Nye digitale sikkerhedsmodeller

- et diskussionsoplæg

IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

Udgivet af:
IT- & Telestyrelsen

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon: 3545 0000
Fax: 3545 0010

Publikationen udleveres gratis

Publikationen kan hentes
på IT- & Telestyrelsens
Hjemmeside: http://www.itst.dk

ISBN (internet): 978-87-92572-38-7

>

Nye digitale sikkerhedsmodeller

- et oplæg til diskussion

IT- & Telestyrelsen
januar 2011

Indhold >

1. Indledning

>

Med den omfattende digitalisering af den offentlige såvel som den private sektor vokser udfordringen med at tilvejebringe sikkerhed og privatlivsbeskyttelse i it-løsninger. Den traditionelle sikkerhedsopfattelse, hvor det gælder om at bygge så høje mure som muligt omkring sine systemer, er ikke længere tidssvarende. Der er behov for at tænke sikkerhed og privatlivsbeskyttelse ind fra starten af løsningsdesignet (at forebygge) frem for at betragte sikkerhed som noget, der tilføjes (at helbrede) efter selve forretningsløsningen er udviklet.

Den traditionelle sikkerhedsopfattelse udfordres bl.a. af cloud computing, hvor data ikke befinder sig på organisationens egen lokation eller i maskinstuen hos en klassisk driftsleverandør, og hvor fysisk kontrol over data ikke længere er nok til at sikre mod misbrug. Offentlige myndigheder kan ved brug af cloud computing opnå markante fordele i form af fleksibilitet og besparelser på it-driften. Men inden disse fordele kan opnås, er der behov for at adressere en række spørgsmål omkring behandling af følsomme data i cloudbaserede løsninger.

Eksempelvis er det på flere områder uklart, hvorledes eksisterende love og regler om persondatabeskyttelse skal fortolkes og anvendes i regi af cloud løsninger, idet der dels ikke findes præcedens på området, og dels fordi lovene er formuleret, før cloud computing fandtes og derfor ikke tager højde for de specielle forhold, der gør sig gældende her.

Tanken om at vi altid kan lokalisere data til et bestemt serverrum i kælderen udfordres, når data flyttes rundt i store servercentraler i hele verden, samt når data og applikationer deles med mange andre virksomheder ved brug af virtualisering (såkaldt *multi tenancy*). Der er behov for sikkerhedsmodeller, der i bedre grad end med de traditionelle modeller kan sikre, at data ikke bliver misbrugt. Der er således nødvendigt at supplere og videreudvikle de eksisterende sikkerhedsmodeller med nye, der i højere grad kan imødekomme de udfordringer vi står overfor i dag – både i forhold de løsningstyper vi kender i dag - men også for at åbne for nye typer af løsninger.

Dette diskussionspapir giver et første bud på, hvordan vi kan skabe en sådan videreudvikling.

Målgruppe
Papiret henvender sig til alle, der er interesseret i digitalt sikkerhedsdesign, men er særligt rettet mod beslutningstagere og it-ansvarlige i det private erhvervsliv og i offentlige myndigheder.

Om diskussionspapiret
Diskussionspapiret er inspireret af to workshops som IT- og Telestyrelsen afholdte i efteråret 2010 med en række interesserede parter. Workshops blev faciliteret af virksomheden Priway, som præsenterede en række visioner og koncepter (herunder Security By Design) samt formulerede de cases, som deltagerne skulle arbejde med. Se evt. [PRIW].

>

På de to workshops blev det drøftet, hvordan der kan udformes digitale sikkerhedsmodeller, der modsvarer tidens behov. Diskussionerne bragte en række spændende tanker på bordet og danner udgangspunktet for denne publikation.

Papiret lægger ud med at skitsere baggrunden for, at der er behov for nye sikkerhedsmodeller. Derefter bliver et bud på en ny sikkerhedsmodel beskrevet i de følgende afsnit. Beskrivelsen rundes af med en skitsering af perspektiver og en diskussion af udfordringer. Sidst i papiret bliver den centrale terminologi defineret.

2. Baggrund – det sociale internet

>

Gennem de seneste ti år har internettet udviklet sig fra at være en informationsbeholder til at være en interaktiv platform, der bliver meget mere værdifuld, når brugerne deler, skaber og kommunikerer med hinanden. Det er i mange sammenhænge brugernes interaktion, der skaber værdien på nettet. Wikipedia, YouTube og Facebook er eksempler på sociale internettjenester, som ville være værdiløse, hvis ikke brugerne skrev artikler, lagde videoer op, debatterede synspunkter eller skrev personlige anekdoter.

Udvikling fra et statisk internet mod et mere dynamisk net af sociale tjenester kaldes web 2.0. Denne betegnelse er et udtryk for, at internettet er blevet en katalysator for en dele- og deltagelseskultur, som på nogen områder har overhalet den virkelighed, der findes i traditionelle digitale service- og sikkerhedsløsninger.

Fremkomsten af det sociale internet har betydet, at der nu er skærpede forventninger til digitale services generelt. Hvilke krav stiller eksempelvis de "digitale indfødte" til offentlige digitale tjenester, når de er vant til at begå sig på Facebook, Youtube, Twitter og Flickr?

De digitale indfødte

En digital indfødt (eller *digital native*, som det kaldes på engelsk) er en person, der er født efter at digitale teknologier er blevet udbredt og som derfor har en høj grad af fortrolighed med digitale apparater og tjenester. De digitale indfødte er vokset op med mobiltelefoner, computere og internettet, men for dem er teknologien bare noget, der skal virke. Teknologien er for dem mest interessant som et socialt værktøj.

Det brugergenerede og sociale internet er sammen med de digitale indfødte ved at omforme den måde, som mennesker kommunikerer med hinanden på. Samtidig sætter det helt nye forventninger til de digitale løsninger, vi møder i form af brugervenlighed, enkelhed og interaktion mellem flere systemer. Jo mere interaktion og samarbejde på tværs af systemer, jo flere udfordringer kommer der i traditionelle sikkerhedsmodeller baseret på forestillingen om, at sikkerhed opnås ved at indhegne systemer bag "høje mure". Derfor må vi udvikle sikkerhedsmodeller, der kan tage højde for eksempelvis interaktionen mellem flere systemer.

Med udgangspunkt i de digitale indfødte, kan man stille sig det spørgsmål, om eksempelvis den første generation af ESDH-systemer i den offentlige forvaltning lever op til den brug af digitale tjenester, som en person født efter 1990 ellers praktiserer?

En anden konsekvens af, at internettet er blevet socialt er, at der kommer flere og flere data om brugerne. Det spænder lige fra statusopdateringer på Facebook, over Googlesøgninger, til hvor og hvornår vi sidst loggede ind på borger.dk. Vi sætter elektroniske fingeraftryk overalt, hvor vi færdes på nettet, og ofte er vi slet ikke klar over, at det sker. Endelig er vi endnu mindre klar over, hvem der bruger oplysningerne og til hvad. Der ligger derfor en meget stor udfordring i at sikre brugernes privatlivsbeskyttelse i den digitale verden.

Virksomhederne står overfor en række udfordringer, når de vil udnytte Web 2.0 og cloud computing. De nuværende sikkerhedsmodeller er ikke altid gode nok til at håndtere disse udfordringer. Faktum er, at en virksomhed ikke længere alene kan beskytte sine systemer ved at bygge høje mure. Perimeteren kan således blive åbnet, fordi medarbejderne bevæger sig ud af virksomhedens interne systemer. Eksempelvis er det ikke alle virksomheder, der har en sikkerhedspolitik for smartphones. Når medarbejderne begynder at tjekke og sende mails via deres smartphones skaber det et hul i virksomhedens perimeter. Det samme er tilfældet, når medarbejderne begynder at udveksle dokumenter i Google Docs frem for at benytte virksomhedens egne systemer, eller hvis medarbejderne begynder at bruge diverse sociale tjenester i kombination med virksomhedens egne systemer.

Derfor kan er det ikke længere nok kun at basere sig på en stærk perimeter for at skabe et tilpas sikkerhedsniveau. For at imødekomme udviklingen er der behov for at supplere de eksisterende sikkerhedsmodeller med nye.

Dette diskussionspapir vil ikke give sig i kast med at løse alle de problemstillinger, som præsenteres i ovenstående. De nye sikkerhedsmodeller, som skitseres i de næste kapitler, kommer kun med nogle af løsningerne.

Eksempelvis er privatliv i forhold til kommunikationskanaler ikke behandlet, så det kan være muligt at profilere brugere på baggrund af deres IP-adresser, hvis man ikke anvender mekanismer, der modvirker dette. Formålet med papiret er således ikke at komme med komplette, produktionsklare løsninger – men i stedet at vise læserne, at tingene kan gøres på nye måder via nogle illustrative eksempler. Ved implementering i fuld skala er der naturligvis en række yderligere aspekter, som skal håndteres – eksempelvis brugervenlighed, revokering, genudstedelse etc.

Hvordan sikres kontrol over data?
Der er to overordnede tilgange til at sikre data, som befinder sig i ”cloud” (udenfor den enkelte virksomhed eller myndigheds direkte fysiske kontrol):

- **Assurance-based sikkerhed** hvor man via kontrakten med cloudleverandøren og ved uafhængig revision kan sikre sig, at leverandøren overholder passende organisatoriske og tekniske sikkerhedsforanstaltninger.
- **Forebyggende-sikkerhed** i form af ”Security by Design” hvor sikkerheden bygges ind i systemet fra start af, og hvor man i langt mindre grad er afhængig af driftsleverandørens egen sikkerhed (herunder cloud leverandøren).

Dette diskussionspapir handler kun om forebyggende sikkerhed i form af ”Security by Design”. IT og Telestyrelsen arbejder også på at fremme Assurance-based sikkerhed, men det vil ikke blive behandlet yderligere i dette papir.

3. Målsætninger for en ny sikkerhedstænkning

>

Herunder beskrives de principper og egenskaber, der har været anvendt som krav i forbindelse med et nyt sikkerhedsparadigme. Disse krav stilles ud fra ønsket om en balanceret sikkerhed med stærk privatlivsbeskyttelse samt muligheden for at rykke data ud i skyen. Nedenstående punkter udgør med andre ord målsætningerne for den sikkerhedsmodel, der beskrives i de følgende afsnit:

1. Der skal være sikkerhed for alle parter – løsningsejere såvel som brugere.
2. Brugerne skal have mulighed for fuld kontrol over, hvilke data der afgives til hvilke løsninger, og kontrol over om deres data i forskellige løsninger kan kobles sammen.
3. Informationer, der gemmes om brugere, må ikke kunne henføres direkte til deres fysiske identitet, med mindre dette er strengt nødvendigt og forhandlet. Der bør således anvendes virtuelle identiteter / pseudonymer frem for identificerende nøgler som eksempelvis CPR numre.
4. Brugernes data skal ikke kunne kobles sammen, selv hvis flere eksterne parter arbejder sammen om at udlede flere informationer, end brugeren eksplicit har godkendt.
5. Serviceudbyderne skal have sikkerhed for, at de kun modtager ægte brugerinformation, og at informationen vedrører den bruger, som sender dem.
6. I de situationer, hvor der er behov for det, skal man kunne etablere mekanismer, der sikrer brugernes ansvarlighed. Et eksempel på dette er såkaldte ansvarlighedsbeviser, som sikrer, at det bliver muligt at identificere en bruger, der ikke følger spillereglerne ved f.eks. at begå kriminalitet. Ansvarlighedsmekanismerne må ikke lede til kompromittering af sikkerheden for alle de transaktioner, hvor der ikke er foregået noget ureglementeret.
7. En sikkerhedsmodel bør så vidt muligt indrettes, så konsekvenserne af sikkerhedsbrud i ét system eller for én bruger er begrænsede til den lokale kontekst – og ikke skalerer til alle systemer eller alle brugere. Dette er særligt vigtigt i forbindelse med cloud løsninger.
8. Generelt skal transaktioner isoleres og det skal sikres, at kontrollerne ikke bare ligger uden for cloud, men ”klient-side” hos brugeren.
9. Man bør designe efter at mange forskellige interessenter kan have forskellig merviden om en transaktion (fine grained) og bruge forskellige teknologier (semantisk interoperabilitet) samtidig med at kontrollen bør følge brugeren.

