Serviceorienteret sikkerhed i teori og praksis

Case: Elektronisk Tinglysning

Forfatter og Projektchef, Henrik Hvid Jensen, Devoteam Consulting,
henrik.hvid@devoteam.dk,

Blogs, nyhedsbrev og konferencetilbud på www.soanetwork.dk

DEVOTEAM CONSULTING CONNECTING BUSINESS & TECHNOLOGY

Dagsorden

- Tinglysningen i dag og i fremtiden
- Opbygningen af elektronisk tinglysning
- Serviceorienteret sikkerhed i teori og praksis
  - Udvalgte sikkerhedsovervejelser
  - Beskedorienterede webservices
  - Elementvis kryptering og signering
  - Single sign on i et webservicemiljø
  - Underskrifter
    - Underskrift i tredje parts miljø
    - Underskift af udvalgte dele af dokumentet

Tinglysningens opgaver

- Rettigheder over objekter skal tinglyses for at opnå beskyttelse mod aftaler om objektet
  - Rettigheder der ikke tinglyses udsætter sig for at blive fortrængt af senere tinglyst rettighedshavere
  - Ejendom, biler, andelsbolig, personer, testamenter, fuldmagter
- Typer af dokumenter (eksempler)
  - Overdragelse af ejendom (Skøde)
  - Pantstiftning (Pantebreve)
  - Rettigheder over ejendom (Servitutter)
- Omfang i dag
  - 4-5 millioner anmeldelser pr. år
  - Værdi af 6 mia. kr.
- Tingbogens troværdighed skyldes statens erstatningsansvar
  - Brugeren skal kunne indrette sig i tillid til tingbogens oplysninger
    - Enten opnå den angivne retsstilling
    - Eller modtage økonomisk kompensation for tab forårsaget af fejlagtigt registreret data
      - 2002 : 1,1 mio, 2003 : 0,5 mio, 2004 : 1,7 mio
- Grundlæggende ret at oplysninger er offentligt tilgængelige

Overordnet arbejdsgang i dag

- Modtagelse af dokument
  - Papirbaseret
  - Indførsel i dagbogen
- Prøvelse
  - Er formkrav overholdt?
  - Kan dokumentet efter sin natur overhovedet tinglyses?
  - Er den åbenbart overflødig?
  - Er udstederen berettiget til at råde over ejendommen eller den pågældende ret?
  - Opfylder rettigheden diverse lovkrav?
  - Kan den opnå ønsket prioritetsstilling?
- Indførsel i tingbogen
  - Alene summariske oplysninger registreres i it-system
  - Påtegning på dokumentet
    - Sidenummer samt oplysning om at dokumentet er tinglyst og datoen for tinglysningen
- Efterbehandling
  - Genpart sættes i aktmappe
    - Papirbaseret genpart af samtlige gældende dokumenter for hver enkelt fast ejendom
  - Tinglyste dokument returneres til anmelderen

Fundamentale ændringer indenfor tinglysning

- **Centralisering**
  - Fra 82 embeder til én Tinglysningsret i Hobro

- **Digitalisering**
  - Udelukkende tinglysning af digitale dokumenter
    - ”Traditionelle” dokumenter kan vedhæftes i elektronisk form
  - Digital signatur er omdrejningspunktet
    - CPR og CVR nummer kræves til den helt grundlæggende prøvelse om ret til at disponere
    - Man kan kun tinglyse med digital signatur
  - Nuværende akt digitaliseres ved indskanning i PDF-dokumenter

- **Automatisering**
  - Prøvelsen foretages af 200 automatiske kontroller
    - Følger de hidtil gældende regler
  - Fokuserer på at automatisere 70% af tinglysningerne
    - Det er de vanskelige 30% der resterer
    - Manuel behandling

Forventede forbedringer i serviceniveauet

- Bygget til at samarbejde med mange forskellige interessenter
  - Realkredit, Banker, Advokater, Ejendomsmægler, Kommuner, SKAT, Landinspektører, Kort og Matrikelstyrelsen, Borgere, mindre virksomheder …
- Professionelle aktører (banker, realkreditinstitutter, advokater og ejendomsmæglere)
  - Kan integrere med e-TL fra egne systemer
  - kan foretage anmeldelser og straks modtage svar fra Tinglysningen om resultatet af den automatiserede prøvelse på "egen skærm".
  - Grundlag for at digitalisere den samlede sagsbehandling
    - Det papirløse huskøb
    - Automatisere administrative og rutineprægede opgaver
- Borgerne
  - Oplevelsen af en hurtigere tinglysningsproces
  - Bedre rådgivning på det tidsmæssige forløb
  - Forenkling af en ejendomshandel
    - Lettere at se, hvilke rettigheder der er tinglyst på ens ejendom
- Ensartet service.
  - Sagsbehandlingstiden vil være ens i hele landet
  - Fortolkning af formalia vil være den samme
- Mindre følsomt over for perioder med særligt mange tinglysninger
  - f.eks. ved konverteringsbølger

