
# Original och verifikationer i en digital värld

## – pilot och sex lösningar med blockkedjeinspirerad teknik

Projektrapport av FAR, Skatteverket, Bolagsverket, Kairos Future och iTeam i samarbete med SEB, Visma, Fortnox, Deloitte, PwC, KPMG och Grant Thornton.

November 2019

KAIROS FUTURE

# Sammanfattning

FAR, Skatteverket, Bolagsverket, Kairos Future och iTeam har i samarbete med SEB, Visma, Fortnox, Deloitte, PwC, KPMG och Grant Thornton arbetat vidare med säkra digitala lösningar för redovisning, revision och skatt.

## Huvudslutsatser i projektet är

• Att tillämpningsområdena för blockkedjeinspirerad teknik är betydligt större än vad de flesta föreställt sig när det gäller möjligheten att skapa system och processer som är säkra, medger lämplig nivå på integritet och möjliggör ansvarsutkrävande ”accountability”. Tekniken och exempelvis de lösningar som projektet arbetat med är i många fall den enda möjliga för att uppnå en tillfredsställande nivå på dessa tre samtidigt. Samhällsnyttan är därför mycket stor.

• Att fokus på strikt tillämpning av blockkedjeteknik, dvs. med fokus på lika rätt hos alla databaser/noder i ett distribuerat nätverk, är starkt begränsande för möjligheterna och bör undvikas. Fokus bör ligga på nytta och genomförbarhet – inte att uppfylla strikta definitioner på en blockkedja. Blockkedjeteknik är ett specialfall som är intressant men i praktiken sannolikt blir ovanligt att tillämpa under överskådlig tid.

• Att standarder och riktlinjer för användandet av blockkedjor bör skrivas med hänsyn till ovanstående, dvs. definitionen av vad som avses bör omfatta en bredare definition än vad som är vanligt idag.

Fas ett i projektet presenterades den 28 januari. I fas ett identifierades tre lösningsförslag digitala kvitton, personalliggare och fullmakter. Projektets fas två har ytterligare stärkt tesen att lösningarna är de bästa kända i världen. Tre nya lösningsförslag har även identifierats som de bästa kända för närvarande. Arbetet med att utreda de rättsliga förutsättningarna för digitala kvitton och att ta fram och vidareutveckla den tekniska lösningen för kvitton och fakturor har påbörjats. För att säkra och digitalisera kvitton och fakturor finns nu en fungerande pilot på www.digitala-kvitton.se och koden finns open source på Github[1].

## Lösningarna är

1. Pilot och lösning säkra digitala kvitton
2. Nästan färdig pilot säkra fakturor
3. Fullmakter som gäller hos många olika parter
4. Behörigheter att företräda en organisation
5. Personalliggare
6. Inlämning av företagsuppgifter till myndigheter

## Blockkedjeinspirerad teknik

Utgångspunkten i projektet har varit blockkedjeteknik. Den snäva definition som många använder för blockkedjor och distributed ledger har emellertid visat sig svår att realisera i praktisk nytta. I detta projekt har vi istället använt oss av de verktyg och synsätt som blockkedjan synliggjort och kallar detta Blockkedjeinspirerad teknik.

”En lösning i alla situationer där en central aktör som samlar in fullständig data kan lösa uppgiften - men där man av något skäl vill undvika det. Skälen kan till exempel vara integritet, manipulation, cyberrisker, tillgänglighet eller likabehandling.”

Den relevanta frågan många ställt sig har varit – men vad ska vi egentligen ha blockkedjan till? Frågan när det gäller blockkedjeinspirerad teknik, dvs. den krypteringsteknik Blockkedjan består av är närmast den motsatta. Finns det några andra sätt än denna typ av lösning? När vi arbetat med projektet och frågat experter så är svaret i princip ett av tre alternativ. 1. Vi gör redan så 2. Vi känner inte till något annat sätt att lösa det på än det ni föreslår 3. Vi har ingen lösning.

## Compliance by design

Visionen kan kallas compliance by design, dvs. det ska vara lätt att göra rätt och svårt att göra fel för såväl medborgare och företag som myndigheter. Är vi intresserade av att skapa digitala, säkra och anonymiserade lösningar är det i princip de alternativ som beskrivs som finns att tillgå. Den rådande trenden idag är att prioritera enkelhet och brottsbekämpning men kompromissa med integritet och datasäkerhet.

Ambitionen med detta projekt är att ta fram lösningar och visa att det går att åstadkomma samma nytta utan att äventyra integritet och säkerhet.

# Innehåll

# Inledning

Denna rapport sammanfattar ett projekt som fokuserat på att undersöka möjligheterna med blockkedjeteknik och även annan teknik som kan sägas inspireras av blockkedjetekniken. Projektet har pågått i två faser. Den första fasen avslutades i januari 2019 och rapporten finns att ladda ner på https://www.far.se/globalassets/pdf-ovrigt/report-swe-blockkedja-skatt.pdf

I denna fas två av projektet har arbetet med lösningarna fortsatt. Framförallt har arbetet fokuserat på att bygga en teknisk pilot för digitala kvitton och säkra fakturor samt att utreda de juridiska frågeställningar, utmaningar och möjligheter som finns på dessa områden för lösningarna.

För att säkra och digitalisera kvitton och fakturor finns nu en fungerande pilot på www.digitala-kvitton.se och koden finns open source på Github https://github.com/iTeam1337/digital-receipts.

Arbetet med övriga lösningar har också fortsatt. När det gäller sink, särskild inkomstskatt för personer bosatta utomlands, har arbetet fortsatt i Skatteverkets regi som ett eget projekt.

Inom ramen för projektet har arbetet fortsatt med

1. Pilot och lösning säkra digitala kvitton
2. Säkra fakturor
3. Fullmakter som gäller hos många olika parter
4. Behörigheter att företräda en organisation
5. Personalliggare
6. Inlämning av företagsuppgifter till myndigheter

## Syfte

Syftet med projektet är att identifiera utmaningar i dagens verksamheter kopplade till redovisning, revision och skatt. Därefter att beskriva dessa utmaningar samt beskriva möjligheter att lösa dessa med hjälp av digitala informationskedjor, exempelvis blockkedjan.

Målsättningen med projektets fas två har varit att säkerställa huruvida de föreslagna lösningarna i projektets fas ett verkligen var så bra som det framstod. Ambitionen har varit att testa teknik, rättsliga frågor och bedöma genomförbarheten i verksamheten.

Ambitionen har också varit att testa förslagen på fler andra aktörer, se vad andra har gjort och vad det finns för lärdomar att dra av detta.

Projektet har även arbetat vidare med frågorna för att utveckla nya lösningar.

## Ansvarsbegränsning

Ingen organisation eller person tar ansvar för innehållet i rapporten. Rapporten och arbetet är koordinerat av Magnus Kempe med stöd av Göran Sundin, Pablo Dias-Taguatinga, Annika Follin och Karin Apelman. Arbetet med teknik har projektletts av Mikael Gråborg. I rapporten används ordet ”vi” och då avses projektgruppen, även om projektgruppen inte tar ansvar för eller är enig kring de formuleringar som finns i rapporten.

Rapporten gör inte anspråk på att de olika lösningarna ryms inom gällande lagstiftning. Det finns en del rättsliga frågor som belyses och tänkt hantering av dessa. Rapporten ska vara en inspirationskälla till fortsatt arbete med de möjligheter som blockkedjeinspirerad teknik ger.

# Medverkande

Medarrangörer i projektets fas två har varit FAR, Skatteverket, Bolagsverket och Kairos Future. Medverkande iTeam, Visma, Fortnox, SEB, PwC, Deloitte, Gran Thornton och KPMG.