4. Privacy-by-Design

>

Ovennævnte målsætninger og principper for sikkerhedsmodellen er i overensstemmelse med konceptet "Privacy-by-Design" (PbD)[1], som bl.a. er beskrevet af den Canadiske privacy ombudsmand Ann Cavoukian i 1990'erne.

Grundlæggende går dette ud på, at forretningsprocesser, it-systemer og infrastruktur fra starten skal designes, så de *forebygger* brud på borgenes privatliv – altså en proaktiv frem for reaktiv tilgang. Det opleves ofte, at privacy indføres som en "lappeløsning" af procedurer og kontroller, der forsøges påklistret et allerede etableret system, hvor det ikke fra starten har været en designparameter.

Privacy skal opnås uden at brugerne gør noget eksplicit for det. Det skal ske ved, at principperne indbygges i systemerne fra starten – altså før de første informationer indsamles.

Privacy-by-Design er bruger-centrisk i den forstand, at brugerne er i kontrol over deres data.

Privacy ses ikke som en modsætning til sikkerhed (for løsningsejeren). Tværtimod er det en væsentlig pointe, at de to egenskaber kan opnås på samme tid. Sagt på en anden måde skal der være sikkerhed for alle parter – dvs. flere parters hensyn skal balanceres mod hinanden.

I de følgende kapitler præsenteres en sikkerhedsmodel baseret på *kontekstafhængige akkreditiver, transaktionsisolering* og *formålsspecifikke nøgler*, der teknologisk kan understøtte Privacy-by-Design i designet af it-systemer. Arkitekturen gør det eksempelvis muligt:

- At kun de nødvendige informationer om brugerne videregives.
- At videregivelsen sker under brugerens kontrol.
- At brugerne kan agere med en virtuel identitet overfor applikationer - herunder ikke blive identificeret med mindre det er strengt nødvendigt.

Disse muligheder tvinger systemdesigneren til bevidst at overveje, hvilken information der frigives hvor, samt i hvor høj grad den skal kobles til brugerens fysiske identitet – i modsætning til traditionelle sikkerhedsmodeller, hvor disse muligheder ikke er til rådighed, og hvor det derfor kan være vanskeligere at designe systemer, der lever op til Privacy-by-Design principperne.

[1] http://www.privacybydesign.ca/

5. Security By Design

>

En af udfordringerne med Privacy-by-Design har været fokuseringen på risiko set fra en interessents synsvinkel, typisk brugerens.

Derfor går dette diskussionspapir skridtet videre i form af et koncept, der kaldes Security-By-Design[2]. Konceptet viser, hvordan man kan tage ansvar for hele transaktionen med flere interessenter involveret. Målet er ikke anonymitet, som kunne optimere privacy - eller overvågning, som ville gøre det stik modsatte.

Målet er at blive operationelt i stand til at designe med sikkerhedsbalancer som passer til den konkrete forretningstransaktion, samtidig med at man designer så de digitale processer kan tilpasse sig de enkelte brugere behov og samtidig leve op til de hastigt stigende sikkerhedskrav med cloud, Internet of Things og den generelt tiltagende integration af it-systemer – alt sammen forhold som kræver nytænkning af sikkerhedsforståelsen.

Det centrale i en ny sikkerhedsforståelse er at gå bort fra identifikationsbaseret sikkerhed ved at eliminere identifikationen og gå direkte til de sikkerhedsaspekter, man ønsker valideret, uden at skabe sikkerhedsproblemer som følger af antagelsen om identifikation. Senere i diskussionspapiret vil vi vise, hvordan man logisk kan nedbryde identitet i forskellige logiske sikkerhedsaspekter, som hensigtsmæssigt afdækkes bedre uden at skabe sårbarhederne. F.eks. forudsætter sikkerhedsmålsætningen ”Ansvarlighed” ikke at brugeren er identificeret overfor modparten. I stedet kan brugeren agere med en virtuel identitet og samtidig demonstrere et bevis på, at der er etableret en måde betinget under specifikke forudsætninger at identificere brugeren.

En anden mekanisme kunne være når f.eks. en patient afgiver data til et cloud-system, hvor lægen – men ikke cloudsystemet – kan henføre data til en bestemt patient. I dette tilfælde er tillidsforholdet mellem patient og læge det samme, men begge parter er mindre sårbare overfor cloud-systemet. Tilsvarende kan cloud-services etableres uden de sårbarheder, som opsamling og brug af personhenførbare data medfører.

Security-by-Design er således en videreudvikling og en operationalisering af Privacy-by-Design, som med nyere kryptografiske mekanismer og bevidst systemdesign skaber nytteværdi samtidig med at sikkerhedsbrud af mange forskellige slags forbebygges.

[2] Konceptet for Security-By-Design som det beskrives her er primært udviklet af Stephan J. Engberg.

6. Beskrivelse af sikkerhedsmodellen

>

I det følgende introduceres de grundlæggende elementer i en ny sikkerhedsmodel, som gør det muligt at realisere de ovennævnte mål. Først beskrives udfordringer med traditionelle akkreditiver i forhold til brugernes sikkerhed og privacy. Herefter beskrives principperne for kontekstafhængige akkreditiver og transaktionsisolering som en løsning på disse problemer, der samtidig opnår en høj sikkerhed for alle parter.

Ved første øjekast kan de beskrevne egenskaber forekomme uopnåelige – det kan eksempelvis virke paradoksalt, at sikkerhed for alle parter kan opnås på samme tid. Ikke desto mindre er de beskrevne egenskaber realisérbare ved brug af kendt teknologi baseret på avanceret kryptografi – og denne teknologi er tilgængelig på markedet.

Denne fremstilling går ikke i detaljer med de bagvedliggende kryptografiske og matematiske principper. Beskrivelsen er i stedet holdt på et overordnet, anvendelsesorienteret og teknologineutralt niveau med henblik på formidling til et bredere publikum.

6.1 Traditionel (fødereret) sikkerhedsmodel

En sikkerhedsmodel, der ofte anvendes når brugerne tilgår flere forskellige tjenester, er den *fødererede* model. I denne skal en bruger præsentere digitale akkreditiver for at tilgå en given tjeneste, mens selve udstedelsen af akkreditiver sker uafhængigt af tjenesten. Når en bruger eksempelvis tilgår borger.dk, skal han logge ind via NemID[3], mens selve udstedelsen af NemID sker helt uafhængigt af borger.dk hos DanID.

Ved et (digitalt) akkreditiv forstås en samling data relateret til en bruger, der udstedes af en ekstern part, og som en bruger kan præsentere (evt. dele af) med henblik på at få adgang til et it-system. I den fysiske verden svarer akkreditiver til en form for ihændehaverbevis, der gør indehaveren i stand til at disponere på en bestemt måde – eksempelvis i form af en fuldmagt. Inden for sikkerhedsterminologien kaldes disse ofte for ”tokens”, ”assertions” – eller slet og ret: ”billetter”.

Modellen opererer med følgende tre typer af aktører:

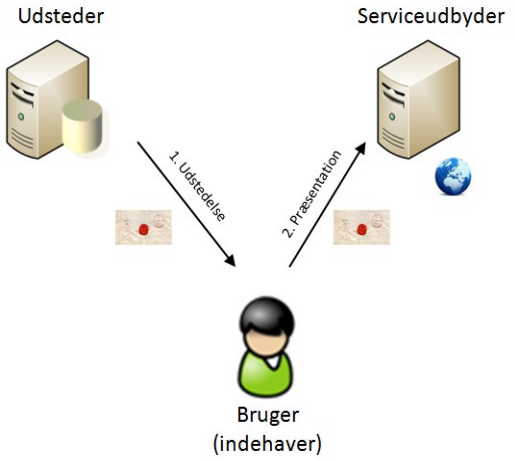
En udsteder af akkreditiver – eksempelvis en myndighed eller en applikation, der har data lagret om en bruger – herunder såkaldte attributtjenester. Dette er en tredjepart, som andre stoler på i forhold til at attestere visse attributter om brugere – eksempelvis kan CPR registret attestere en brugers alder eller køn, Sundhedsstyrelsen kan attestere at en bruger er autoriseret læge, og et seminarium kan attestere, at en bruger har bestået pædagogeksamen. I traditionelle modeller udgøres denne rolle af certifikatudstedere (PKI), Identity Providere (SAML) eller en Security Token Services (WS-*) som attesterer brugerens identitet, men i den nye sikkerhedsmodel vil rollen i højere grad blive spillet af applikationer eller såkaldte attributtjenester, der har data registreret om brugeren, men hvor akkreditivet ikke identificerer brugeren.

[3] Borgeren anvender sit NemID til at logge på Single Sign-On løsningen NemLog-in, der så giver adgang til borger.dk

>

- *En serviceudbyder* som udbyder en service / applikation til brugerne, og giver adgang til funktioner og data på baggrund af præsenterede akkreditiver. Dette kan eksempelvis være en digital selvbetjeningsløsning hos en offentlig myndighed så som borger.dk. Denne rolle betegnes ofte for ”relying party” eller ”verifier” på engelsk, idet der indgår validering af brugerens præsenterede akkreditiver.
- *Brugeren* som modtager akkreditiver fra udstederen og tilgår services hos serviceudbydere ved at præsentere akkreditiver. Denne rolle kaldes også for indehaver – og på engelske ”prover” på grund af rollen med at bevise akkreditiver.

Modellen er illustreret på nedenstående figur:



Figur 1: Grundprincip i modellen

6.2 Traditionelle akkreditiver

Ovenstående principper for en fødereret model med brugere, udstedere af akkreditiver og tjenesteudbydere er meget udbredt. Som eksempler på traditionelle akkreditiver kan nævnes:

- Ved log-in med den digitale signatur agerer DanID som udsteder af et OCES certifikat, som er det akkreditiv, brugeren præsenterer for løsningen for at autentificere sig (sammen med bevis for kendskab til den tilhørende private nøgle). Et personcertifikat indeholder et såkaldt PID nummer (person ID nummer), der er direkte koblet til personens CPR nummer.
- Ved brug af den fællesoffentlige single sign-on løsning NemLog-in, udstedes en såkaldt SAML Assertion, som er det akkreditiv, brugeren præsenterer for løsningen for at autentificere sig. En SAML Assertion kan i OIOSAML profilen være (og er ofte) koblet til brugerens identitet via en ”CPR-nummer-attribut”, men kan også blot indeholde et persistent pseudonym.