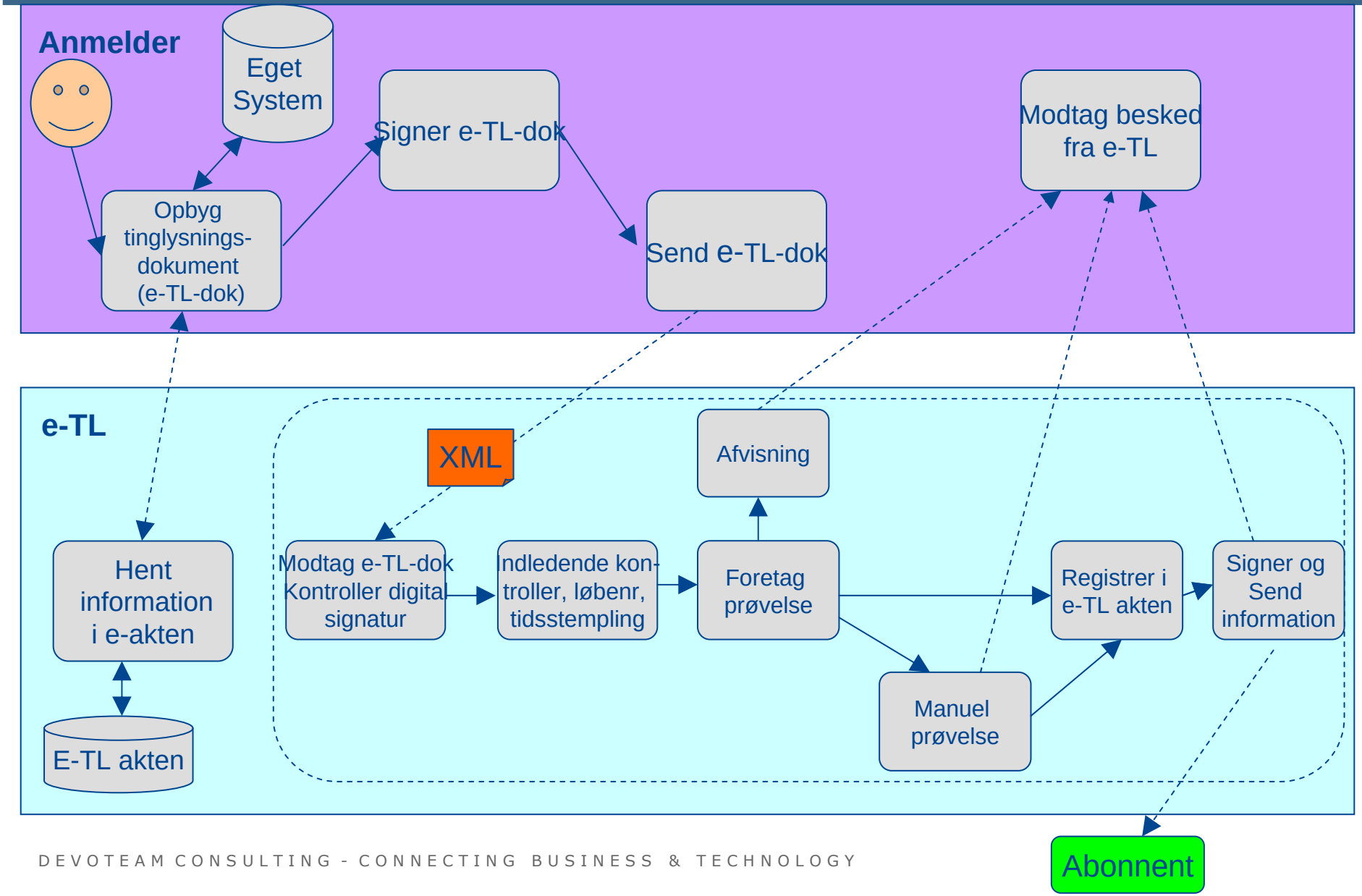
Business casen vedr. elektronisk tinglysning

- Digitaliseringen af tinglysningen vil medføre væsentlige besparelser hos Domstolene
  - Fra ca. 400 medarbejdere til 150 medarbejdere