## Från projektgruppen har följande medverkat

Karin Apelman, FAR
Claes Håkan Johansson, FAR
Åsa Olsson, FAR
Lennart Ihredahl, FAR
Göran Sundin, Skatteverket
Pablo Dias Taguatinga, Skatteverket
Björn Erling, Skatteverket
Patrik Lindström, Skatteverket
Örjan Lundberg, Skatteverket
Annika Follin, Bolagsverket
Joakim Nyström, Bolagsverket
Sara Söderholm, Bolagsverket

Mikael Gråborg, iTeam
Radu Achim, iTeam
Christian Landgren, iTeam
Einar Persson, iTeam
Emma-Klara Wächter, iTeam
Patrik Cardell, Visma
Johan Yman, Visma
Henrik Olsson, PwC
Lars Alm, Fortnox
Stefan Andersson, KPMG
Jens Gullfeldt, Deloitte
Magnus Folkesson, SEB
Magnus Kempe, Kairos Future

Skatteverkets rättsavdelning, ett tiotal personer

**Intervjuer samt inbjudna till workshopar**
Roger Fagerud, DIGG
Stefan Cohen, Findity
Erik Ageberg, Företagarna
David Furlonger, Gartner
Christophe Uzureau, Gartner
Ville Sirviö, Nordic Institute For Interoperability Solutions
Petteri Kivimäki, Nordic Institute For Interoperability Solutions
Johan Schmalholz, Riksbanken
Patrik Andersson, Rise och Mydata
Tage Borg, Scrive
Jan Sjösten, Skatteverket
Conny Svensson, Skatteverket
Sofia Bildstein-Hagberg, Svenskt Näringsliv

# Scenario: ekonomiavdelningen 2030

Här följer ett fiktivt scenario för hur en intervju av medieföretaget *Samhället i stort* med ett par anställda på en ekonomiavdelning skulle kunna se ut år 2030.

Jannicke på *Samhället i stort* publicerar här en spännande intervju med Elof och Amina om hur arbetet på ekonomiavdelningen ser ut idag.

Jannicke: Kan ni berätta lite om hur ert arbete förändrats jämfört med för tio år sedan?

E & A: Idag skickas alla fakturor till en elektronisk adress hos ReReSk AB som sedan fördelar fakturorna vidare till rätt mottagare. Det sparar mycket tid och arbete för oss på ekonomiavdelningen. Eftersom all information är maskinläsbar kan vi automatisera arbetet enormt, det blir också betydligt färre fel. Även betalningarna registreras via en liknande tjänst som är kopplad till Riksbankens e-kronaregister och moms är redan dragen från betalningen vilket minskar oro för skatteskulder, försenade skatteinbetalningar och försvårar bedrägerier med exempelvis moms. Vi känner oss inte lika oroade för ojuste konkurrens, något som var vanligt i vår bransch i slutet av 90-talet.

Jannicke: Kan ni ge ett exempel på hur fusket minskas?

E & A: Vi som företag och våra revisorer behöver inte oroa oss över om uppgifterna i en faktura stämmer överens med motpartens uppgifter, de är alltid lika eftersom tjänsten ReReSk dit fakturorna skickas till och från säkerställer detta. Egentligen jobbar inte våra revisorer som revisorer längre men vi har fortsatt att kalla dem så. De vill egentligen att vi säger rådgivare och att vi ser dem som en del av vårt företags framgång oav-

sett om de är anställda eller ej. Revisionen föreslog de att vi skulle sluta genomföra när lagen ändrades och företag upp till 500 miljoner i omsättning inte längre behövde det. Med modern AI kan riskbedömningen av vilka som ska få skattekontroll ske med enorm träffsäkerhet. För de bolag som inte har många utländska dotterbolag eller filialer utanför EU finns det små möjligheter att missköta sig. Det är mycket bättre än tidigare – brott lönar sig inte. Det är skönt för oss att slippa göra fel i den egna verksamheten också, avprickning av poster och jämförelser mellan konton har vi nästan glömt bort för det är en så liten del av vårt jobb idag. Våra beslutsunderlag är betydligt bättre än tidigare, något som också är nödvändigt när komplexiteten och förändringshastigheten i vår bransch är väldigt hög.

Jannicke: Tar det inte mycket tid att hantera it-system istället?

E & A: Vi använder mycket teknik och det finns säkert många system men det ser vi sällan och det är inget vi tänker på. All rapportering till myndigheter är väldigt enkel idag. Den sker direkt från vårt affärssystem. Vi trycker i princip på en knapp en gång i månaden och så går filen i väg till olika myndigheter i olika format. De myndigheter som vill ha glesare tidsintervall på rapporteringen får det, men det håller systemet reda på. I Sverige vill vi fortfarande att vi aktivt ska skicka uppgifterna men i en del länder i EU hämtas data löpande vid behov. Det gäller till exempel för vårt dotterbolag i Frankrike. Där hämtas uppgifterna via ett API som ger några myndigheter access till den data de har rätt till att hämta.

Jannicke: Hur har arbetsgivare och fack ställt sig till detta?

E & A: I Sverige har det varit en del diskussion kring de anställdas integritet när uppgifter om anställda och deras behörigheter och anställnings-

villkor nu är tillgänglig hos statliga myndigheter. Flera av de system som införts i Sverige med uppgifter om anställda, exempelvis införandet av arbetsgivarinlämning på individnivå, fick en positiv respons när det begav sig. Antagligen var det de erfarenheterna som gjorde att såväl fack som arbetsgivare ställt sig bakom detta, trots allt. Och frågan var kanske om Sverige hade haft särskilt goda förutsättningar att be om särskilda undantag och begränsningar när de flesta andra länder inom EU i första hand såg fördelar med systemet.

Jannicke: Är det lättare för er som lite större företag med 175 anställda att anpassa er till den nya världen?

E & A: Det är inget vi har hört i alla fall. För de minsta företagen är det dessutom redan vanligt att använda den bokförings- och redovisningstjänst som tillhandahålls via molnet av ReReSk. Det har blivit så enkelt att vara företagare idag att många som varit med förr verkligen är positiva till framtiden och ”utvecklingsoptimister”, skulle man kunna säga. Tänk bara på all trasslande kvittohantering som försvunnit till exempel. Nu är de flesta kvitton digitala. De skickas direkt in i bokföringen och papperskvitton fotas bara, betalordernumret kopplas på med en knapp och så läggs det in i bokföringen direkt. Det matchas dessutom automatiskt och vi behöver inte vara oroliga för att samma kvitto finns på två ställen i vår eller någon annans bokföring.

## Är scenariot möjligt? Är det önskvärt?

*”I know this looks like science fiction. It's not.”*

Jeff Bezos lanserar en film på Prime Air 2013, en drönare som levererar ett paket.[2]

Scenariot kanske framstår som science fiction men det finns flera delar i detta som redan finns eller som finns som förslag till lagstiftning i EU och enskilda medlemsländer. Scenariot förenklar arbetet för företag som sköter sig. De som fuskar har däremot svårare att komma undan. Samtidigt är scenariot ovan inte bara en önskedröm, det är också ett hot mot integritet, privatliv, fri företagsamhet och demokrati. Om alla tjänster som exemplifieras ovan införs under statlig kontroll finns det betydande risker. Det finns cyberrisker, risker för korruption och utpressning, risker med resilliens och redundans. Det finns risk att data kommer i orätta händer medvetet eller omedvetet eller säljs till de som önskar köpa den.

**Kan integriteten bevaras?**
Hela Europa har problem med de offentliga finanserna och en utmanande demografi med allt fler äldre. Finns det inga pengar är risken stor att många länder driver på den utveckling vi ser redan idag i alla länder inom EU – dvs. där mer och mer uppgifter samlas in om personer och företag för att säkerställa skatteintäkter och minska brottslighet, även när det finns administrativa kostnader för företagen, rättsprinciper och integritetsfrågor som egentligen borde värderas högre. (Även privata företag och privatpersoner samlar som bekant in mer och mer data.)