Traditionelle X.509 certifikater og SAML assertions har en række stærke sikkerhedsmæssige egenskaber, men rummer også en række potentielle udfordringer for brugeren:

- Koblingen til brugerens fysiske identitet gør det umuligt for brugeren ikke at identificere sig overfor tjenesteudbydere.
- Certifikater indeholder entydige nøgler, der gør det muligt at sammenkoble brugerens færden på tværs af alle tjenester. Når et certifikat præsenteres, afsløres endvidere alle attributter – uanset om modtageren har behov for at kende dem eller ej.
- SAML Assertions (eller rettere protokollerne) har den svaghed, at selv når de kun indeholder pseudonymer og kun anvendes én gang (transiente pseudonymer), da har udstederen kendskab til koblingen mellem brugerens identitet og hans pseudonymer, og han kan yderligere følge med i, hvilke tjenester brugeren tilgår, samt hvornår han gør det. Desuden er udstederen (eller kriminelle som kan stjæle hans signaturnøgle) i stand til at udstede Assertions uden brugerens medvirken – og således impersonere brugeren overfor samtlige serviceudbydere.
- Sikkerhedsbrud kan påvirke mange interessenter på samme tid – især brud hos identitetsudbydere kan skalere voldsomt.
- Når brugerne identificeres og data let kan sammenkobles uden brugerens medvirken, kan der opstå et pres for at anvende data på nye måder, som ikke oprindeligt var planlagt, og som brugerne ikke nødvendigvis er indforståede med. På den måde kan der ske et skred i forhold til den oprindelige anvendelse.

Ovenstående udfordringer håndteres traditionelt ved at stille skrappe sikkerhedskrav til udvikling og drift af it-systemer indeholdende personfølsomme data, hvilket imødegår misbrug af tredjeparter (f.eks. hackerangreb). Disse høje krav kan påføre betydelige meromkostninger til udvikling, drift og forvaltning af systemerne samt hindre anvendelse af cloud computing. Endvidere er systemerne underlagt persondataloven, der ud over rent sikkerhedsmæssige krav også giver en række begrænsninger på tilladte anvendelser af data.

6.3 Fra identifikation til identitet

Som beskrevet i indledningen er det hensigtsmæssigt at gå fra en simpel en-dimensionel forståelse af identitet (alt pakkes ind i en og samme digitale nøgle eller akkreditiv) til en fleksibel og nuanceret identitetsmodel, hvor de forskellige sikkerhedshensyn varetages med specifikke mekanismer.

I den traditionelle en-dimensionelle identitets- og sikkerhedsforståelse tenderer man til at reducere identitet til identifikation (hvor godt er brugeren identificeret overfor systemet?). Baggrunden er, at man dermed antager at kunne slå identiteten op i mange andre systemer med henblik på at fastslå autorisationer, hente data og genkende med en og samme mekanisme. Det kan argumenteres, at denne fremgangsmåde rummer to centrale udfordinger:

- Sikkerhedsmodellen fastlåses i en uholdbar model, der akkumulerer sårbarheder (f.eks. skalerbare angreb og databeskyttelsesproblemer)
- It-systemerne fastlåses og ”spagettihardkodes” på kryds og tværs, så de bliver stadigt mere ufleksible og dyrere at vedligeholde og opgradere.

>

Den traditionelle en-dimensionelle identitetsforståelse kan rumme faren for dyrere og dårligere løsninger, samtidig med at man på den anden side får dårligere sikkerhed. Det betyder endvidere, at den marginale værdi af investeringen i dem falder.

I den nye sikkerheds- og identitetsforståelse bryder man identitet ned i de logiske adskilte komponenter som hver især kan gøres:

- *Interoperable* (sammenlignes og udskiftes – f.eks. opgradere algoritimer).
- *Konkrete* (holdes semantisk op mod operationelt formulerede policies eller krav som derved bliver styrende som alternativ til plug-on security).
- *Begrænsede* (ikke-invasive og formålsspecifikke, så sikkerhed ikke bliver et valg mellem onder).

Centrale logiske komponenter for en identitet er:

- *Autentificering / genkendelse* – de mekanismer, som man bruger til at verificere, at en bruger er den samme som i en tidligere transaktion og som oftest anvender på forhånd aftalte mekanismer, som brugeren kontrollerer (ihændehaverbeviser, userid-password, nøgler etc.).
- *Ansvarlig / Betinget Identifikation* – de mekanismer, som man optionelt kan bruge til at holde modparten ansvarlig i tilfælde af, at modparten ikke lever op til aftaler eller lovgivning.
- Kommunikation – de kommunikationskanaler, krypteringnøgler, algoritmer etc. som brugeren ønsker at bruge for denne specifikke transaktion.
- Integritet – de sikkerhedsmekanismer, som man bruger til at verificere sandsynligheden for, at ingen 3. part har overtaget brugerens rolle.
- Akkreditiver, som kan deles op i 2 typer – positive hvis de er til gavn for brugeren (såsom en erhvervet akademisk grad eller statsborgerskab) eller negative hvis de er til skade for brugeren (som en udelukkelse eller en fængselsdom).

De positive akkreditiver er verficérbare, positive udsagn om brugeren, dvs. vil altid udgøre en 3. parts verificeret sandhed. Disse kan eksempelvis være:

- Identifikation (en krypteret besked til en læge indeholdende en Digitalt Signeret besked).
- Ihændehaverbeviser (billetter, penge, aktiver).
- Autorisationer (beviser for at man tilfører gruppen af personer, som må eller har ret til en given handling – f.eks. Læge, Administrator eller Prokura).

De negative akkreditiver er verificérbare negative udsagn om brugeren, dvs. vil også altid udgøre en 3. parts verificeret sandhed:

- Udelukkelse.
- Dømt/Straffet for.
- Dårlig Betaler.

Et problem med negative akkreditiver er i sagens natur, at brugeren kan have en interesse i at undgå at vise dem, hvorved de lettest bevises som et positivt akkreditiv

>

(jeg er *ikke* udelukket, jeg har *stadig* adgang, jeg er *ikke* dømt, jeg *har* kreditmuligheder/trækningsret osv.).

Arbejdet med at nedbryde, strukturere og standardisere identitetselementerne samt på den anden side at etablere standarder for at evaluere, sammenligne og opgradere sikkerhed er langt fra afsluttet – som alle markedsområder under udvikling er det er et "moving target", hvor man lokalt må fokusere på hvor værdien er størst.

6.4 Kontekstafhængige akkreditiver

Et centralt element i den nye sikkerhedsmodel er de såkaldte *kontekstafhængige akkreditiver (eng. anonymous credentials)*. Kontekstafhængige akkreditiver kan opfattes som en digital pendant til velkendte anonyme akkreditiver i den fysiske verden, som eksempelvis busbilletter, mønter, stemmesedler til folketingsvalg etc. Alle disse har sikkerhedsmekanismer indbygget, som modvirker svindel - men tillader samtidigt indehaveren ikke at blive identificeret i brugssituationen. Kontekstafhængige akkreditiver har en række ligheder med traditionelle sikkerhedsakkreditiver som eksempelvis X.509 certifikater, SAML Assertions eller Kerberos tickets:

Ligheder:

1. Indeholder en samling attributter med information om indehaveren (brugeren) af akkreditivet. Attributter kan eksempelvis beskrive indehaverens fødselsdato, medlemskab af en gruppe (så som "dansk statsborger", "autoriseret læge", "studerende på Københavns Universitet") osv.
2. Akkreditivet kan ikke forfalskes eller ændres, da det er beskyttet af udstederens digitale signatur som valideres af modtageren – og de er (ligesom sædvanlige akkreditiver baseret på kryptografi) resistente mod replay og phishing angreb grundet bindingen til en hemmelig nøgle, som kun brugeren er i besiddelse af.
3. De kan spærres (revokeres) og kan have en udløbsdato.
4. De kan kun anvendes sammen med en privat (hemmelig) nøgle, der alene kendes af indehaveren. Dette giver altså en stærk binding til indehaveren. Den hemmelige nøgle (eller dele heraf) kan beskyttes af tamper-resistente smart cards.

De kontekstafhængige akkreditiver adskiller sig dog fra traditionelle akkreditiver ved også at have følgende egenskaber:

1. De indeholder normaltingen informationer, der direkte kan udpege indehaverens identitet - eksempelvis indeholder de ikke CPR-numre etc[4]. I stedet vil et kontekstafhængigt akkreditiv blive benyttet sammen med en virtuel identitet (*pseudonym)*, som er dekoblet fra den fysiske person. En virtuel identitet er altså en digital stedfortræder for den fysiske person –

[4] I givet fald skal brugeren ikke afsløre disse attributter under præsentationen af akkreditivet (jævnfør *"selective disclosure"* under punkt 5 nedenfor), hvis han vil undgå at blive identificeret.

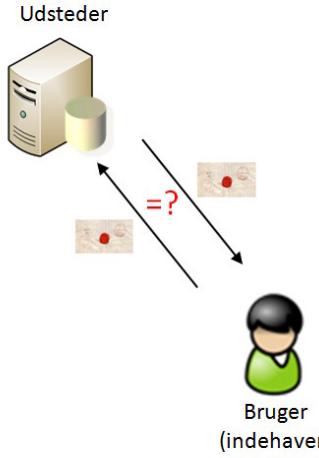
>

analogt til når forfattere i den fysiske verden udgiver tekster under et pseudonym frem for at bruge deres fysiske identitet. En væsentlig forskel er blot, at man i den digitale verden kan benytte mange forskellige virtuelle identiteter for at holde forskellige transaktioner adskilt.