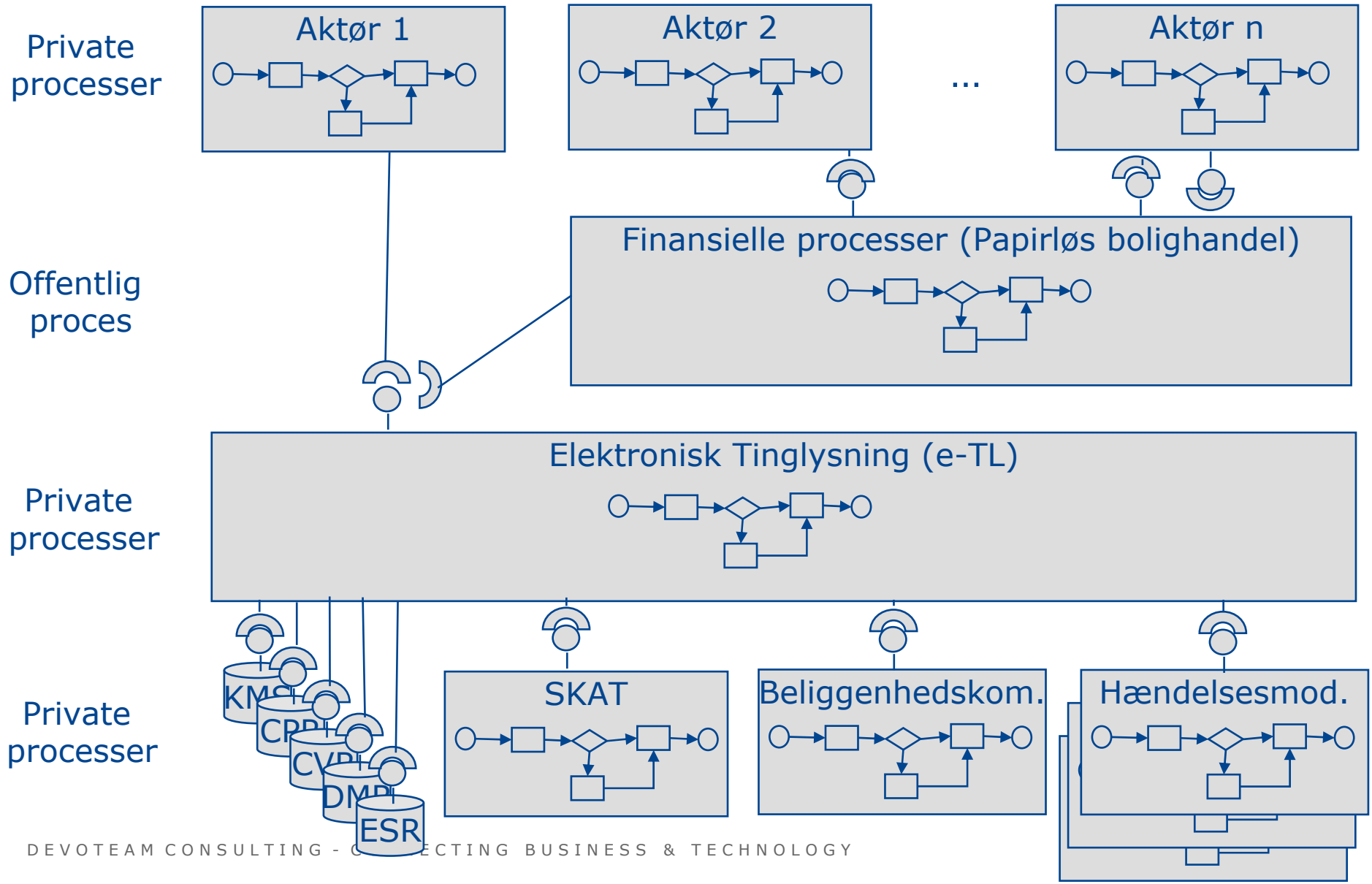
- Samfundsmæssige besparelser er højere
  - Ekspeditionstiden for tinglysning falder fra op til 14 dage til få sekunder
    - Gennemsnit i dag er 5 dage
  - Anslået til 300-400 millioner kr. om året
    - Et reduceret tidsforbrug for medarbejderne hos de professionelle aktører
      - Automatisk indhentning af informationer
      - Automatisk udfyldelse af elektroniske dokumenter/formularer.
      - Færre afbrudte arbejdsprocesser og kundemøder
      - Bortfald af kopiering, kuvertering, udarbejdelse af følgebreve m.m..
      - Ingen ekspeditioner til og fra arkivet
    - En reduktion i direkte omkostninger (materialer og porto m.m.)
    - Sparede finansielle omkostninger for borgeren ved en hurtigere tinglysningsekspedition (estimeret til 100 mio kr).
      - Bankgaranti i kortere tid
      - Rentetab på deponering af salgsprovenue

- Samlet pris for e-TL indtil 2012 er ca. 250 millioner kr.

