenten og tjenesteleverandøren.

## Utfordring 5

### En brukerkonto alle steder

Det er ofte en forutsetning at man har en brukerkonto hos tjenesteleverandøren hvis man ønsker å få tilgang til en tjeneste. Noen identitetsføderingsløsninger har funksjonalitet for å opprette brukerkonti fortløpende etter behov hos tjenesteleverandøren basert på identitetsbeviset og tilleggsopplysninger som propageres til tjenesteleverandøren. IAM (Identity Access Management) prosjekter inneholder ofte aktiviteter og infrastrukturimplementering for å synkronisere brukerkonti mellom alle interne brukerdatabaser, noe som kan være en formidabel utfordring å gjennomføre. I en "Software as a Service" (SaaS) verden er det lite hensiktsmessig å gjennomføre kompliserte og proprietære brukerkonti synkroniseringsprosjekter hovedsaklig pga av to forhold a) slike løsninger skalerer ikke og b) er lite hensiktsmessige å gjennomføre pga av kompleksitet, kostnader og tiden det tar å gjennomføre. Man bør da heller vurdere identitetsføderingsløsninger som kan håndtere dette vha standarder som "Service Provisioning Markup Language" eller har innebygde mekanismer for "just-in-time" opprettelse av brukerkonti.

### Identitetsfødering og SAML som en mulig løsning

Autentiseringsmodell man velger internt er ofte "proprietær" dvs. ofte ikke understøtter tværr-organisatorisk samhandling på en standardisert måte f.eks. Kerberos og NTLM. En Web Service basert SOA må dermed være i stand til å transformere identitetsbeviset brukt i en sikkerhetsprotokoll til et annet identitetsbevis basert på en standard sikkerhetsprotokoll f.eks. "Security Assertion Markup Language" (SAML).

I en Web Service basert SOA bør en Web Service konsument kunne benytte standarder som WS-Trust for å be om å få en standard identitetsbevis uavhengig av autentiseringsprotokoll som brukes. Det godkjente sikkerhetsbeviset bør kunne berikes med flere opplysninger etter behov som deretter benyttes som autorisasjonsgrunnlag til tjenestene. Hos tjenesteleverandøren bør man kunne validere og "konsumere" identitetsbeviset slik at tilgang til tjenesten kan gis. En slik løsning krever at identitetsføderingsløsningen i de samhandelnde virksomheter er basert på standarder og kan gi tilgang til en WS-Trust basert "Security Token Service" (STS). En STS brukes til utstedelse og validering av SAML identitetsbevis og er ofte en integrert komponent i en identitetsføderingsløsning.

### Konklusjon

Sikkerhetsarkitekturen i en SOA bør inneholde en identitetsføderingsløsning som kan oppfylle det viktige SOA prinsippet om løsekoblinger mellom komponenter i sikkerhetsarkitekturen bl.a. brukerdatabaser, sikkerhetsprotokoller, autorisasjonsmodeller, Web Service tjenester og konsumentapplikasjoner. Mangelen på denne løsekoblingen medfører store utfordringer bl.a. skalerbarheten ved opptak av SaaS baserte tjenester og unødig kompliserer integrasjoner som må til for å etablere en skalerbar, effektiv og sikker Web Service basert samhandling internt og på tvers av virksomheter. Dermed blir en standards basert identitetsføderingsløsningen en viktig forutsetning for en fremtidsrettet SOA.

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](mailto:acando@acando.no)