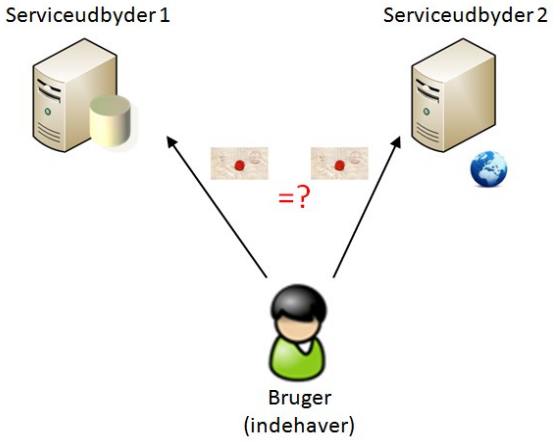
2. Et kontekstafhængigt akkreditiv, som præsenteres hos en serviceudbyder, kan ikke spores tilbage til udstedelsesprocessen. Selv udstederen af akkreditivet kan ikke bagefter se på det enkelte akkreditiv, hvem det er udstedt til, selvom indehaveren var kendt på udstedelsestidspunktet (se figur 2 nedenfor). Dette svarer eksempelvis til en stemmeseddel ved folketingsvalg: man kan ikke se på stemmesedlen, hvem der har brugt den, selvom personen var kendt på udstedelsestidspunktet (da stemmesedlen blev udleveret).
3. En indehaver kan benytte *forskellige* kontekstafhængige akkreditiver hos forskellige serviceudbydere, uden at det er muligt at spore, at der er tale om samme indehaver (se figur 3 nedenfor). Dette gør det f.eks. umuligt for to serviceudbydere at sammenkoble de informationer, de hver især har registreret om indehaveren, på basis af information fra forskellige kontekstafhængige akkreditiver.
4. Et kontekstafhængigt akkreditiv bliver teknisk set ikke sendt til serviceudbyderen men i stedet præsenteret via en protokol, hvor brugeren beviser, at det indeholder visse attributter med visse værdier.
5. Brugeren har i sin dialog med serviceudbyderen fuld kontrol over, hvilke attributter fra akkreditivet han vil afsløre (se figur 4 nedenfor). Han kan eksempelvis vælge at afsløre én attribut med sit køn, men holde en anden attribut med sin fødselsdato hemmelig. Dette kaldes ofte for ”*selective disclosure*”.
6. Man kan indbygge mekanismer, der sikrer, at kontekstafhængige akkreditiver kun kan anvendes et bestemt antal gange. Eksempelvis kan man lave elektroniske kontanter, hvor det sikres, at en digital pengeseddel kun kan anvendes én gang.
7. Det er muligt at signere data med den private nøgle hørende til et kontekstafhængigt akkreditiv, således at man kan opnå de samme egenskaber som med en traditionel digital signatur (herunder integritet og uafviselighed).
8. Det er muligt for en bruger at sende krypterede data til en serviceudbyder og dernæst bevise egenskaber om dem uden at afsløre indholdet (såkaldt *verifiable encryption*). Brugeren kan eksempelvis sende sin identitet krypteret under en tredjeparts nøgle, som serviceudbyderen ikke er i besiddelse af, men samtidig bevise over for serviceudbyderen, at det er den korrekte identitet, som er sendt. På den måde kan serviceudbyderen sikre sig, at han ved at gå til tredjeparten kan få dekrypteret brugerens sande identitet (eng. *identity escrow*) – eksempelvis hvis der er svindel involveret i transaktionen. Bemærk at dette er et meget forsimplet eksempel på et ansvarlighedsbevis, som tjener til at illustrere mekanismen.

Der er altså væsentlige forskelle mellem de traditionelle og de kontekstafhængige akkreditiver. Man kan sige, at X.509 certifikater (traditionelle akkreditiver) giver sporbarhed per design samt obligatorisk visning af alle attributter, mens kontekstafhængige akkreditiver giver *anti*-sporbarhed per design og brugerkontrol over hvilke attributter, der præsenteres.

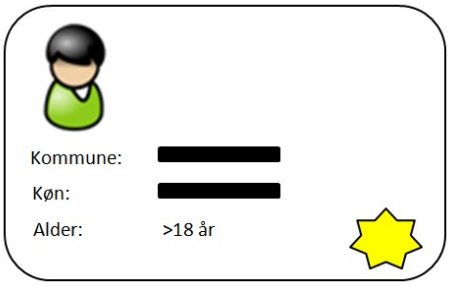
>



Figur 2: Akkreditiv som ikke er sporbart / genkendeligt selv for udstederen



Figur 3: Bruger kan ikke sammenkædes på tværs af serviceudbydere



Figur 4: Selektiv afsløring af attributter fra akkreditiv

Udstederen vil normalt autentificere brugeren før udstedelse af et kontekstafhængigt akkreditiv, men der behøver ikke være tale om en identificering af brugeren (f.eks. fastlæggelse af CPR nummer) – og i mange situationer er dette ikke ønskeligt. Eksempelvis kan et kontekstafhængigt akkreditiv udstedes på baggrund af et andet kontekstafhængigt akkreditiv fra en anden udsteder eller til et pseudonym. Eksempelvis kan akkreditivet sige, at personen med pseudonym ”1234abcd” har en kandidateksamen i medicin fra Københavns Universitet, og indehaveren ved brug af

>

akkreditivet overfor modtageren skal bevise kendskab til en given hemmelig nøgle (eng. *proof key / holder-of-key*).

Eksempler på kendte realiseringer af kontekstafhængige akkreditiver er de såkaldte ”U-Prove Tokens” fra Microsoft [UPCS] og ”Identity Mixer Anonymous Credentials” fra IBM [IDMX2]. Bemærk at disse opererer med en Identity-Provider centrisk model, og at der i dette papir opereres med en bredere tilgang, hvor dette ikke er altid er tilfældet.

Bemærk, at når kontekstafhængige akkreditiver anvendes, da vil udsteder og serviceudbyder ikke sende brugerdata direkte *mellem* hinanden – det sker i stedet via brugeren og er underlagt dennes kontrol. Dette indebærer i praksis, at brugeren skal være i besiddelse af en agent / klient[5], der faciliterer anvendelsen af de kontekstafhængige akkreditiver.

[5] Klienten kan være en kombination af hardware og software – eller evt. ren softwarebaseret. Et eksempel på en klient er Microsoft Windows CardSpace eller et borgerkort.

>

Hvor sikre er kontekstafhængige akkreditiver?

Teorien for kontekstafhængige akkreditiver bygger på avancerede kryptografiske teknikker, hvor det (med passende forudsætninger) er muligt at føre matematiske beviser for en række af de påståede egenskaber herunder at kontekstafhængige akkreditiver ikke kan spores til udstedelsen, sammenkædes på tværs af anvendelser eller lækker mere information end brugeren aktivt godkender. Der er dermed en meget høj grad af sikkerhed for, at de ovenfor beskrevne egenskaber rent faktisk holder vand i modellen.

Eksempler på de underliggende kryptografiske teknikker er såkaldte "blinded signatures", "secret sharing" og "zero knowledge" protokoller. For detaljer om den matematiske teori henvises til [BRA], [UPCS] og [IDMX2] (se referencer i afsnit 12).

Som altid skal der indgås nogle tekniske kompromis'er, når en matematisk model skal implementeres i den virkelige verden – og skal kunne benyttes af almindelige borgere. Disse kompromis'er kan give anledning til svagheder, som ikke findes i den matematiske model. Som eksempel kan nævnes sporbarheden af et anonymt akkreditiv: hvis en udsteder vælger at inkludere en udløbsdato som en attribut i akkreditivet, der har en meget finkornet værdi (fx udstedelsestidspunktet med en nøjagtighed i millisekunder plus to år), da kan det i praksis være muligt at korrelere akkreditivet til udstedelsestidspunktet og indsnævre de mulige brugeridentiteter. Et andet eksempel er, at når udstedelsen af et anonymt akkreditiv tidsmæssigt er koblet til brugen i en applikation (just-in-time udstedelse) - da vil udstederen og tjenesteudbyderen kunne arbejde sammen om at identificere brugerne ud fra den tidsmæssige kobling. Begge disse eksempler er karakteriserede ved, at den praktiske anvendelse af kontekstafhængige akkreditiver sker på en uhensigtsmæssig måde, der lækker information via såkaldte sidekanaler.

Sådanne problemer er dog alle *praktiske* implementeringsproblemer, som der er praktiske løsninger på, og hvor man udbedrer fejl eller uhensigtsmæssigheder ved at forbedre implementeringerne. Dette er i modsætning til de modeller, der ligger til grund for traditionelle akkreditiver som eksempelvis X.509 certifikater. Her vil alle implementeringer lede til de tidligere nævnte problemer med kobling til brugerens fysiske identitet, sporbarhed via entydige nøgler og mulighed for at en tredjepart kan impersonere brugeren.

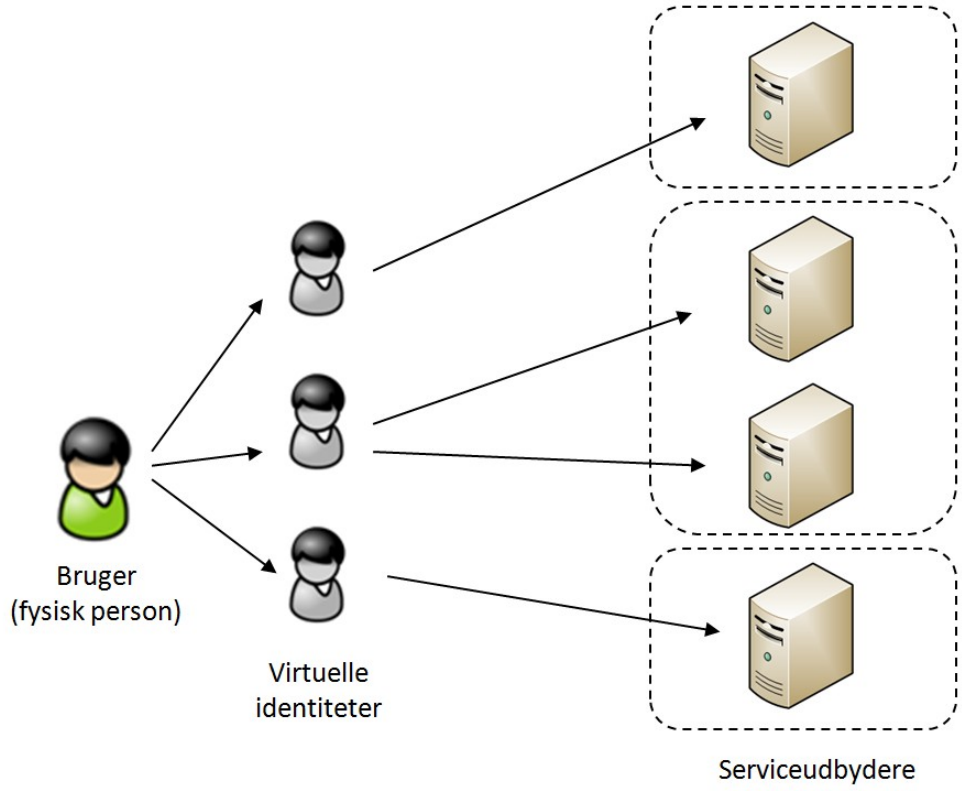
6.5 Virtuelle identiteter og transaktionsisolering

Med introduktion af den nye sikkerhedsmodel skiftes fra et identifikationsbaseret paradigme til et valideringsorienteret paradigme. Dette betyder, at i stedet for at alle applikationer identificerer brugerne og knytter lokale data til identiteten (f.eks. CPR nummer), da skal man i stedet knytte data til virtuelle identiteter (pseudonymer), som kan valideres (dvs. brugeren kan bevise, at han repræsenterer et pseudonym via en hemmelig nøgle).

Sammenknytningen mellem virtuelle identiteter og data kan ske med forskellig detaljeringsgrad:

- Brugeren vælger en ny virtuel identitet for hver transaktion. Dette giver total isolering af brugerens transaktioner, og en tjenesteudbyder kan ikke se forskel på, om to transaktioner hører til samme eller forskellige brugere.
- Brugeren vælger samme virtuelle identitet til flere transaktioner hos samme tjenesteudbyder. På den måde kan tjenesteudbyderen opbygge historik – eksempelvis kan en on-line filmudlejer opbygge viden om brugerens præferencer fra gang til gang (uden at han dog behøver at kende brugerens rigtige identitet).

På den måde kan brugeren opbygge helt isolerede "ø'er" af profiloplysninger knyttet til forskellige virtuelle identiteter hos forskellige serviceudbydere. Der kan dog som før nævnt (hvis anvendelsen nødvendiggør det) indbygges ansvarliggørende mekanismer, hvor den fysiske person bag en virtuel identitet kan blive frigivet under på forhånd definerede omstændigheder.