Generisk arbejdsgang i e-TL



Orkestering - Praksis



Sikkerhed i teori og praksis

CONNECTING BUSINESS & TECHNOLOGY

Dagsorden

- Tinglysningen i dag og i fremtiden
- Opbygningen af elektronisk tinglysning
- Serviceorienteret sikkerhed i teori og praksis
  - Udvalgte sikkerhedsovervejelser
  - Beskedorienterede webservices
  - Elementvis kryptering og signering
  - Single sign on i et webservicemiljø
  - Underskrifter
    - Underskrift i tredje parts miljø
    - Underskift af udvalgte dele af dokumentet

Udvalgte sikkerhedsovervejelser ved serviceorientering

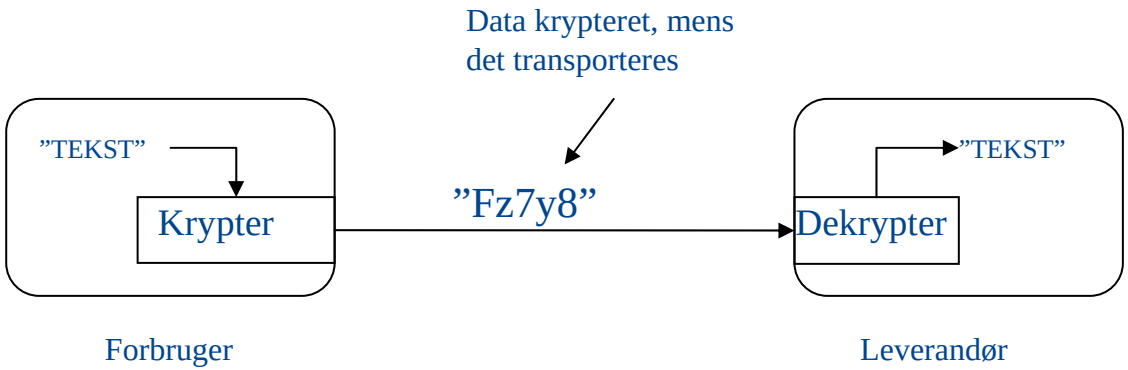
- Web Services vil tilføje hundredvis af enkelte services til virksomhedens it-miljø,
  - Web Services distribuerede natur vil gøre det endnu mere vanskeligt at håndhæve sikkerhedspolitikker.

- Sikkerhedsløsningen skal understøtte fleksibiliteten i at kunne samarbejde med den rette partner på det rette tidspunkt.
  - Målet er, at deltagere i et Web Service-miljø let kan bygge *interoperable* og *sikre* løsninger ved brug af heterogene systemer.
  - Løses på en omkostningseffektiv facon både for virksomheden såvel som for partnerne.

- Fundamentale sikkerhedsprincipper kræver, at en service autentificerer en forbruger.
  - Servicen og dets forbruger risikerer derved at blive tæt koblet, medmindre sikkerheden selv kan håndteres på en løst koblet facon.
  - Hvis hver Web Service og applikation udviklet i værdikæden kræver en unik tilgang, vil potentielle fordele blive tabt på grund af omkostningerne til at bygge og styre den krævede infrastruktur.

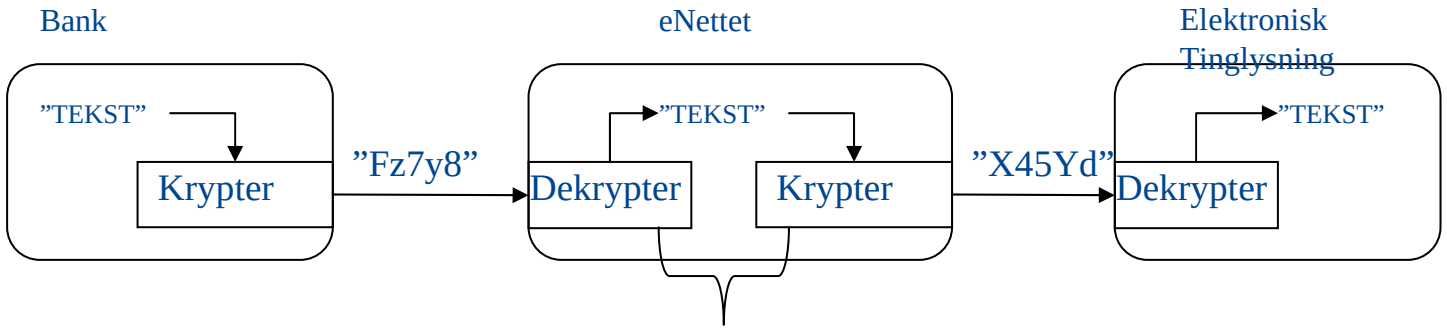
Forbindelsesorienterede webservices

- Traditionelle applikationer er *forbindelsesorienterede*,
  - Tillader, at mange sikkerhedsdetaljer implementeres på forbindelsesniveauet
  - Kræver en direkte forbindelse mellem serviceleverandøren og forbrugeren.
- I dag er de fleste Web Services synkrone punkt til punkt-løsninger, som bruger SOAP over HTTP.
- Mange virksomheder beskytter Web Services med veletablerede internetbaserede sikkerhedsværktøjer såsom SSL/TLS
  - Fungerer i en sikkerhedssammenhæng, der er den samme som på internettet.