Ett sätt att försöka hejda utvecklingen är att ta fram lösningar som ger kontroll och säkrar skatteintäkter, samtidigt som arbetet hos företag och myndigheter underlättas – utan att fullständig data samlas in i centrala

register. Ambitionen med detta projekt är att visa på konkreta lösningar för hur detta kan se ut. Vi menar att det finns lösningar som går att lagstifta om, som är enkla att bygga rent tekniskt, som är förhållandevis billiga och som kan hantera datasäkerhet och integritet tillfredsställande enligt ledande experter i Sverige.

# Utgångspunkten i projektet - förtroende i en digital värld

En central del, kanske rent av kärnan, i projektet är att skapa förtroende för olika former av processer och innehåll. Möjligen kan detta sammanfattas med begreppet "compliance by design".

## Compliance by design

Skatteverket har arbetat med devisen ”det ska vara lätt att göra rätt.” Inom teknik används ibland begreppet ”security by design”. “Compliance by design” kan ses som en variant eller kombination av dessa begrepp. Vem som kom på det vet vi inte men det finns en bok som heter det. I detta sammanhang använder vi tillsvidare en beskrivning av begreppet med tre delar.

**Enkelhet**
Ambitionen är att ta fram lösningar som gör det lätt för medborgare, företag och myndigheter att göra rätt. Det ska samtidigt vara svårt att göra fel.

**Ansvarsutkrävande ”accountability”**
Lösningarna ska göra det lätt att säkerställa ansvarsutkrävande. Såväl medborgare, företag och myndigheter som deras anställda ska kunna ställas till svars för sina felsteg. Det ska vara lätt att identifiera felaktigheter som någon gör. Idag och ännu mer i framtiden kan detta behov även innefatta algoritmer där till exempel Digitaliseringsrättsutredningen SOU 2018:25 föreslagit lagkrav på arkivering av bevis för hur överväganden gjorts av algoritmer.

Lösningarna ska bevara integritet och säkerhet i den mån det är möjligt och önskvärt.

## Blockkedjeinspirerad teknik

Utgångspunkten i projektet var blockkedjeteknik. Den snäva definition som många använder för blockkedjor och distributed ledger har emellertid visat sig svår att realisera i praktisk nytta. I detta projekt har vi istället använt oss av de verktyg och synsätt som blockkedjan synliggjort och kallar detta blockkedjeinspirerad teknik, dvs. verktyg som kan användas för att uppnå ”compliance by design”. Blockkedjeinspirerad teknik är:

”En lösning i alla situationer där en central aktör som samlar in fullständig data kan lösa uppgiften - men där man av något skäl vill undvika det. Skälen kan till exempel vara integritet, manipulation, cyberrisker, tillgänglighet eller likabehandling."

Den relevanta frågan många ställt sig har varit – men vad ska vi egentligen ha blockkedjan till? Frågan när det gäller blockkedjeinspirerad teknik, dvs. den krypteringsteknik blockkedjan består av är närmast den motsatta. Finns det några andra sätt än denna typ av lösning? När vi arbetat med projektet och frågat experter så är svaret i princip ett av tre alternativ. 1. Vi gör redan så 2. Vi känner inte till något annat sätt att lösa det på än det ni föreslår 3. Vi har ingen lösning.

Blockkedjan har beskrivits som ett sätt att ta bort mellanhänder. Det har visat sig både sant och falskt i detta projekt. Alla lösningar vi tittar på i detta projekt är enklare att genomföra om vi lämnar ifrån oss all data till en mellanhand. Två viktiga skillnader finns emellertid.

**Det finns inte alltid en mellanhand idag**

I de flesta fall lämnar vi inte ifrån oss alla data till en mellanhand idag. När det gäller kvitton, fakturor, fullmakter, behörigheter, personalliggare skickas dessa inte in till en central server – varken till ett företag eller till

en myndighet. De lösningar vi föreslår möjliggör ”compliance by design” utan att skicka in fullständig data till en mellanhand. Vi ersätter däremot inte en existerande mellanhand.

**Effektivt ansvarsutkrävande viktigare än att ersätta mellanhänder**
Även i de fall vi har eller vill ha en mellanhand kan blockkedjeinspirerad teknik säkerställa ansvarsutkrävande ”accountability”. På samma sätt som offentlighetsprincipen är tänkt att avhålla offentliga aktörer från misskötsel kan blockkedjeinspirerad teknik göra detsamma med myndigheter, företag och medborgare. En viktig del i detta är att undvika att samla in fullständig data. Data som inte samlas in är svårare att missbruka.

Den rapport som närmast beskriver de frågeställningar som projektet arbetat med är Digitaliseringsrättsutredningen SOU 2018:25. Det är många frågeställningar och problem som identifierats i den utredningen som passar in i projektet. I Digitaliseringsrättsutredningen nämns också växande krav på datasäkerhet. Två exempel är NIS direktivet dvs. Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. Även Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/eg (allmän dataskyddsförordning) i dagligt tal GDPR. Ett ökat dataskydd är svårförenligt med mer omfattande datainsamling i centrala register. Lösningarna i denna rapport kan ses som mer attraktiva med stöd av ökade datasäkerhetskrav. Digitaliseringsrättsutredningen är på 562 sidor och tar naturligtvis upp en mängd frågor som inte detta projekt arbetat med. Det är däremot mycket sannolikt att flera av de problem som beskrivs kan finna stöd i förslagen och tekniken i denna rapport.

## System som möjliggör ansvarsutkrävande

*"When I was a teenager I wished for world peace, but now I yearn for a world in which competing ideologies are kept in balance, systems of accountability keep us all from getting away with too much, and fewer people believe that righteous ends justify violent means."*

Jonathan Haidth, The Righteous Mind: Why Good People are Divided by Politics and Religion.

I dagens samhälle är vi på väg att förstå varandra allt sämre. Pew Research har undersökt utvecklingen i USA under lång tid och beskriver en bild som framstår som likartad i många länder. Pew visar hur demokrater tycker allt mer som demokrater förväntas tycka och republikaner tycker allt mer som republikaner förväntas tycka. Skillnaden mellan åsikterna hos mediandemokraten och medianrepublikanen var relativt liten 1994 och 2004. År 2014 hade den blivit betydande. Oavsett vilka förebilder och auktoriteter vi har blir vi mer lojala med dem vi delar värderingar med och mer blinda för de positiva sidor som personer med andra värderingar har. Istället för att forma våra värderingar utifrån egna erfarenhet och fakta dras fler människor idag till att tycka det som förväntas.

Givet att åsiktsskillnaderna mellan olika personer ökar och misstron mot de som tycker annorlunda blir större behövs nya institutioner. För att hantera en värld där vi ska försöka leva tillsammans och ibland styras av dem vi inte alls delar åsikt med är det viktigt att etablera institutioner som säkerställer att makt inte kan missbrukas.

Många talar idag om att demokratier är på väg att centralisera makt i en utsträckning som gör dessa mer lika diktaturer. En aktör som vill öka sin makt är idag ofta intresserad av att samla in mer data. Data brukar beskrivas som det nya guldet eller den nya oljan. Ambitionen med lösningarna i detta projekt är med andra ord att öka förutsättningarna för förtroende även för personer och institutioner som många människor i övrigt är starkt kritiska till.

# Original och verifikationer i en digital värld

I den analoga världen har det givetvis funnits ett intresse av att säkerställa dokument, deras egenskaper och deras äkthet. Kraven varierar mellan länder men syftar i princip till att minska risken för medvetna och omedvetna fel. Till exempel krav på:

- Skriftlighet
- Pennsort (ej blyerts)
- Uppvisande i original
- Namnteckning
- Egenhändig namnteckning
- Arkivering
- Arkivbeständigt papper
- Bevittning
- Företagsstämpel
- Fingeravtryck
- Sidnumrering
- Ansiktsfoto
- Utgivningsbevis
- Samtidig närvaro och fotografering
- Registrering i ett register
- Meddelande ”denuntiation” t.ex. av vissa panter
- Delgivning

Alla dessa exempel är tänkta att öka sannolikheten att uppgifter, deras avsändare och sammanhang kan säkerställas. Inget av dessa är absolut – det går att förfalska vittnens underskrifter, företagsstämplar kan tillverkas på beställning. Ansikten kan opereras, sminkas med mera, men det är i de flesta fall svårare. I varje samhälle och tidsålder får de som bestämmer avgöra vad som är tillräckligt i en given situation. Nu när digitaliseringen öppnar nya möjligheter för kontroll, förfalskning och misstag behöver samhället anpassa sig.