Figur 5: Brug af virtuelle identiteter til adskillelse af brugerdata hos serviceudbydere

Hvis en bruger allerede har en eksisterende profil hos en serviceudbyder, kan han endvidere vælge at koble en virtuel identitet til denne ved at autentificere sig på traditionel vis (eksempelvis afgive det brugernavn og password som er koblet til hans profil) og i samme session præsentere det nye akkreditiv. Dermed kan tjenesteudbydere foretage en sammenkobling af profilen med den virtuelle identitet fra akkreditivet, hvorefter brugeren ikke længere behøver at anvende det traditionelle akkreditiv. Denne teknik kaldes ofte for "account linking" og kan være interessant i en overgangsfase.

>

6.6 Data i skyen

Det fremføres ofte, at traditionelle sikkerhedsmodeller baseret på paradigmet om perimetersikkerhed ikke er tilstrækkelige til, at personoplysninger (og personhenførbare data) kan flyttes til skyen grundet de øgede risici forbundet hermed.

Ved at designe applikationer på en ny måde herunder anvende de ovenfor beskrevne mekanismer med kontekstafhængige akkreditiver, brugerdata knyttet til virtuelle identiteter og transaktionsisolering kan man i høj grad nedbryde disse barrierer. Ved et fornuftigt design af sikkerhedsmodel er konsekvenserne ved kompromittering af applikationer og data nemlig minimale – og de skalerer ikke ud af kontrol. Hvis applikationen og dens data kompromitteres, vil de således ikke kunne henføres til fysiske personer men kun virtuelle identiteter, og data vedrører kun lokale transaktioner og kan ikke sammenkobles med øvrige data, hvorved konsekvenserne ved kompromittering er inddæmmede til den lokale kontekst. Dermed falder behovet for at passe på data drastisk – og dermed de økonomiske omkostninger, der ville være forbundet hermed. Bemærk at disse fordele opnås uden at skulle stole på eller være afhængig af cloud leverandøren.

Et tænkt eksempel med følsomme (men ikke personhenførbare) data i skyen beskrives nedenfor i workshop case A.

7. Workshop Cases

>

I dette kapitel beskrives to cases[6], som blev behandlet på workshops som IT- og Telestyrelsen har afholdt i 2010. De to cases er tænkte eksempler som illustrerer realistiske situationer, hvor sikkerhed for alle parter og data i cloud kan opnås ved brug af en ny sikkerhedsmodel, hvor man bl.a. undgår at bruge personhenførbare data i cloud.

7.1 Workshop case A: Indberetning af indkomst for sæddonorer

På første workshop blev der gennemgået en case, der havde til formål at illustrere, hvorledes et realistisk problem med indlysende behov for anonymitet kan løses på en måde, hvor sikkerhed for alle parter opretholdes.

Problem
Sædbanken Cryos udbetaler kontante honorarer til deres donorer, der i sagens natur ikke ønsker, at omverdenen får kendskab til deres relation til Cryos. Imidlertid kræver SKAT, at Cryos indberetter de udbetalte honorarer via e-indkomstsystemet på donorernes CPR numre. SKAT kræver dette for at sikre, at der betales skat af indtægten. Dermed bliver det registreret centralt hos SKAT, hvem der er donorer hos Cryos, og den indberettede, månedlige honorarstørrelse fortæller noget om frekvensen af ydelsen. Dette leder altså til en konflikt med ønsket om hemmeligholdelse donorernes identitet.

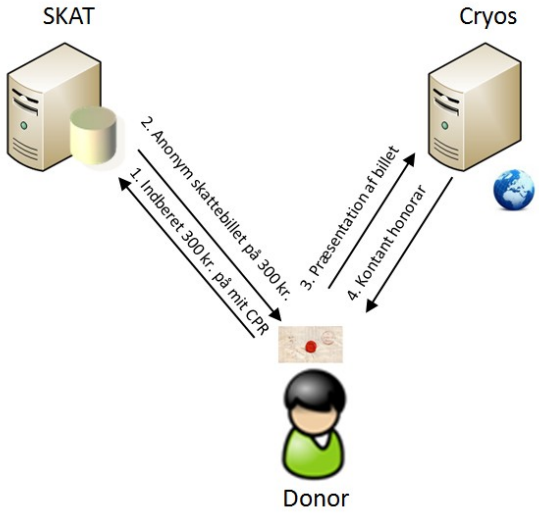
Workshopdeltagerne fik til opgave at undersøge, om man kunne sikre, at skatteindberetning har fundet sted *uden* at SKAT kan vide, hvad borgerne har tjent pengene på.

Løsningsforslag 1
Det første (simple) løsningsforslag går ud på, at SKAT etablerer et it-system, hvor personer kan indberette en skatteindtægt på et givet beløb på deres personnummer og herefter få udstedt en ikke-identificerende éngangsbillet (et kontekstafhængigt akkreditiv med en virtuel identitet), hvori den indberettede indtægt fremgår. Dette kunne eksempelvis være en web applikation hos SKAT, hvor borgeren kan logge ind med digital signatur (for at sikre man ikke indberetter indtægt på andres CPR numre). Efter log-in downloades den udstedte, virtuelle "skattebillet" til en lokal klient, hvorfra den senere kan overføres til arbejdsgiveren.

En sæddonor kan herefter mod præsentation af den virtuelle skattebillet til sædbanken få udbetalt et kontant honorar på et tilsvarende beløb. Billetten er indrettet således, at donoren kun kan benytte den én gang – i modsat fald frigives hans identitet og modtageren får mulighed for at opdage, at der er tale om genbrug.

[6] De to cases og forskellige løsningsforslag blev præsenteret af Priway.

>



Figur 6: Skatteindberetning uden identifikation

I en kontrolsituation kan sædbanken ved at fremvise de modtagne billetter (udstedt af SKAT) dokumentere (også overfor en tredjepart som eksempelvis en revisor), at der er indberettet skat for alle udbetalte honorarer – uden at SKAT eller andre får kendskab til identiteten af sæddonorerne. Dermed er både sikkerheden (korrekt skatteindbetaling) og donorernes privatliv overfor SKAT opnået.

Løsningsforslag 2
Ovenstående løsningsforslag løser en del af problemstillingen i forhold til hemmeligholdelse af sæddonorers identitet overfor SKAT - men har også uløste udfordringer:

- SKAT's indberetningsapplikation kan ikke flyttes til skyen fordi indkomstdata stadig er tæt koblede til CPR numre. Dermed ville kompromittering af SKAT's applikation i værste fald medføre, at samtlige danske borgeres indtægter bliver offentligt kendt.
- Hvis en person mister sit NemID kan andre lave identitetstyveri og indberette SKAT på hans personnummer. Hvis en hacker kan angribe DanID's centrale servere, kan han i værste fald lave skatteindberetninger for hele befolkningen eller udtrække alle personers indtægter. Dermed skalerer et sikkerhedsbrud i NemID eller DanID til SKAT.

For at imødegå disse udfordringer kan det første, simple løsningsdesign ændres i SKAT's ende, så skatteindberetning ikke knyttes til CPR numre men til virtuelle identiteter. Hver borger har dermed en "virtuel skattekonto", hvortil han kan indberette indkomst hos SKAT, hvis han kan bevise ejerskab over en hemmelig nøgle, der er knyttet til den virtuelle identitet, og som kun borgeren er i besiddelse af. Dermed vil SKAT potentielt kunne flyttes deres indberetningsapplikation og data til skyen, idet data nu ikke længere er personhenførbare. Udstedelsen af kontekstspecifikke akkreditiver efter skatteindberetning, som kan anvendes til at få løn udbetalt hos arbejdsgivere, er uændret fra den simple løsning.

>

Derudover bør man sikre, at en borger højst kan oprette én virtuel skattekonto, eksempelvis i et forsøg på at omgå progressiv beskatning – og af forskellige andre grunde kan SKAT have brug for kende den fysiske identitet bag hver virtuelle identitet. Dette kunne man løse ved at lave en ny applikation (som ikke kører i cloud), som hver borger anvender til at oprette den virtuelle skattekonto. Ved oprettelsen kunne borgeren anvende NemID / NemLog-in til at identificere sig med CPR nummer og initielt tilknytte sin virtuelle identitet og hemmelige nøgle – herefter anvendes CPR nummeret ikke længere. SKAT gemmer relationen mellem CPR nummer og virtuel skattekonto i en database[7] (som ikke befinder sig i cloud'en). Herefter vil al autentifikation af borgeren i forbindelse med skatteindberetning i cloud ske via borgerens hemmelige nøgle og ikke hans NemID.

På den måde opnår man flg. egenskaber:

- SKAT kan sikre sig, at der højst er én virtuel skattekonto til hvert CPR nummer.
- Ingen andre end borgeren kan lave indberetninger i borgerens navn (hvis de skal signeres med den hemmelige nøgle, som kun borgeren kender). Ikke engang DanID eller en hacker, som har kompromitteret DanID, vil kunne gøre det – de kan højst oprette en ny tom, virtuel skattekonto, hvis borgeren ikke har en i forvejen.
- Hvis databasen i cloud med skatteindberetninger kompromitteres, kan hackeren ikke henføre de virtuelle identiteter til fysiske personer. Dermed er data ikke særligt attraktive at angribe.
- SKAT kan udstede et bevis (et kontekstafhængigt akkreditiv) til borgeren på, at han har oprettet en skattekonto. Dette kan efterfølgende bruges til at bevise overfor andre tjenesteudbydere, at man er "kunde" hos SKAT.

Ovenstående model forudsætter, at en borger ikke han overdrage sine akkreditiver, virtuelle identiteter / hemmelige nøgler til andre – eksempelvis ved at forældre forsøger at indberette indtægt på deres børns virtuelle skattekonti for at undgå topskat. Dette findes der en række forskellige metoder til at forhindre, som det vil føre for vidt at komme ind på i detaljer her. I Cryos casen kunne man udstede de virtuelle skattebilletter til et tamper-resistant smart card med biometrisk autentifikation, som tilhører donoren. Her kan donoren så ved personligt fremmøde bevise, at han råder over kortet og herefter overføre skattebilletten til Cryos. En anden teknik til at modvirke overdragelse er at udstederen kan indlejre hemmeligheder (f.eks. elektroniske kontanter, passwords, kreditkortnumre eller personlige oplysninger), som er følsomme for brugeren, i den private nøgle. Da hemmelighederne skal angives for at kunne benytte den private nøgle, kan brugeren ikke overdrage sit token til en anden bruger uden også at overdrage hemmeligheden.

[7] Denne database bliver single point of failure. Til gengæld anvendes den ikke til daglig men kun ved oprettelse af nye skatteydere i systemet.

7.2 Workshop case B: Elektronisk ansøgning om job som pædagog

Problem
Den anden workshop case undersøgte, hvorledes sikkerhed kan opretholdes i en situation med elektroniske ansøgninger til et job som pædagog i en institution – eksempelvis gennem en elektronisk job-portal, der afvikles i skyen. Casen fokuserede på den tidlige fase i ansøgningsprocessen, hvor der foretages en første grovsortering af ansøgerne ud fra en række objektive kriterier, samtidig med at ansøgernes identitet skal forblive hemmelig.