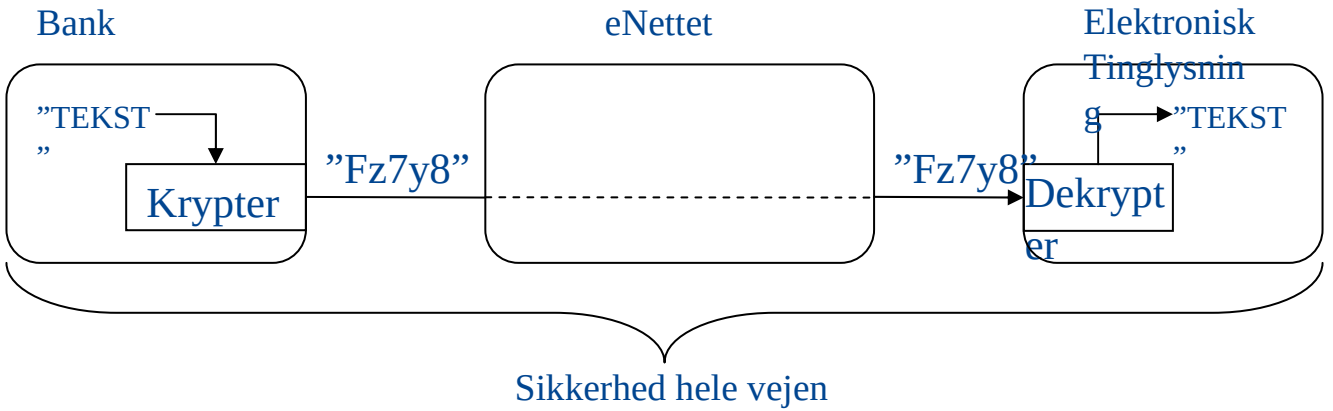
Beskedorienterede webservices

- Mere avancerede Web Services er *beskedorienterede*,
  - uden sikkerhed for at der er en direkte forbindelse mellem serviceleverandøren og forbrugeren.
  - Traditionelle tilgange til at imødegå sikkerhedsudfordringerne er ikke velegnede eller er utilstrækkelige for en Web Service-sikkerhedsarkitektur.
  - SOAP er som udgangspunkt uafhængig af de underliggende kommunikationslag.
  - Forskellige kommunikationsteknologier kan bruges i forbindelse med en SOAP-besked, der bevæger sig over mange led.
- Sikkerhedsinformation tilgængelig efter der ikke mere er forbindelse til afsenderen
  - Sikkerhedsinformation vedligeholdes over en længere periode
  - Kan verificeres på et vilkårligt tidspunkt i den periode.

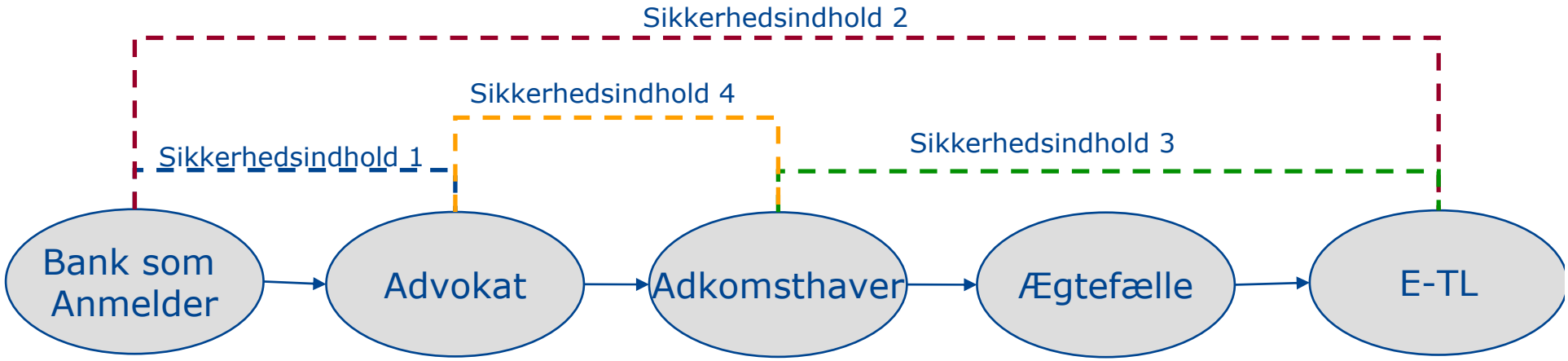


Sikkerhed hele vejen

- En komplet Web Service-sikkerhedsmekanisme skal tilbyde sikkerhed *hele vejen* fra leverandør til forbruger
- Flytte sikkerheden væk fra netværkslaget og ind i højere lag, hvor selve beskeden bevæger sig.
  - Tillader sikkerhedskoncepter at blive implementeret uafhængigt af en speciel netværks- eller transportprotokol.
  - Kryptering forblive uafhængigt af, om beskeden sendes ved brug af HTTP, SMTP eller andre protokoller.
  - Netværks- og transportuafhængig sikkerhed er krævet for alle beskeder, der transporteres via mere end én protokol på dets vej til den endelige modtager.
- WS-Security beskriver, hvordan webservice-sikkerhed opnås hele vejen fra afsender til modtager.