## Original i en analog värld

Ett viktigt begrepp inom juridiken är original. Det kan till exempel stå i lagtexten att en fullmakt ska visas upp i original, eller att ett kvitto ska kunna uppvisas i original (t.ex. i Bokföringsnämndens allmänna råd). Ett problem som uppstår i den digitala världen är att begreppet original i den analoga värden har flera olika innebörder. Digitaliseringsrättsutredningen SOU 2018:25 har arbetat med frågan och bland annat lyft betydelsen av det uppstått en skillnad i den digitala världen som inte är lika tydlig i den analoga världen. Under rubriken Originalinnehåll och originalexemplar skriver man i betänkandet:

….
Pappersbaserade handlingar kan sägas bestå av tre delar med varsin Urskiljbar funktion vilka tillsammans utgör en helhet:
• Bäraren (papperet),
• Texten (uppgifterna), och
• Utställarangivelsen (t.ex. en underskrift).

Sambandet mellan bärare, text och utställarangivelse framstår i pappersmiljön som så självklar att endast bäraren (papperet) anges, t.ex. en faktura. Även i den elektroniska miljön har man talat om originalinnehåll under förutsättning att ett visst informationsinnehåll t.ex. har skrivskyddats eller försetts med en elektronisk signatur så att det kan återskapas gång på gång utan risk för att det förvanskas. Det har emellertid också hävdats att det inte på traditionellt sätt går att skilja ett originalexemplar från en kopia när data förs över från en databärare till en annan eftersom informationen endast förekommer som ett originalinnehåll. Det förekommer också förarbetsuttalanden där ett elektroniskt original jämställs med en bestyrkt papperskopia.

…

Konsekvenserna av att det inte går att skilja en kopia från ett original är en central del i texten. Tittar vi på exempelvis kvitton och testamenten har det en avgörande betydelse. Ett viktigt skäl till att det inte självklart accepteras en inscannad kopia av ett kvitto eller ett testamente är att det kan skapas kopior som inte går att skilja från originalet. Ett kvitto skulle då lättare kunna finnas som en kostnad i flera företag. Ett testamente kan inte återtas och förstöras eftersom det inte går att veta om det finns kopior som finns kvar.

När det gäller tillämpningen av lagen finns det däremot skillnader mellan testamenten och kvitton. Ett kvitto får sparas om det sparas i original, dvs. det får sparas digitalt om det utfärdades digitalt. Det talas om ursprungligt medium. Ett testamente får däremot inte upprättas digitalt, bland annat av skälet ovan. En fullmakt får däremot som huvudregel upprättas digitalt och signeras digitalt. Ett säkert återkallande av ett testamente betraktas troligen av lagstiftaren som viktigare än ett säkert återkallande av en fullmakt. Det är också ibland väldigt komplicerat att återta en fysisk fullmakt eftersom den kan ha försvunnit och det då krävs offentliggöranden och långa tider för att säkerställa återtagandet.

## Olika egenskaper i den digitala världen

I praktiken kan vi tala om ett antal egenskaper som den analoga världen haft svårt att skilja åt. Åtminstone sex egenskaper som den digitala världen kan skilja åt. Det går att identifiera fler egenskaper men dessa är några av de viktigaste.

- Ursprungsformat (bäraren)
- Ursprungsinnehåll (texten, fotot, data etc.)
- Utfärdare (utställarangivelsen)
- Version
- Innehavare
- Exemplar

När vi talar om dessa egenskaperna så är de i den analogas världen ofta sammankopplade. I ursprungsformatet går det att fastställa det som nämndes tidigare dvs. bäraren, texten och utställarangivelsen. I den digitala världen är det däremot möjligt att låta dessa vara intakta och ändra version, innehavare och tillverka flera exemplar. Huvudregeln i den digitala världen är att all data går att manipulera och att det blir allt lättare att göra det. En anställd som arbetar i en organisation och som har fullständig kontroll över sin data kan manipulera den, liksom en aktör som får eller skaffar sig tillgång till datan. De sätt som hittills visat sig fungera för att säkerställa data är att låta en utomstående aktör delta i säkerställandet av datan. Två huvudtekniker för detta är hashar och privata och publika nycklar som beskrivs i det avslutande teknikavsnittet.

**Ursprungsinnehåll**
I fallet med kvitton ligger det i det företagens och lagstiftarens intressen att ett kvitto inte kan kostnadsföras två gånger. Nuvarande lagstiftnings krav på arkivering av kvitton lägger emellertid fokus på ursprungsformat. Ett digitalt skapat kvitto ska lagras digitalt och ett fysiskt lagrat kvitto ska lagras fysiskt (inte ett foto av ett papperskvitto). En möjlighet är att lagstiftaren gjort bedömningen att digitala kvitton bör tillåtas för att det sparar kostnader, miljö och på sikt underlättar för företagen. Lagstiftaren har därför kompromissat och accepterat risken att ett digitalt kvitto är lättare att kopiera än ett papperskvitto. Ett skäl kan också vara att digitala kvitton ofta lämnas i en i övrigt digital process, t.ex. en identifierbar mottagare eller en kortbetalning, som ökar spårbarhet och minskar risken för fusk.

I dagsläget finns det förslag på att lagstiftaren ska bortse från kravet på att lagra kvitton i ursprungsmediet. I praktiken finns det önskemål om att det ska vara accepterat att fotografera ett papperskvitto och arkivera fotot men slänga papperskvittot. Liknande lagstiftning finns i flera andra länder till exempel Finland och Norge.

I fallet med kvitton är det framför allt angeläget att säkerställa ursprungsinnehåll och existensen av en unik utfärdare. Lösningen som presenteras i denna rapport fokuserar därför på dessa egenskaper.

**Utfärdare**
Avtal kan redan idag signeras digitalt. Detta regleras exempelvis med lagstiftningen kring digital identifiering och underskrifter, EIDAS. I detta projekt är det ingen lösning som beskrivs som bygger på enbart denna form av kontrollmekanism, det finns redan lösningar som fungerar och de accepteras i de flesta fall.

**Version**
I fallet med personalliggare och behörigheter finns det ett ytterligare krav på lösningen. Det finns ett stort värde att veta om det är den aktuella versionen som visas vid en kontroll. Analoga personalliggare har därför ett krav på sig att de ska ha sidnumrering. Tanken är att det ska vara svårare att ändra ordning på bladen och ha flera parallella personalliggare.
Lösningen med digitala kvitton skulle kunna lägga med denna versionshantering till hashregistret – med i det fallet är det inte nödvändigt och därför onödigt att öka komplexiteten och kostnaden med systemet. Kvitton och fakturor är numrerade i sitt ursprungsinnehåll och det är inte nödvändigt att lägga in denna information i hashregistret.
I fallet med personalliggare är det däremot nödvändigt att veta att det är den senaste versionen som visas upp vid en kontroll. Lösningen för personalliggare använder därför ett Merkleträd (som också beskrivs in teknikavsnittet) för att säkerställa att informationen ordnas i en tidsordning.

**Innehav**
Kravet på fullmakter i den analoga världen hårdare än på kvitton. Det är angeläget att veta vem som signerat ett dokument, men också göra det

möjligt att återta fullmakten. Idag tillåter lagstiftningen digitala fullmakter i de flesta fall. Det är alltså inte nödvändigt att göra någon ny lösning. I den lösning som beskrivs i detta projekt finns det däremot en del förbättringar när det gäller möjlighet att återta en fullmakt, visa upp att den är giltig när den används, meddela fullmaktstagaren att den har använts osv. Det skulle vara möjligt att begränsa kvitton och personalliggare med krav på innehav som i fallet med en faktura. Det är däremot mer komplicerat och har därför inte bedömts önskvärt.