Ansøgerne skal eksempelvis kunne fremlægge flg. slags dokumentation:

- Dokumentation for gennemført pædagoguddannelse (eksamensbevis fra anerkendt uddannelsessted)
- Beviser for efteruddannelse (kursusbeviser)
- Bevis for at man ikke er straffet for pædofili (del af straffeattest)
- Antal års erfaring som pædagog
- Referencer eller anbefalinger fra tidligere ansættelser
- Nuværende løn

Ønsket om beskyttelse af ansøgernes identitet tjener flere formål herunder:

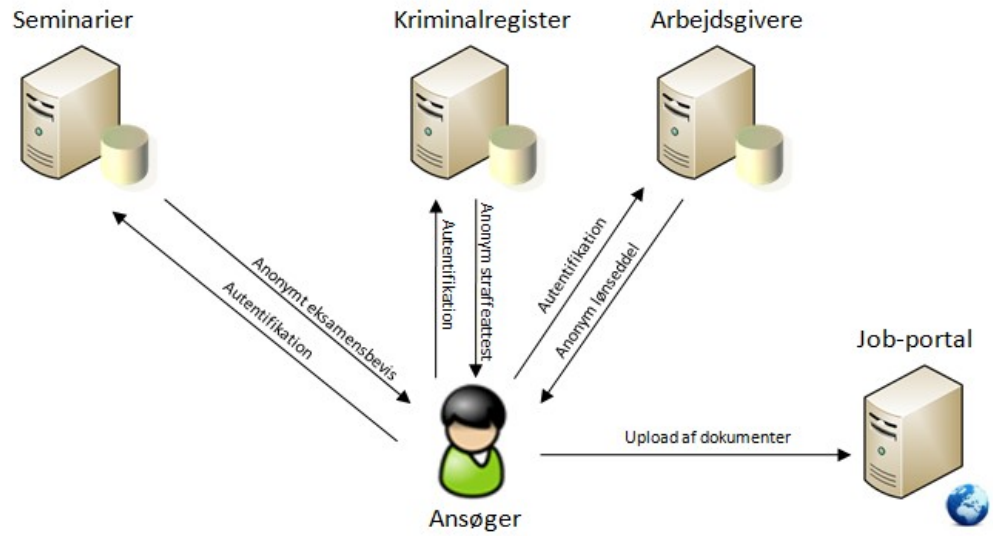
- Det sikrer ansøgerne mod diskrimination på grund af race, alder, køn eller andet.
- Nepotisme undgås.
- Det sikrer ansøgere, der sidder uopsagte stillinger, at deres nuværende arbejdsgiver eller kollegaer ikke får kendskab til, at de søger en ny stilling.

Løsning
Der blev på workshoppen diskuteret forskellige løsningsmodeller, men herunder gengives blot en enkelt. Forslaget bygger på antagelsen om, at en række institutioner etablerer it-systemer, der kan udstede autoritative dokumenter (f.eks. eksamensbeviser) som kontekstafhængige akkreditiver, hvori der kun indgår en virtuel identitet. Dvs. seminarier kan udstede elektroniske eksamensbeviser, kriminalregistret kan udstede elektroniske straffeattester, kursusudbydere kan udstede digitale kursusbeviser, og arbejdsgivere elektroniske beviser for ansættelser, opnået løn eller anbefalinger. Hver af disse kunne basere udstedelsen på, at brugeren forinden autentificerede sig fx med en digital signatur for at sikre, et beviser kun blev udstedt til rette vedkommende – eller de kunne mere ideelt basere sig på, at man havde tilknyttet virtuelle identiteter knyttet til hemmelige nøgler, som man kunne autentificere sig med.

En potentiel ansøger kan nu oprette en ansøgning på en job-portal uden at identificere sig og uploade de elektroniske akkreditiver, der dokumenterer de egenskaber, som kræves. Dokumenterne er digitalt signeret med udstedernes certifikat, og dermed kan ansøgeren bevise, at dokumenterne er udstedt af anerkendte institutioner. Samtidig kan dokumenterne ved udstedelse (eller via selektiv afsløring af attributter) være indsnævret til formålet, så der ikke afsløres mere information end højst nødvendigt. Et

>

eksempel herpå er straffeattester, hvor der ikke er nogen grund til at fortælle om evt. fartbøder mv., idet modtageren i dette tilfælde kun har krav på at vide, om personen er straffet for pædofili.



Figur 7: Ikke-identificerende ansøgning

Et andet perspektiv i casen er, portalen efter evaluering af ansøgerne kan udstede et bevis (i form af et kontekstafhængigt akkreditiv) til ansøgeren for, at han har søgt et job samt evt. indikere hvor langt han kom i ansøgningsprocessen. Med et sådant bevis kan ansøgeren dokumentere overfor andre, at han søger jobs og at disse er relevante (f.eks. at han kommer forbi den første grovsortering) – hvilket eksempelvis kunne tjene som dokumentation i forbindelse med udbetaling af arbejdsløshedsunderstøttelse.

Det blev på workshoppen diskuteret, at ikke alle dokumenter egner sig til at blive gjort ikke-identificerende. Eksempelvis kan en jobreference, der beskriver, at personen har været ansat i en given periode i en given funktion, godt indsnævre antallet af mulige personer så meget, at man vil kunne udlede personens identitet. Et andet eksempel er, at det med en ikke-identificerende reference er svært at ringe tilbage til en tidligere arbejdsgiver for at få en samtale om personens kvalifikationer. Endelig kan referencer indeholde ”ustruktureret prosa” skrevet af mennesker, hvor det ikke umiddelbart er muligt (maskinelt) at fjerne identificerende information.

Disse forhold blev dog ikke vurderet som en hindring for, at casen kunne løses fornuftigt efter ovenstående principper. Her kan en praktisk løsning være at afvikle ansøgningsprocessen i flere trin: i de første trin foretages den indledende screening af ansøgerne, hvor opfyldelse af de formelle krav verificeres mens ansøgeren ikke er identificeret (og i cloud), mens der i de senere trin i processen sker en (delvis) identificering af ansøgerne i forbindelse med vurdering af referencer samt personlige samtaler med kandidaterne. Her bør man indrette systemet, så åbningen af de identificerende dokumenter senere i processen ikke sker i cloud løsningen – eksempelvis kan dokumenterne krypteres under en hemmelig nøgle, som kun reviewpanelet har adgang til.

8. Andre eksempler

>

I dette afsnit beskrives yderligere en række eksempler på, hvorledes sikkerhedsmodellen kan anvendes i form af en række case beskrivelser. Beskrivelserne er holdt på kort form, da eksemplerne i høj grad bygger på de principper, der er introduceret i de to foregående cases.

Case: Feedback til lærer på kursus

Problem
Et universitet ønsker at give studerende mulighed for at give feedback på deres kurser og undervisere via deres studieportal. Det skal kunne ske uden at blive identificeret, så de studerende ikke behøver at frygte repressalier, hvis de kritiserer en lærer. Det skal samtidig sikres, at kun studerende, der har fulgt et specifikt kursus, kan afgive feedback om kurset. Desuden skal det sikres, at hver studerende kun afgiver feedback én gang.

Løsning
Universitetet bygger to systemer. I det ene system trækker de studerende et kontekstafhængigt akkreditiv med en virtuel identitet og i det andet giver de feedback med dette. Det første system autentificerer den studerende (eksempelvis på baggrund af en digital signatur) og udsteder en ikke-identificerende engangsbillet med en attribut der fortæller, hvilket kursus den studerende har deltaget i. Samtidig registreres det, at den studerende har trukket en billet, så der ikke efterfølgende kan trækkes flere (for dette kursus). I det andet system, hvor der kan afgives feedback, modtages og valideres billetten. Det kan her kontrolleres, at der er tale om en legitim stemme via kursusattributten, samt at den ikke er brugt før. Det er derimod *ikke* muligt at udlede ud fra akkreditiverne, hvem der giver feedback – selv hvis de to systemer arbejdede sammen om dette.

Case: Elektroniske auktioner / licitationer

En anden variation over de foregående to cases er elektroniske auktioner eller licitationer. Her kan man etablere et registreringssystem, hvor deltagerne bliver identificeret og godkendes (prækvalificeres) til at måtte byde. Herefter får de udstedt et kontekstafhængigt akkreditiv, som skal bruges i det system, der modtager budene. Det er endda muligt at signere det afgivne bud med den private nøgle hørende til akkreditivet, så uafviselighed kan opnås.

Case: Adgang til videnskabelige artikler

Problem
Et universitet abonnerer på videnskabelige tidsskrifter, som kan læses on-line. Man ønsker at give adgang for registrerede studerende samt undervisere, men udbyderen af publikationen må ikke vide, hvem der læser hvilke artikler – kun at der er tale om berettiget brug.

Løsning
Universitetet etablerer et system, som kan udstede et kontekstafhængigt akkreditiv til studerende og lærere, hvori det via en attribut fremgår, at de berettiget til at læse

publikationer fra en bestemt udbyder. Udbyderen kan nu validere det kontekstafhængige akkreditiv og give adgang til artiklerne på den baggrund – men uden at kunne spore, hvem der læser hvad. Samtidig kan udbyderen registrere, hvor mange forskellige brugere fra et givet universitet, der tilgår udbyderens artikler, for dermed at kunne sammenligne med universitetets abonnement, hvor prisen kunne afhænge af antallet af brugere.

Se også en case med indhentning af lånetilbud i det følgende kapitel.

Case: Et dating tjeneste

Problem
En dating tjeneste[8] ønsker viden om brugernes alder samt køn, således at brugerne ikke kan give urigtige oplysninger om disse forhold i deres personlige profiler. Eksempelvis vil man udelukke personer under 16 år samt undgå brugere, der laver en profil med forkert alder eller køn for sjov. Samtidig vil man undlade at registrere brugernes identitet, idet dette vil afskrække mange fra at benytte tjenesten, hvis deres handlinger kan spores til deres identitet.

Løsning
Dating siden udvides, så den tillader log-in med kontekstafhængige akkreditiver, hvori der skal fremgå to attributter: alder og køn. Til at udstede akkreditiverne anvendes enten en eksisterende tjeneste eller dating siden kan udvikle sin egen, der eksempelvis på baggrund af log-in med NemID kan udlede værdien af attributterne og udstede et akkreditiv med disse. På den måde kan brugerne oplyse mindst mulig information overfor datingsiden og samtidig være sikre på, at deres gøren og laden ikke kan spores til deres øvrige digitale aktiviteter på nettet.

En mere avanceret udvidelse kunne være, at datingsiden kan udelukke brugere fra tjenesten, hvis de opfører sig i strid med sidens etiske retningslinjer – stadig uden at kende brugerne. Dette kan eksempelvis opnås ved at brugerne beviser, at de ikke befinder sig på en liste af udelukkede brugere – dog stadig uden at afsløre, hvem de er – og på en sådan måde, at brugerne ikke bare kan skifte virtuel identitet, hvis de bliver udelukket.

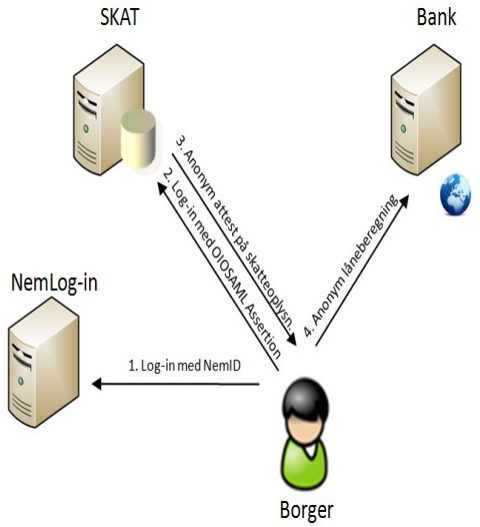
[8] Siden love.dk tillader eksempelvis brugerne at logge ind med NemID.