Elementvis kryptering og signering



Flere underskrifter på et dokument - XML Signatur

- Underskrift skal kunne påføres i forskellige systemer på forskellige tidspunkter
- E-TL bruger XML Digital Signatur
  - Man kan signere et komplet XML-dokument
  - Man kan signere et enkelt element i et XML-dokument
  - Man kan signere indholdet i et XML-element
  - Man kan signere ikke-XML-data (f.eks. jpg-billeder)
  - Underskriften er en del af XML-dokumentet
  - Flere kan tilføje informationer, der underskrives individuelt
    - Anmeldelses- og afgiftsinformation tilføjes efter debitors underskrift
- Al information signeres med Tinglysningsrettens digitale signatur
  - Dokumentet kan sendes rundt mellem uafhængige interessenter
    - Alle kan kontrollere signaturen
    - Man kan tilføje egen information og beholde tinglysningens signatur

Problemer ved digital signatur

- Digital signatur er ikke mobil
- Ikke alle har en Digital signatur
- Imødegås ved tre initiativer
  - Fuldmagtsordningen
  - Anmelderordningen
  - Underskriftmappen

Fuldmagtsordningen

- Fuldmagt indsendes på papir til Tinglysningsretten
  - Kan også dannes på portalen
  - Fuldmagten indskannes og OCR-læses
  - Fuldmagten kontrolleres og lagres i fuldmagtsbogen

- Fuldmagten er designet til at være generel elektronisk fuldmagt
  - Fuldmagtshaver
    - CPR/CVR
  - Fuldmagtsgiver
    - CPR/CVR
  - Omfang af fuldmagten
    - XML-dokument der kan defineres af enkelte myndigheder
    - Separat ekstern webservice kan kaldes til kontrol
  - Tildeles et unikt nummer
  - Kan hentes via webservice-kald

- En anmeldelse skal angive, at der tinglyses i henhold til fuldmagt
  - CPR-nummer på den digitale signatur kontrolleres

Anmelderordningen – Den valgte løsning

- Virksomheder med specielt forretningsformål kan anmelde uden kundens signatur
  - De garanterer, at de har den rette aftale med kunden
  - Erstatningsansvar
    - Overtager statens objektive erstatningsansvar
- Medarbejder- eller virksomhedscertifikat oprettes i e-TL
  - Virksomheden udnævner en digital signatur til administrator
    - Opretter hvilke certifikater der har lov til at anvende anmelderordning
      - Medarbejder- eller virksomhedscertifikat
    - Kan angive beløbsgrænse
    - Antal krævede underskrifter

Den rigtige webservice-løsning – Fælles forståelse
Autentifikation og autorisation over flere led

- Adgang til en Web Service skal besluttes, baseret på informationer om slutbrugeren

- Web Service må have adgang til information, der gør den i stand til at træffe autorisationsbeslutning.
  - hver enkelt virksomheds unikke relationer med brugeren beskyttes.
  - Oplysninger om identiteten på brugeren er ikke nødvendig, relevant autorisationsinformation er tilstrækkeligt.

- Hvert led i en Web Services orkestrering kan være ejet af forskellige enheder,
  - det forventes, at de har hver deres modeller, systemer og standarder for autentificering.
  - Troværdige mekanismer, hvormed disse adskilte modeller kan udveksle identiteter.
  - Da autentifikationsmodeller kan variere, må et sådan system også være løst koblet.
  - Godt designede Web Services skal være fleksible i forhold til deres forventninger omkring andre systemers autentifikationsmodeller.

- Autentifikations- og autorisationsinformationen følger kaldet på tværs af applikationer, netværk og organisationer
  - Videresende autorisationsinformation om, at anmelderen er en autoriseret medarbejder og derfor skal have adgang til at anmelde via anmelderordningen

Billetter i SAML

- Udtrykker information omkring autorisation og autentifikation såvel som attributter omkring slutbrugeren
  - Information om en autentifikations- eller autorisationshandling, der er sket tidligere
    - ”Bruger X er autentificeret ved brug af password klokken Y”.
  - Ved at autentificere én gang og genbruge denne autorisation for efterfølgende Web Services kan ”single-sign-on” for Web Services opnås.
- Autentifikationspåstand
  - Udstedt af en autentifikationsservice, der erklærer, at identiteten af en bruger eller en Web Service er blevet autentificeret til at tilgå beskyttede ressourcer
  - Autentifikationspåstanden drejer sig kun om identiteten af entiteten.
  - Behøver ikke indeholder ikke nogen information om emnet.
- Attributpåstande er genereret af en attributservice.
  - Verificerer, at en bruger eller Web Service besidder
    - statiske attributter f.eks. jobposition eller tilknytning til en virksomhed
    - dynamiske attributter såsom en forbrugers bankkontosaldo eller en forhandlers kvartalsvise salg.
  - Kræver fælles forståelse for, hvad f.eks. en indkøbschef er mellem de involverede parter
  - SAML specificerer ikke selv nogen sikkerhedsattributter.
  - SAML-brugere skal designe deres egne sikkerhedsattribut-namespace
- En autorisationsbeslutningsservice
  - samler autentifikationspåstande, attributpåstande og autorisationspolitikker og genererer autorisationspåstande, som definerer, hvilke ressourcer en bruger/Web Service har tilladelse til at tilgå.