# Metod och val av lösningar

Projektets fas två har delvis delats upp i tre delar i huvudsak.

**Arbetet med teknikutveckling** har koordinerats med ett agilt arbetssätt med avstämningar varje vecka och kontinuerligt uppdaterade lanseringar av olika typer av funktionalitet.

**Arbetet med rättsliga frågor** har till stor del skett i dialog med ett tiotal personer på Skatteverkets rättsavdelning med avstämningar tillsammans med bland annat FAR och bokföringsnämnden.

**Arbetet med personalliggare, fullmakter och företagsfakta** har pågått delvis gemensamt och delvis med avstämningar med olika intressenter och experter.

## Verksamhetsnytta teknikval juridik

Projektet tog sin utgångspunkt i en lista på alla tänkbara problem som kunde identifieras av en stor grupp personer som arbetar med redovisning, revision och skatt. Deltagarna fick välja vilka problem och möjligheter som det var mest önskvärt att ta fram lösningar för. De områden där det bedömdes finnas störst verksamhetsnytta valdes att arbeta vidare med. Resultatet var fem områden, varav tre lösningar, som i projektets fas två har blivit sex lösningar. Eftersom urvalet närmast bestod av en önskelista har verksamhetsnyttan delvis tagits för given. Omprioriteringar har också gjorts mot bakgrund av detta. Lösningen med fakturor motiverades med insikten om det stora behovet av lösningar för momsbedrägerier. Lösningar för företagsfakta nedprioriterade mot bakgrund av att det var svårt att identifiera några stora verksamhetsnyttor. (Det enda konkreta exemplet var behovet av enkel tillgång kontroll om ett företag har f-skattsedel). Lösningen som tagits fram fokuserar därför på inlämning av företagsuppgifter till myndigheter.

Projektet har som nämnts arbetat med olika tekniska lösningar inte enbart blockkedjeteknik. Konkreta fördelar av en blockkedjelösning finns endast identifierade och föreslagna i frågan om fullmakter. Alla andra lösningar använder de tekniker som är anpassade efter de verksamhetsbehov som ska fyllas. Den enda begränsningen är att projektet har prioriterat bort lösningar med en central server som samlar in fullständig information.

Projektet fokuserar på lärande och innovation. Detaljkunskap om juridik, processer och teknik har inte varit i fokus, förutom i fallet med digitala kvitton. I de mycket övergripande förslag på teknik, anpassning efter lagar och regler samt nuvarande och framtida processer har vi tagit hänsyn till samhällsnyttan. Krävs det en lagändring är vi medvetna om att det tar tid och försenar lösningen. Det som presenteras är en kvalificerad gissning av vad vi bör göra för att uppnå det värde vi vill uppnå inom rimlig tid. I några fall kan det också byggas tekniska lösningar som kan börja tillämpas redan innan ny lagstiftning är på plats.

Den slutliga tolkningen av lagar och regler kan vi inte veta säkert på förhand. Vi har anlitat expertis inom juridik men det är inga slutliga bedömningar, ställningstaganden eller liknande i rapporten.
För att förstå lösningarna är det givetvis värdefullt med en viss kunskap om juridik, processer och teknik. När det gäller teknik finns en genomgång av de allra viktigaste begreppen/tekniker som används i slutet av rapporten. Är du som läsare bekant med vad en hash, ett Merkleträd och en Certificate Authority (CA) är behöver du antagligen inte läsa denna del.

Nedan följer beskrivningar av lösningarna. Lösningen för kvitton är mest genomarbetad och där finns också teknikpiloten framtagen.

# Digitala fakturor och kvitton

Först kommer här en vidareutveckling av lösningen som fanns i rapporten från det första projektet. Därefter följer ett antal frågeställningar och förslag på hur dessa kan hanteras med fokus på juridik som projektet arbetat med.

## Effektiv och säker hantering av kvitton och fakturor

Den ursprungliga frågan i projektet har varit att effektivt och säkert hantera kvitton och underlätta digitaliseringen av dessa. Under arbetets gång har det blivit tydligt att säkerställandet av fakturor, som också möjliggörs med systemet är av stort intresse. När det gäller det internationella intresset är fakturor den mest angelägna frågan. Detta beror devis på att flera andra länder, exempelvis i norden, redan accepterar digitala foton av papperskvitton och därför inte är lika angelägna om en ny lösning för denna fråga. När det gäller fakturor är det däremot mycket angeläget för alla länder – i synnerhet där olika former av oegentligheter är vanliga.

Eftersom lösningen för såväl kvitton som fakturor får mycket större nytta om fler länder hanterar frågan med samma eller liknande process och arkitektur är det motiverat att förtydliga generaliserbarheten och nyttan med lösningen även för fakturor.

**Vilken nytta och vilket värde kan skapas**

Med en pågående digitalisering har digitala kvitton varit en funktion som många i Sverige efterfrågat. Kassaregisterlagstiftningen gör det möjligt att kassaregistret producerar ett elektroniskt kvitto. Till skillnad mot i många andra länder är det däremot inte tillåtet i Sverige att ta ett foto av ett papperskvitto och arkivera endast fotot.

Även i Sverige har det blivit vanligt att företag tagit ett foto på pappers-kvittot och använda den digitala kopian av kvittot i sin bokföring. Den nuvarande lagstiftningen kräver emellertid samtidigt att en anställd som vill dra av kostnader för utlägg och ett företag som vill dra av kostnader och moms måste spara kvittot i original i bokföringen, dvs. det ursprung-liga filformatet när det gäller digitala filer och pappersformat för pappers-kvitton, vilket försvårat den praktiska hanteringen.

Att registrera och spara papperskvitton kräver stora resurser och försvårar moderna arbetsplatser där många helt eller delvis arbetar på distans eller av andra skäl gör resor och har utlägg från hotell, tåg, taxi, restauranger etc.

En möjlig orsak till att digitala kvitton som är en kopia av ett fysiskt kvitto inte accepteras utan förbehåll är att de kan underlätta bedrägerier och försvåra skatteutredning. Vidare kan digitala kvitton kopieras och ett och samma kvitto kan användas för att göra avdrag och t.ex. få tillbaka moms i flera olika företag. Det är dessutom lättare att förändra ett digitalt kvitto om kvittot tillåts ha vilket format som helst. Det är till exempel lättare att obemärkt lägga till en nolla i en Wordfil än på ett papperskvitto.

Värdet av att skapa en helt digital process för kvitton som underlättar och möjliggör digital lagring och automatiserad kontering skulle spara många miljarder per år om det genomfördes fullt ut i Sverige. Detta projekt syftar till att stimulera och underlätta en utveckling i den riktningen utan att samla in alla kvitton i ett statligt register. För att vägen dit ska vara möjlig och snabb att sätta igång bygger systemet på att papperskvitton tillåts produceras, åtminstone till en början. Såsom det beskrivs i denna rapport finns en rad ytterligare förbättringar som möjliggörs av systemet. Bland annat innebär en liknande process för att säkerställa fakturor fördelar. Fakturorna kan exempelvis säkerställas så att utställare och mottagare har samma uppgifter. Exempelvis personer som arbetar med Nordic Smart Government har visat stort intresse för att säkerställa fakturor.

**En ny lösning är helt nödvändig**
Över tid blir de digitala hjälpmedel som finns för att redigera digitala filer allt mer sofistikerade, mer tillgängliga och billigare i pris. På sikt är det därför troligt att verifikationer som kvitton och fakturor kan manipuleras lika lätt som att redigera Wordfiler. I praktiken äventyrar detta värdet av verifikationer och i förlängningen skatteintäkter och nationalstatens möjlighet att fungera.