9. Relation til eksisterende fællesoffentlig brugerstyring >

Den beskrevne sikkerhedsmodel kan betragtes som en naturlig videreudvikling af eksisterende standarder, arkitekturer og løsninger indenfor fællesoffentlig brugerstyring som eksempelvis NemID, OIOSAML og OIOIDWS profilerne samt NemLog-in og KFOBS løsningerne. Der er således tale om en evolution frem for en revolution.

Som tidligere beskrevet er modellen grundlæggende en fødereret model, hvor brugere får adgang til tjenester ved at fremvise akkreditiver (security tokens) udstedt af en tredjepart. Den primære forskel er, at der er tale om ny slags akkreditiver / security tokens, der sikrer at brugeren ikke bliver identificeret. Man kan eksempelvis forestille sig, at eksisterende Security Token Services[9] videreudvikles til at kunne udstede kontekstafhængige akkreditiver.

En anden lighed er, at brugeren ofte skal autentificeres, før der kan udstedes et akkreditiv. Her vil den digitale signatur / NemID således kunne anvendes på samme måde som brugeren i dag kan logge på NemLog-in løsningen. Samspillet mellem eksisterende brugerstyringsløsninger og nye elementer med kontekstafhængige akkreditiver er illustreret på nedenstående figur:



Figur 8: Samspil med eksisterende løsninger

Figuren illustrerer en bruger, som ønsker et tilbud fra en (fremmed) bank på et lån, men som ikke i første omgang ønsker at afsløre private forhold så som CPR-nummer, før han har set tilbuddet og besluttet sig. Denne case kunne eksempelvis løses ved, at brugeren logger på den eksisterende NemLog-in løsning med sit NemID, og herefter får adgang til SKAT's løsninger, der kan udstede et kontekstafhængigt akkreditiv (knyttet til en virtuel identitet) med brugerens indkomstoplysninger. Brugeren kan nu præsentere akkreditivet for banken som grundlag for låneberegningen. Banken kan

[9] KFOBS løsningen (den konsoliderede, fællesoffentlige brugerstyringsløsning) etableres med en Security Token Service i henhold til OIOIDWS profilerne for identitetsbaserede web services, og er forberedt på muligheden for indførelse af kontekstafhængige akkreditiver.

ved at verificere SKAT's signatur på akkreditivet se, at oplysningerne er ægte, men kan ikke henføre dem til brugerens identitet. På denne måde er eksisterende brugerstyringsløsninger kombineret med den nye model. Casen kan også implementeres uden kontekstafhængige akkreditiver, men dog næppe under realisering af den samme sikkerhed både for bruger (pseudonymitet) og bank (autentiske skatte- og indkomstdata om aktuel bruger).

Der er dog også en række forskelle i forhold til eksisterende teknologier og løsninger, herunder at tjenesteudbydere og udstedere aldrig kommunikerer direkte sammen. SAML protokollerne er således ikke kompatible med modellen (en SAML IdP forudsættes at vide hvilken serviceudbyder, der er tale om), hvor WS-Trust som nævnt godt kan anvendes. Endelig forudsætter den brugercentriske model, at der findes klienter hos brugerne, der understøtter denne interaktionsform, hvorimod nuværende brugerstyringsløsninger kun forudsætter en standard web browser.

Offentlige myndigheder kan håndtere dette ved at udstille brugerdata på både traditionelle måder samt via tjenester, der kan danne kontekstafhængige akkreditiver. Dette giver brugerne mulighed for at tilvælge de nye privacy-venlige former i takt med at klienter udbredes og efterspørgslen modnes. Moderne applikationer kan designes og udvikles, så de er uafhængige af, hvordan data om brugeren tilflyder systemet – såkaldte "claims aware" applikationer. På den måde er applikationerne forberedt for de nye typer akkreditiver og skal ikke senere omprogrammeres.

9.1 Interaktion med brugerne

Den skitserede sikkerhedsmodel gør det muligt at designe applikationer, hvor brugerne har kontrol over deres data. Dette forudsætter dog, at brugerne aktivt deltager og at brugerinteraktionen både er effektiv, forståelig og brugervenlig for den gruppe af brugere, man henvender sig til. I en række situationer kan man forestille, at en del af brugerne ikke har ønske om eller viden nok til at kunne deltage aktivt i orkestreringen af akkreditiver og identiteter, og her kan det således være relevant at designe applikationen, så det kan vælges fra og lade valget være op til brugeren. Visse brugere har måske i bund i grund tillid til, at offentlige og private virksomheder (eksempelvis banker) behandler deres data sikkert, og er måske ikke interesserede i at træffe ekstra valg.

Der er altså ikke tale om, at de nye sikkerhedsmodeller nødvendigvis tvinger brugerne til gøre noget anderledes i forhold til, hvordan de anvender it-løsninger i dag. Essensen er, at de nye sikkerhedsparadigmer modsat de traditionelle sikkerhedsmodeller giver brugeren en valgfrihed med hensyn til hvornår, brugeren vil involveres i orkestreringen af identiteter og akkreditiver.

10. Perspektiver i forhold til interoperabilitet og innovation på længere sigt >

I beskrivelsen af den nye sikkerhedsmodel er der i dette papir fokuseret på, hvorledes sikkerhed for alle parter i en transaktion kan opnås samtidig. Derudover kan den beskrevne sikkerhedsmodel med fordel anvendes ved cloud computing. Der er dog en række yderligere egenskaber, som også er ønskelige i en ny sikkerhedsmodel. Disse egenskaber blev også behandlet på de to workshops, som har været grundlaget for dette diskussionspapir. Her vil vi særligt fremhæve aspekterne *interoperabilitet* og muligheden for *behovsdreven innovation*.

Interoperabilitet
Ved interoperabilitet forstås helt overordnet, at en sikkerhedsmodel bør være åben for, at nye elementer kan introduceres i fremtiden og spille sammen med eksisterende løsninger. Dette kan eksempelvis være indførsel af nye typer akkreditiver, kommunikationskanaler, klienter etc. Understøttelse af interoperabilitet har dermed en direkte sammenhæng med en virksomheds mulighed for at være innovativ.

Et konkret eksempel kunne være, at en selvbetjeningsløsning ikke kun skal være tæt bundet til danske akkreditiver. Der skal i systemdesignet skabes mulighed for, at borgere fra andre EU lande også kan anvende deres lokale akkreditiver til at tilgå selvbetjeningsløsningen, så længe de opfylder applikationens krav til sikkerhed og den nødvendige information i øvrigt er til stede. Denne form for interoperabilitet er mere ambitiøs end den traditionelle forståelse af begrebet, hvor softwareleverandører kan implementere en teknisk standard (f.eks. GSM) således at deres produkter kan tale sammen, men hvor der godt kan være tale om en høj grad af ”hard coding” til standarden – såkaldt ”plug” kompatibilitet.

En mere ambitiøs form for interoperabilitet kan ske modeldrevet eller på det semantiske niveau ved brug af ontologier, hvor en applikation eksempelvis udtrykker sine behov i form af en eksplicit politik, således at anden software på ”run-time” kan læse politikken og dynamisk forsøge at opfylde den. Der er altså tale om de velkendte arkitekturprincipper for løs kobling og sen binding. I praksis betyder det, at åbne systemer bør være lyttende, således at de fortæller hvad de har brug for – i stedet for at diktere det.

Behovsdreven innovation
Ved behovsdreven innovation forstås, at det er brugerne, der gennem deres behov og efterspørgsel af løsninger styrer flow af data og samspillet mellem systemerne. Den behovsdrevne innovation forudsætter fleksible, interoperable systemer, der kan indrette sig efter den aktuelle situation. Hvis systemerne derimod er stive og låser brugerne fast uden valg, er der ikke mulighed for, at den ønskede dynamik og innovation kan opstå.

Målet med den behovsdrevne innovation er at opnå synergier, genbrug af løsningselementer, facilitere konkurrence samt forbedre produktivitet og kvalitet i løsningerne. Derudover nedsætter man fremtidige omkostninger, fordi man kan videreudvikle systemet uden at være tvunget til at bygge helt nye løsninger.

Ud fra et økonomisk perspektiv syntes der derfor at være god grund til at designe systemer, der i højere grad tager højde for interoperabilitet og behovsdreven innovation.

11. Opsummering / Diskussion

>

11.1 Opsummering

På baggrund af internettets forandrende karakter og at perimeteren som sikkerhedskoncept er kraftigt udfordret, er der behov for at videreudvikle traditionelle sikkerhedsmodeller til at modsvare fremtidens krav.

Det er blevet beskrevet, hvordan sikkerhedsmodeller med fordel kan udvikle sig mod et nyt paradigme der:

- Giver sikkerhed for alle parter i en transaktion (herunder brugerne).
- Dekobler data fra brugernes fysiske identitet.
- Er baseret på kontekstafhængige akkreditiver og transaktionsisolering
- Går fra et identifikationsbaseret paradigme til et valideringsorienteret paradigme.

Hvis disse egenskaber indbygges i designet af applikationer, er det i en række tilfælde muligt at benytte cloud computing uden større risici[10], selvom der indgår følsomme data. Hvis applikationen og dens data kompromitteres, vil de således ikke kunne henføres til fysiske personer men kun virtuelle identiteter, og data vedrører kun lokale transaktioner og kan ikke sammenkobles med øvrige data, hvorved konsekvenserne ved kompromittering er inddæmmede til den lokale kontekst. Bemærk at disse fordele opnås uden at skulle stole på eller være afhængig af cloud leverandøren.

Dernæst er en række cases blevet beskrevet som samlet illustrerer, hvorledes ovenstående principper kan benyttes i design af sikkerhedsmodeller for tænkte applikationer.

Endelig blev det beskrevet, hvordan den beskrevne sikkerhedsmodel er en videreudvikling af eksisterende standarder, arkitekturer og løsninger inden for den fællesoffentlige brugerstyring.

11.2 Fremtidsmusik eller eksisterende teknologi?

Selvom modellerne beskrevet i dette papir ved første øjekast kan forekomme avancerede, findes de basale mekanismer allerede implementeret i kommercielle produkter, og de første pilotprojekter er allerede afviklet med succes.

Som eksempel kan nævnes, at firmaet Fraunhofer FOKUS, som står bag det tyske eID-system, har udviklet en løsning, hvor borgere via kontekstafhængige akkreditiver[11] anonymt kan deltage i meningsmålinger men samtidig via det tyske eID kort kan bevise, at de er myndige samt i hvilken by, de bor. Eksempelvis må man kun deltage i afstemninger for Berlin, hvis man er bosiddende her. For detaljer om det konkrete pilotprojekt henvises til [EPAR] samt siden:

[10] Her tænkes primært på tab af fortrolighed og ikke tab af tilgængelighed eller integritet.
[11] UProve teknologi

>

http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/eid.aspx

Når man designer nye applikationer i dag, bør disse indrettes fleksibelt, så man i fremtiden let kan anvende de nye typer akkreditiver uden at applikationen grundlæggende skal skrives om. I stedet bør håndtering af akkreditiver være udskilt i et separat identitetslag, som kan udbygges efterhånden som behovet opstår - uden at forretningsfunktionaliteten i applikationen påvirkes.