Underskriftmappen

- Anmeldelser der kræver flere underskrifter, kan placeres i underskriftmappen
  - Angiver hvilke roller som et CPR/CVR nummer skal underskrive for
- Underskrivere kan besøge underskriftmappen uafhængigt for at påføre sin digitale signatur
  - Besked til opretter om hver ny påført underskrift
  - Dokument ugyldigt hvis signatur trækkes tilbage
- Hvis tegningsregler for virksomhed kræver flere underskrifter
  - Anmelder ved ikke hvem som vil underskrive
    - F.eks. *2 underskrifter fra direktionen* eller *direktør sammen med et medlem fra bestyrelsen*
  - Opretter antal roller med korrekt CVR-nummer
  - Vælger rolle og påfører medarbejder eller personligt signatur
    - Stillet krav om at medarbejder signatur skal indeholde CPR
  - Tinglysningsretten kontrollerer korrekt CPR-nummer i henhold til tegningsregler
    - Manuel kontrol sker gennem automatisk opslag på rigtig hjemmeside hos CVR
    - CVR har ikke tegningsregler i struktureret format, så ingen webservice er mulig
      - Ca. 1.000-2.000 manuelle opslag om dagen
      - Ingen mulighed for automatisk tinglysning af virksomheders dispositioner over egne aktiver
    - CVR som en Trust-service?
- Designet til at være en fælles offentlig underskriftmappe

Opsummering

- Sikkerhed afgørende for virksomhedens fleksibilitet
- Sikkerhed skal være løst koblet
- Sikkerhed på tværs af teknologier, netværk og organisationer bliver en nødvendighed
- Sikkerhedsstandarder en nødvendige for at bygge bro mellem heterogene sikkerhedsmiljøer

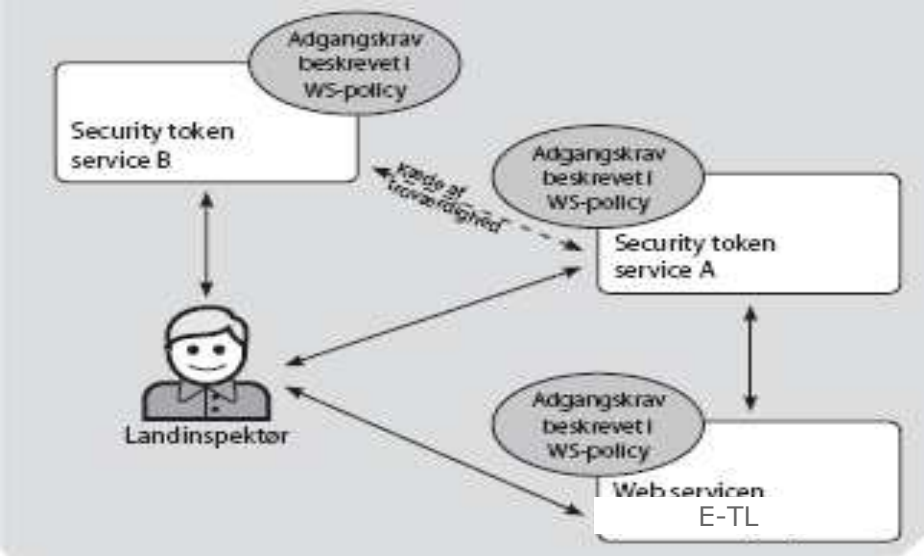
Mere information på www.e-tl.dk

Henrik Hvid Jensen, Devoteam Consulting
Henrik.hvid@devoteam.dk, 22 99 87 55
Blogs, nyhedsbrev og konferencetilbud på www.soanetwork.dk

DEVOTEAM CONSULTING CONNECTING BUSINESS & TECHNOLOGY

Den rigtige webservice-løsning –afkoblet

- Nuværende autentificerings- og autorisationsløsninger fokuserer primært på menneske til maskine-interaktion.
  - Med Web Services vil maskine til maskine-interaktionen vokse
  - kræver mekanismer til at etablere tillid mellem Web Services.
- Hver virksomhed udnævner Trust-webservice
- Når e-TL modtager en anmeldelse med brug af anmelderordningen
  - Spørger Trust-webservice om den pågældende signatur gerne må dette
- Medfører
  - Ingen brugeroprettelse hos e-TL
  - Kontrollen sker hos virksomheden