Fler och fler länder har redan hamnat i en situation där kontrollen därför behöver skärpas och alltmer utförliga underlag samlas in hos staten. Flera länder som Italien och Brasilien, samlar med andra ord in kopior av samtliga fakturor, Ryssland och Slovenien samlar in samtliga kvitton.

Projektets medverkande har identifierat ett antal utvecklingsspår, bland annat i opublicerat material som visar en utveckling som kan beskrivas som:
- Det samlas in en bredare grupp data och information i allt fler länder i Europa.
- Data samlas in allt oftare och närmare transaktionstillfället.
- Regelverket kring vilken teknik, format och innehåll som ska användas för att samla in data blir allt mer styrt av respektive stat och myndighet.
- Flera länder har planer eller påbörjat försök till beskattning i realtid eller närmare transaktionstillfället.

I praktiken är allt fler länder på väg mot en situation där alla verifikationer, leverantörsreskontran och kundreskontran samlas in parallellt hos staten utöver den bokföring som redan finns hos företagen. Detta kan i förlängningen liknas vid ett statligt koncernredovisning/huvudbok med nationens samtliga företags kostnader och intäkter samt transaktionernas motparter lagras.

Detta alternativ säkerställer beskattningsmöjligheter, men innebär också insamlandet av extremt känslig och närmast fullständig data över allt som köps och säljs inom ett land. Riskerna för cyberattacker, korruption, utpressning, och missbruk av den makt som ligger i denna data är enorm. I kombination med växande förmåga hos maskininlärning och AI kan analyser av den data som samlas in bli mycket kraftfull.

Värdet av att skapa ett system som undviker dessa två ytterligheter, dvs. ett system utan fungerande beskattningsmöjlighet och ett system med oöverblickbar makt och kontroll hos staten, eller den som kan komma över dessa uppgifter, kan knappast överskattas.

Utöver dessa risker finns givetvis möjligheten att privata företag samlar in motsvarande känslig data. Oavsett om detta sker med företag och privatpersoners medgivande eller ej utgör det en samhällsrisk.

**Krav på verifikationer idag**
Det finns idag lagkrav på såväl digitala som fysiska kvitton. Dessa reglerar bland annat tillverkardeklarerade kassaregister och de funktioner som ett kassaregister ska ha. Kassaregisterlagstiftningen tillåter att det tillverkardeklarerade kassaregistret tar fram ett digitalt kvitto. Lagstiftningen ställer emellertid krav på att kvittos ska ges ut till köparen. Det digitala kvittot måste med andra ord ges ut och tas emot i någon form. Eftersom något system eller standard för att ge ut digitala kvitton för butikerna och ta emot digitala kvitton hos konsumenterna inte har etablerats har butikerna valt att fortsätta med papperskvitton i stor utsträckning.
Tyvärr har införandet av digitala kvitton av den anledningen dragit ut på tiden i handeln och bland företagen. Det finns emellertid företag som påbörjat utgivning av digitala kvitton och det finns en standard framtagen i ett arbete som organiserats av it- och telekomföretagen.[3]

**Lösningen har många tillämpningar**
Diskussionen inom projektet kring digitala kvitton har rört en rad olika områden såsom ”svarta lådor” för kontantkassor, automatkonteringar i bokföringen, realtidsredovisning, fakturor osv. I slutändan har den lösning som föreslås i denna rapport en möjlighet att underlätta för de flesta av dessa frågeställningar. Utgångspunkten för att detta ska vara möjligt är att kvitton inte bara är digitala utan att de också är formatoberoende, dvs. det är den digitala informationen som är central och inte formatet, m.a.o. om det är en Pdf eller liknande. När det gäller fakturor regleras formatet bland annat av lagen (2018:1277) om elektroniska fakturor till följd av offentlig upphandling/ direktiv 2014/55/eu om elektronisk fakturering vid offentlig upphandling. Med elektroniska fakturor avses i den lagen/det direktivet fakturor som utfärdas, översänds och tas emot i ett strukturerat elektroniskt format som gör det möjligt att behandla dem automatiskt och elektroniskt. Standarden kallas PEPPOL.

Lösningen utgörs av en säker faktura- och kvittohantering och bygger på två viktiga insikter.

1. Ett kvitto eller en faktura har i sig ett begränsat värde. Det är ingen större fara om någon stjäl ett digitalt kvitto. Det är till exempel redan idag ofta möjligt att få en kopia på gamla kvitton från försäljningsstället.

2. Skatteverket och andra intressenter är framförallt intresserade av om ett kvitto redan har kostnadsförts och därmed påverkat redovisningen sedan tidigare i samma eller något annat företag. Även företag vill gärna veta om ett kvitto redan använts för ersättning till en anställd i en reseräkning, eller av ett annat bolag. Skatteverket m fl är givetvis även intresserade av att kvitton inte är felaktiga, falska, att de har koppling till verksamheten, att uppgifterna stämmer osv.

När det gäller fakturor är risken för dubbelavdrag mindre eftersom en faktura specificerar en mottagare.

Den största nyttan med ett digitalt kvitto ligger sannolikt i att minska företagens och de anställdas administration och arbete med att redovisa och överföra papperskvittot till digital form samtidigt som papperskvittot ska arkiveras. Eftersom en helt digital lösning även underlättar maskinläsbarhet och digitaliserade processer, exempelvis automatkonteringar i bokföringen, i högre utsträckning kan betydande arbetsinsatser sparas.

En fullt ut digital hantering av kvitton, som dessutom underlättar automatkontering bedöms generera ett värde i Sverige på mer än tio miljarder per år i Sverige. Uppskattningar av denna karaktär är givetvis svåra men med hänsyn till storleken på redovisningsmarknadens storlek, antalet personer som arbetar på ekonomiavdelningar med att registrera och säkerställa dessa uppgifter, antalet personer i arbetskraften totalt som berörs av

kravet på arkivering av utlägg i arbetet och det mycket stora intresset från arbetsgivarorganisationerna att lösa denna fråga är det projektets bedömning. Det bör noteras att detta innefattar automatkontering, inte enbart digital lagring. Som jämförelse bedömer Lantmäteriet värdet av digitaliserad geodata i Sverige till 22,5-42,5 miljarder per år.[4]

Den beskrivna lösningen kan vara central för att uppnå detta. Ett internationellt samarbete är inte nödvändigt för ett enskilt land att få nytta av systemet med den beskrivna lösningen.

**En mjukvara/tjänst och arkitektur för digital kvittohantering/fakturahantering**
Följande situationer är lösningen tänkt att hantera:

- Möjliggöra digital lagring av samtliga kvitton oavsett i vilket format de ges ut.

- Minska risken för misstag och bedrägerier med manipulerade fakturor och kvitton och kvitton som kostnadsförs flera gånger.

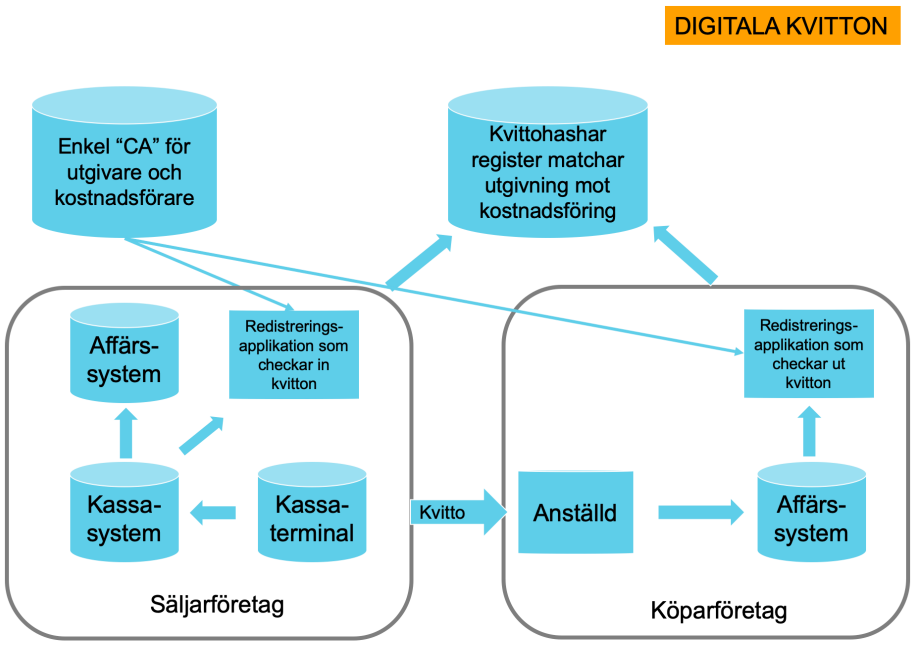
- Snabba på införandet av digitala kvitton och fakturor.