11.3 Diskussion

Der knytter sig en række spørgsmål til de principper for en ny sikkerhedsmodel, som er beskrevet i dette papir. Nogle af dem vil vi berøre i dette afsnit, hvor vi også lægger op til at føre debatten videre på digitaliser.dk.

Nye løsningsmuligheder
Den beskrevne sikkerhedsmodel giver en række muligheder for nye løsninger. Eksempelvis giver teknologien mulighed for, at man kan indhente lånetilbud fra pengeinstitutter anonymt - det vil sige uden at ”give” flere oplysninger om sig selv til pengeinstituttet, end der er behov for i forbindelse med den pågældende låneansøgning. Man vil med denne model kunne designe et system, hvor man i en låneansøgning ”kun” oplyste om sine relevante økonomiske forhold.

Teknologien vil givetvis også kunne anvendes til en række andre nye løsninger, som vi ikke har tænkt på i dag. Vi vil gerne høre bud på sådanne løsninger på digitaliser.dk

Demokrati og social responsibility
Privatlivsbeskyttelse har som oftest været et element der er tilkoblet en løsning efter den er blevet iværksat. Med Privacy-by-Design og Security-by-Design er det muligt at tænke sikkerhed og privatlivsbeskyttelsen ind i selve designet af systemet. Spørgsmålet er, om der ikke i et demokratisk samfund bør være mulighed for at beskytte sit privatliv på nettet? Om muligheden for at beskyttes ens privatliv ikke bør tænkes ind i systemerne fra starten af?

Det er relevant at tænke over, hvilken udvikling vi går i møde, hvis der ikke etableres mekanismer, der kan imødekomme privatlivsbeskyttelsen. Spørgsmålet er især aktuelt, når der tænkes på den voksende datamængde på nettet, samt de øgede teknologiske muligheder for at indhente disse automatisk.

Det er i den forbindelse relevant at spørge om, hvad det i det hele taget er for data, som private virksomheder kan trække ud af vores færden på nettet?
Hvad er incitamenterne for en privat virksomhed til at højne privatlivsbeskyttelsen? Et argument kan være, at det er billigere at passe på få eller ikke-følsomme data end at passe på mange, følsomme data. Omvendt bygger en række virksomheders forretningsmodeller på, at de indsamler så mange oplysninger om deres brugere som muligt og herefter kombinerer dem på forskellig vis. Debatten om retten til privacy er taget til de seneste år og internetbrugerne er begyndt at sætte højere krav samt efterspørge løsninger, der kan leve op til disse. Man kan forestille sig, at virksomhederne frivilligt begynder at sikre en højere grad af privatlivsbeskyttelse for at vise, at de tager et socialt ansvar – eller ser det som en ren og skær konkurrenceparameter, der differentierer dem fra konkurrenterne. Endelig kan der

være en række applikationer, hvor brugerne simpelthen ikke vil medvirke, hvis ikke de har tillid til, at deres privatliv respekteres.

Arbejdet med nye sikkerhedsmodeller indeholder tilsyneladende flere perspektiver og potentialer, der rækker udover det rent sikkerhedsmæssige område, og som det er relevant at drøfte yderligere.

11.4 Spørgsmål på digitaliser.dk

Nedenstående spørgsmål vil blive diskuteret på digitaliser.dk, hvor der også er mulighed for at diskutere andre vinkler:

1. Er de nye sikkerhedsmodeller reelt bedre?

- Er der behov for at videreudvikle digitale sikkerhedsmodeller i den retning, som er skitseret i dette papir.
- Er sikkerhedsmodellerne, som beskrevet i dette papir sikre og fleksible nok?

2. Hvordan kommer vi til den nye model – hvilke udfordringer er der?

- Hvilke praktiske udfordringer er der for at iværksætte nye sikkerhedsmodeller?
- Hvad er det for en holdning, der skal gøres op med for at komme i gang med nye sikkerhedsmodeller?

3. Hvor kan den nye model iværksættes enkelt?

- Kan nogen af de principper der er præsenteret i dette papir eksempelvis implementeres i mindre skala?
- Hvilke områder vil det være relevant at anvende de nye sikkerhedsmodeller på?
- Hvordan designes applikationer, så de er forberedt på den nye sikkerhedsmodel?

4. Hvad kræver de nye sikkerhedsmodeller af brugerne?

- De nye sikkerhedsmodeller kan i visse tilfælde forudsætte, at brugeren (eller rettere dennes klient) skal administrere en række nøgler til forskellige tjenester og services. Stilles der for høje krav til brugernes kompetencer til at indgå i interaktionen med applikationen samt træffe valg?
- Det kræver også, at brugerne aktivt tager stilling til, hvilke oplysninger brugeren ønsker at videregive til forskellige services og tjenester. Er det noget, den gennemsnitlige danske bruger vil interessere sig for?

5. Hvilke nye løsninger kan du forestille dig?

Vi håber meget, at du vil bidrage med din holdning ved at følge dette link:

[Indsæt link til spørgsmålene på digitaliser.dk her]

12. Terminologi

>

Privacy
Retten til privatliv i forhold til éns færden både offentligt og privat, i det fysiske rum, på telefon og på internettet. Privacy kan forstås som en sikring mod forskellige former for risici – herunder risikoen for tab af kontrol over personlig information. Se evt. flere definitioner i [OVG].

På de afholdte workshops blev begrebet privacy opfattet som sikkerhed ud fra én persons synsvinkel (brugeren / borgeren) - se [PRIW1]. Et afgørende mål med de nye sikkerhedsmodeller er at opnå en balance, hvor der er sikkerhed for flere / alle parter (såkaldt *multiparty security*).

Udsteder (af akkreditiv)
En udsteder af akkreditiver er en betroet tredjepart, som andre stoler på i forhold til at attestere visse attributter om brugere – eksempelvis en persons alder eller at vedkommende er autoriseret læge.

Serviceudbyder
En organisation som udbyder en digital service / applikation til brugerne, og giver adgang til funktioner og data på baggrund af præsenterede akkreditiver. Dette kan eksempelvis være en digital selvbetjeningsløsning hos en offentlig myndighed. Denne rolle betegnes ofte for ”relying party” eller ”verifier” på engelsk, idet der indgår validering af de af brugeren præsenterede akkreditiver.

Identitet
En teknisk repræsentation af en juridisk person i en given sammenhæng.

Virtuel identitet (pseudonym)
En virtuel identitet er en digital stedfortræder for den fysiske person – analogt til når forfattere i den fysiske verden udgiver tekster under et pseudonym. Virtuelle identiteter benyttes ofte til at ramme en balance mellem anonymitet og identifikation – hvor brugeren hverken bliver identificeret overfor serviceudbydere (potentielt tab af brugerens sikkerhed) men heller ikke kan være helt anonym (potentielt tab af ansvarlighed / serviceudbyderens sikkerhed). Begge ekstremer (fuld identifikation og fuld anonymitet) kan rummes indenfor begrebet, men i mange situationer er ingen af dem ønskværdige.

Identifikation
En proces hvor en persons identitet fastlægges – eksempelvis via et CPR nummer.

Autentifikation
En proces hvormed en bruger genkendes. Visse autentifikationsmekanismer identificerer brugeren direkte (eksempelvis en OCES digital signatur) mens andre kun

tilvejebringer en teknisk nøgle (virtuel identitet). Autentifikation sker ofte ved præsentation af et akkreditiv[12] (se nedenfor).

Akkreditiv (eng. credential)
En samling data relateret til en bruger, der typisk udstedes af en tredjepart, og som en bruger kan præsentere (evt. dele af) med henblik på at få adgang til et it-system. Eksempler er traditionelle akkreditiver er X.509 certifikater, SAML Assertions og brugerid+kodeord.

Kontekstafhængigt akkreditiv (eng. anonymous credential)
Et akkreditiv som ved brug ikke identificerer indehaveren men i stedet rummer en virtuel identitet (pseudonym), som ikke kan spores til udstedelsesprocessen, og hvor brugeren har direkte kontrol med hvilke attributter fra akkreditivet, der frigives.

Transaktionsisolering
Transaktionsisolering er det princip, at en brugers data hørende til en specifik kontekst kan adskilles, så de ikke kan sammenkobles med andre data eller handlinger for den samme bruger. Isoleringen kan både ske mellem forskellige serviceudbydere eller indenfor samme serviceudbyder. Som eksempel på det sidste kan nævnes, at transaktionsisolering kan benyttes på en jobsøgningsportal (se case beskrivelse tidligere i dokumentet), så portalen ikke kan udlede, at samme bruger søger flere forskellige jobs, idet brugerens ansøgninger er isolerede transaktioner. Transaktionsisolering kan bl.a. opnås ved at brugeren benytter forskellige virtuelle identiteter til forskellige transaktioner samt benytter kontekstafhængige akkreditiver, som ikke indeholder nogle korreleringsnøgler, der muliggør sammenkobling. Bemærk at selvom serviceudbydere ikke kan sammenkoble isolerede transaktioner, da kan brugeren evt. godt (frivilligt) bevise (ved brug af private nøgler), at et sæt af isolerede transaktioner alle hidrører fra ham.

(SAML) Assertion
En SAML Assertion er et traditionelt akkreditiv på XML format. En SAML Assertion er som regel digitalt signeret af udstederen og indeholder attributter om brugeren (f.eks. CPR numre eller persistente pseudonymer) samt autentifikationshændelser (f.eks. at brugeren loggede ind med digital signatur kl. 12:56). For detaljer om OIOSAML henvises til http://digitaliser.dk/resource/524480 og for detaljer om SAML standarden henvises til http://docs.oasis-open.org/security/saml

[12] I praksis autentificerer man ofte ved at bevise kendskab til en hemmelighed (en privat nøgle), der er knyttet til akkreditivet (fx. en offentlig nøgle).

13. Referencer

>

[BRA] ”Rethinking Public Key Infrastructures and Digital Certificates – Building in Privacy”, Stefan A. Brands, MIT Press.

[UPCS] “U-Prove Cryptographic Specification V1.0”, Stefan Brands og Christian Paquin, Microsoft Corporation.

[IDMX1] “A Quick Introduction to Anonymous Credentials”, Gregory Neven, IBM Zürich Research Laboratory.

[IDMX2] “Specification of the Identity Mixer Cryptographic Library”, Jan Camenish, IBM Zürich Research Laboratory.

[UPROV1] “U-Prove Technology Overview”, Stefan Brands, Microsoft Corporation.

[UPROV2] “U-Prove CTP White Paper”, Christian Paquin og Greg Thompson, Microsoft Corporation.

[OVG] ”De overvågede”, DI & Forbrugerrådet.

[EPAR] “eParticipation Scenario Reference Guide”, Microsoft Corporation.

[PRIW1] “Without PETs, democracy and markets won’t work”, Stephan J. Engberg, Priway. http://ec.europa.eu/justice/news/events/workshop_pets_2009/presentations/ENGBERG_Stephan.pdf

[PRIW2] “A World without PETs”, Stephan Engberg, Priway. http://danskprivacynet.files.wordpress.com/2008/08/a20world20without20pets20v2.pdf

>

<