Signering i e-TLs miljø

- Det er XML-dokumentet som man underskriver
- Men det er en tekst-repræsentation som underskriveren ser
- E-TL kan ikke stole på at en anmelder loyalt har vist XML-dokumentet
  - Objektivt erstatningsansvar
- Al underskrift skal foretages i e-TL's miljø
  - Anmelder kalder en webservice hos e-TL
  - E-TL viser en tekst-repræsentation af XML-dokumentet
  - Brugeren underskriver
  - E-TL bekræfter at det er i dets miljø underskriften er foretaget
  - Det underskrevne dokument returneres til anmelder

Identifikation af systemer

- Systemer identificeres ved digital signatur
  - Godkendte systemers signatur er påført i SOAP-header
  - WS-Security standarden anvendes
- Al information signeres med Tinglysningsrettens digitale signatur
  - XML Signatur
  - Dokumentet kan sendes rundt mellem uafhængige interessenter
    - Alle kan kontrollere signaturen
    - Man kan tilføje egen information
- Ingen kryptering nødvendig når e-TL sender information ud
  - Information er offentlig

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="..."
xmlns:wsse="..." xmlns:wsu="..." xmlns:ds="...">
  <soap:Header>
    <wsse:Security>
      ...
      <ds:Signature>
      </ds:Signature>
    </wsse:Security>
  </soap:Header>
  <soap:Body wsu:Id="soapbody">
    <etl:Anmeldelse>

      <etl:AnmeldelseDokument id=”dokument”>
                ...
      </etl:AnmeldelseDokument>

      <etl:AttachmentBinaryData id=”bilag1” … />
      <etl:AttachmentBinaryData id=”bilag2”… />
                ...
      <etl:Underskrifter>
        <ds:Signature … />
        <ds:Signature … />
                ...
      </etl:Underskrifter>
    </etl:Anmeldelse>
  </soap:Body>
</soap:Envelope>
```

Andre beslutninger

- Ugyldig signatur ved modtagelsen
  - Ingen afvisning
  - Udtages til manuel behandling
- Samme i tilfælde af udenlandsk signatur
  - EU-regler betyder, at der ikke er lovhjemmel til at kræve udelukkende OCES
- Medarbejdercertifikat skal være med CPR

Kommunikation fra e-TL

- På portalen
  - Ingen oprettelse af brugere
  - Digital certifikat bruges til identifikation
    - Giver adgang til egne tinglysninger uden afgift
  - Medarbejdercertifikat giver adgang til virksomheders egne tinglysninger
    - Kan påføre virksomheden udgifter ved forespørgselsafgift
    - Uberettiget brug er et problem mellem virksomheden og den ansatte

Elementvis kryptering og signering

- Når en SOAP-besked skal transporteres over multiple SOAP-stationer mellem afsenderen og slutpunktet, kan det ikke forventes, at systemerne har andet til fælles end muligheden for at parse og dirigere en SOAP-besked. Det må derfor forventes, at et sådant scenarium involverer mere end én form af sikkerhedsindhold
- Alt sikkerhedsindholdet skal indgå i det samme SOAP-dokument, men skal være rettet til forskellige parter.
- Web Services kan opsamle information fra mange forskellige kilder, hvilket giver mere komplekse sikkerhedsudfordringer.
  - For eksempel når dokumenter er flyttet mellem forskellige stadier af elektronisk godkendelse, skal dokumenter opsamle digitale signaturer, men det oprindelige indhold må ikke blive ændret.
  - XML understøtter dette, ved at man kan opdele dokumentet i individuelle elementer.
  - Der kræves derfor en digital signaturløsning til understøttelse af dette.

Andet vedr. sikkerhed

- Vi opretter ikke brugere
  - Alle har lov til at se alt (mod betaling)
  - Alle kan anmelde en tinglysning (mod betaling)

- Vi overlader det til partnerne at sikre at medarbejderne overholder deres interne regler
  - Vi har godkendt alle system-system virksomheders servercertifikat
    - Hvem de tillader at bruge deres services er deres problem
  - Alle medarbejdere med et certifikat kan se virksomhedens tinglysninger!
    - Men det kan de jo alligevel
  - De kan også påføre udgifter ved køb af tinglysningsattester!
    - Virksomhedens interne procedure må kontrollere regninger fra e-TL
  - Hvor speciel tilladelse kræves (Anmelderordning og enkelte offentlige myndigheder)
    - Billet sendes med anmeldelsen (SAML-Token)
      - Virksomhedens ”portvagt” udsteder
      - E-TL kontrollere billetten

- Vi signerer al information der udsendes fra e-TL

- Vi krypterer ikke tinglyst information

- Krav om at notarfunktionen kan bruges som generel offentlig notarfunktion
  - Tidsstempling og opbevaring af kopi af dokumentet

Den fremtidige elektroniske tinglysningsmodel