- Underlätta för digitala transaktioner och händelsedata och möjliggöra realtidsrapportering och automatkonteringar i bokföringen.

- Förhoppningsvis ersätta kassaregisterkrav på ”svarta lådor”.

## Process kvitton

**Övergripande arkitektur**
Denna arkitektur är en övergripande arkitektur med fokus på kvitton som ges ut från ett kassaregister. För fakturor och distansförsäljning utan kassaregister är bilden inte riktigt representativ, men snarlik.




**Process**
I enlighet med vad som står i avgränsningen är åsikterna som beskrivs i rapporten inte något som någon person eller organisation tar ansvar för. Såväl Id-hantering (CA) som verifikationshashregister i denna lösning kan ligga hos Skatteverket eller en annan myndighet. Oberoende av var lösningen ligger är det tänkt att vara en rent teknisk administration, dvs. det finns ingen skatteutredning eller annan myndighetsutredning av innehållet i verifikationshashregistret. Inga slagningar mot registret behöver göras för att kontrollera verifikationerna som, liksom idag, lagras i affärssystemen och kassaregistersystemen.

Hypotesen är att verifikationshashregistret bör vara myndighetsägt medan CA gärna kan vara privata aktörer. I detta specifika fall har Skatteverket varit särskilt angelägna om att betona att det inte är ett ställningstagande från myndigheten att man önskar samla in information eller önskar ytterligare handläggning av information in ett nytt register. Lösningen är designad för att detta inte ska behöva ske. Kärnan i lösningen är att samla in så lite data som möjligt, utöver dagens lagstadgade krav, men fortfarande säkerställa riktigheten i verifikationerna.

**Förberedelser för att registrera sig i systemet:**
För att vara godkänd som utgivare av kvitton/fakturor, respektive kostnadsförare av kvitton/fakturor behöver företagen registrera sig hos ett certificate authority, CA. Dennes uppgift är att se till att hashar som registreras har en godkänd avsändare. På så sätt undvikes att registret fylls med spam. Alla uppgifter har en avsändare men det innehåll som registreras är oläsbart och ytterst begränsat, dvs. en hash. Avsändaren kan också vara anonymiserad för hashregistret och alla andra enligt nedan. Ett CA måste ha tillgång till alla avsändare och deras samlade idn däremot har CA inte tillgång till hashregistret eller kunskap om förekomsten av eventuella låtsashashar.

**Steg 1 transaktion**
Säljaren tar emot en betalning och ger ut ett kvitto. Formatet på kvittot kan tillåtas vara valfritt. Målet är givetvis att alla kvitton ska bli helt digitala, men för att systemet ska gå att implementera snabbare behöver befintliga lösningar vara juridiskt giltiga åtminstone under en övergångsperiod. Ett skäl till detta är likabehandlingsprincipen (jfr 1 kap. 9 § Regeringsformen och 5 § förvaltningslagen). Köpare som inte har möjlighet att ta emot kvitto i digital form ska kunna få ett papperskvitto som idag, då kvitto, oavsett vilken form det är i, ska tas fram och erbjudas kunden vid kontant försäljning (se 39 kap. 7 § Skatteförfarandelagen, sfl).

**Steg 2 registrering av kvittot i kassaregistersystemet hos utgivaren**
Det säljande företaget hämtar data om det utgivna kvittots innehåll från kassaterminalen/datorn. Innehållet består av två delar dels ett unikt ID som finns kopplat till varje kvitto och dels uppgifter om transaktionen dvs. datum, tid, belopp, moms, artiklar som köpts. All denna information regleras redan idag i lag. Ingen ytterligare information krävs. Ingen förändring av kassaterminalerna som används idag är därför nödvändig.

**Steg 3 registrering av kvittohash hos verifikationshashregistret**
Den inhämtade informationen hos kvittot som beskrivs ovan krypteras till en hash. Till hashen läggs också en publik nyckel eller liknande kod som företaget registrerat hos en part liknande en certificate authority, CA, dvs. någon som kopplar ihop koden och företaget. Eftersom kvitton har ett lågt värde kan hanteringen av dessa nycklar hålla en lämplig och kostnadseffektiv lägre nivå och företag som vill registrera kvitton kan använda stora mängder nycklar om de vill. Verifikationshashregistret har nu en hash av ett kvitto och en kod som en annan databas (ca för kvitton) kan knyta till ett företag (d.v.s. det företag som registrerat kvittot). Observera att själva originalinformationen inte finns hos verifikationshashregistret. Originalinformationen ligger enbart där den ligger i den befintliga processen, dvs. i kassaregistersystemet.

**Steg 4 utläggsregistrering av kvittot**
Den anställde som haft ett utlägg, t.ex. en taxiresa, registrerar sitt kvitto och ger in det till sin arbetsgivare. Är kvittot digitalt kan det läsas av en programvara som kan läsa digitala filer eller också är kvittot maskinläsbart. Är kvittot fysiskt behöver den anställde ta ett kvitto med en app som kan scanna informationen och göra den maskinläsbar. Arbetsgivaren, eller den anställde, registrerar informationen i affärssystemet med en eventuell förkontering inför attest. Eftersom det med den tänkta lagstiftningen inte behövs något fysiskt kvitto kan kvittot sparas digitalt även om det givits ut i pappersform. Registrering och kontering kan också lättare utföras automatiskt av ett system eller någon på en ekonomiavdelning eller redovisningsbyrå. Automatkonteringen underlättas om kvittot ges ut i ett digitalt maskinläsbart format. Krävs attest av utlägget hanteras det som idag i affärssystemet.

**Steg 5 registrering av kvittot som kostnadsfört hos kvittoregistratorn**
Den inhämtade informationen hos kvittot som beskrivs ovan krypteras till en hash. Eftersom kvittots innehåll är detsamma som det som registreras av kassaregistrets ägare kommer hashen att vara likadan. Till hashen läggs också en publik nyckel eller kod kopplad till det kostnadsförande företaget på motsvarande sätt. Hashen får på så sätt en avsändare.

**Steg 6 kvittoregistratorn matchar utgivarensoch kostnadsförarens hash**
Kvittoregistratorn har nu en hash av ett kvitto och en publik nyckel för det utgivande företaget. Denna hash kan sedan markeras som ”använd” när ett kostnadsförande företag registrerar samma hash. Kvittoregistratorn vet inte något om innehållet men kan validera att samma kvitto blivit utgivet och kostnadsfört.

**Steg 7 återrapportering av godkända verifikationer**
När verifikationshashregistratorn identifierat en matchning mellan en utgiven hash och en kostnadsförd hash signerar verifikationshashregistratorn denna och skickar tillbaka denna signarade verifikation till såväl utgivare som kostnadsförare. Ett förslag är att de signerade verifikationerna skickas CA en gång om dagen tillbaka till utfärdare och kostnadsförare. Fördelen med detta är att verifikationerna kan kontrolleras av revisorer och vid skatteutredning enbart med den data som ligger i affärssystemet, respektive kassaregistersystemet.

**Steg 8 revision och skatteutredning**
På samma sätt som idag görs revision och skatteutredning av de verifikationer som ligger i affärssystemet hos kostnadsföraren och kassasystemet hos utfärdaren. Varken revisorer eller skatteutredare behöver göra slagningar i verifikationshashregistret. Skillnaden gentemot idag är att verifikationerna (dvds kvittona men vilka även kan vara fakturor enligt

samma system) kan kontrolleras med betydligt högre grad av säkerhet. Verifikationerna måste motsvaras av en motpart med samma information. Det enda revisorerna och skatteutredarna behöver är en publik nyckel som verifikationshashregistret kan ha publicerat på sin hemsida och som visar hur verifikationerna ska vara signerade för att vara godkända.

**Steg 9 felregistreringar**
För det fall en hash inte matchas av någon kostnadsförare kommer även detta återrapporteras till utfärdaren. När en privatperson är köpare är detta inget ovanligt. Ska det däremot finnas en kostnadsförare uppstår ett antal möjligheter där det till en början inte behöver vara obligatoriskt att kostnadsföra i hashregistret. Blir detta ett lagkrav uppstår möjligheter att minska exempelvis momsbedrägerier och bluffakturor. Blir en hash registrerad av en kostnadsförare och denna inte registreras av en utgivare blir verifikationen inte godkänd och därmed inte signerad av verifikationshashregistret. Kostnadsföraren får därmed höra av sig till utgivaren och felsöka. På sikt kan kassaterminaler och fakturor skicka med den framräknade hashen för att undvika en felkälla.

## Process fakturor

Processen för fakturor är i grunden likartad. I fallet med fakturor finns det emellertid oftast ingen mellanhand i forma av en anställd som tar emot verifikationen. Fakturor skickas direkt till ett företag eller en särskild fakturamottagare. Eftersom fakturor har en specificerad mottagare är det också ett mindre problem med dubbelavdrag – men det förekommer också.

Ett större problem när det gäller fakturor är momsbedrägerier. Det stora problemet med momsbedrägerier ligger inte i att det är problem med dubbelavdrag utan att ett säljarled (så kallade missing traders/skenbolag) inte betalar in sin utgående moms avseende en utställd faktura, det kallas

även momskarusell. Såvida inte köparen i nästa led kände till eller borde ha känt till att transaktionen ingick i ett momsbedrägeri så kan inte denne nekas att göra avdrag för den ingående momsen (köparen är i god tro vad gäller sitt inköp) enligt nuvarande momslagstiftning.

*MTIC/carousel fraud is the most damaging type of cross-border VAT fraud (eur 50 billion losses in average per year). Whilst the 'definitive system' proposal (2017) is meant to put an end to it, its entry into application is not envisaged before 2022. Therefore, it is essential that the Member States take immediate actions to control the damage. This can be done within existing frameworks, in particular Eurofisc and the newly created European Public Prosecutor Office. " Page 8 ("VAT fraud, Economic impact, challenges and policy issues", EP 2018 )*

För att komma åt den problematiken behövs ett antal justeringar i tekniken och lagstiftningen. Projektgruppen är inte enig i huruvida det kommer att vara möjligt att minska denna typ av bedrägeri. Givet de stora belopp som frågan berör är det något som är värt att undersöka vidare.

## Juridik och viktiga frågor fakturor och kvitton

**Uppdrag och mandat för verifikationshashregister**
Det centrala i arkitekturen är att det skapas en gemensam liggare för registreringen av de krypterade verifikationerna av kvittona. Om den gemensamma liggaren samlar in fullständig data, dvs. själva kvittona i sin helhet, blir databasen sammantaget oerhört stor och en betydande säkerhetsrisk. Idag finns det ett flertal länder, även i Europa, som är på väg i denna riktning, dvs. att skapa fullständiga databaser med försäljnings- och leveransdata. I den föreslagna lösningen är det däremot möjligt att lämna ifrån sig data utan att denna kan återskapas, eftersom data är reducerad till

ett minimum i form av kryptering som hashar. Även om en kypteringsnyckel avslöjas kan datan inte återskapas eftersom den är reducerad och aldrig skickas i sin helhet. Detta förfarande skiljer sig från en molnlösningen där datan är krypterad men skickas i sin helhet.

Projektet har tillsvidare gjort bedömningen att en svensk myndighet bör vara ägare till den gemensamma liggaren eftersom det inte kan finnas okända liggare. Det går att lagra dessa som en blockkedja men det är sannolikt enklast om Skatteverket, DIGG, Bolagsverket eller annan myndighet är ägare av liggaren eller i vart fall har lagstyrd tillgång till liggaren i ett fastställt format.

Om uppdraget att hålla en registratur för verifikationshashregistret ska ligga på en myndighet krävs det att myndigheten har ett författningsreglerat uppdrag för detta. Kravet på författningsreglering hänger samman med legalitetsprincipen såsom den kommer till uttryck i 1 kap. 1 § Tredje stycket regeringsformen och 5 § förvaltningslagen. Uppdraget som sådant kan troligen regleras i myndighetens instruktion, jmf förordning (2017:154) med instruktion för Skatteverket.

Utöver uppdraget i myndighetens instruktion ska arbetsuppgiften att hålla registraturen och att utföra de arbetsuppgifter som följer därav regleras i en särskild författning. Eventuellt kan viss ledning hämtas från t.ex. Författningar kring registrering av verkliga huvudmän, lag om (2017:631) resp. Förordning om 2017:667). I den särskilda regleringen ska funktionerna i registraturen behandlas, åtkomstmöjligheter beskrivas, ev. beslutsfattande, möjligheter till överklaganden samt registerförande myndighets mandat att lämna föreskrifter. Myndighetens föreskriftsrätt skulle kunna handla om giltiga format, vilken eller vilka CA-lösningar som är giltiga m.m.

**Åtkomst och tjänster**
Tjänsten är i första hand tänkt att ta emot registreringar av utgivna kvitton och fakturor samt registreringar av kostnadsföringar. Utöver registreringar är det tänkt att bekräftelser på att dessa registreringar är genomförda och korrekta skickas tillbaka till respektive utfärdare och kostnadsförare. Denna process kan vara helt automatiserad och autonom – dvs. helt styrd av tekniska regler och den ska inte kräva någon form av handläggning.

Det finns emellertid möjligheter att använda ytterligare funktionalitet. Två exempel kan vara att undvika försäkringsbedrägerier samt bluffakturor.

**Bluffakturor**
Om en utgivare av fakturor i har något forma av bedräglig verksamhet, till exempel skickar bluffakturor i stora mängder kan kostnadsföreraren få en varning om detta. Verifikationshashregistret kan när bekräftelsen av den korrekt registrerade fakturan göra en notifiering efter en given regel. Regeln kan exempelvis vara att om en utgivare av fakturor har mindre än 50% av dessa kostnadsförda hos en motpart får kostnadsföraren ett meddelande. Meddelandet kan bestå av ett automatiskt meddelande om att det finns skäl att vara extra uppmärksam på denna fakturas riktighet.

**Kostnadsförda kvitton**
En hemförsäkring kan exempelvis användas för att få en vara lagad eller ersatt enligt bättre villkor än en vara som köps av ett företag. Ett försäkringsbolag kan därför vilja säkerställa att ett kvitto inte nyttjats av ett företag innan ersättning för en vara betalas ut på en hemförsäkring. En förfrågan kan därför skickas till verifikationshashregistret för att kontrollera om en given hash finns kostnadsförd. Verifikationshashregisteret kan dela med sig av uppgiften om kvittot är registrerat som en kostnad i ett företag utan att avslöja vare sig utgivare eller kostnadsförerare.

Lagstiftaren behöver med andra ord ta ställning till i vilken utsträckning verifikationshashregistert kan medge åtkomst för exemplet ovan eller andra syften och erbjuda andra tjänster än grundfunktionen.

**Tvister och överklaganden**
För det fall ett företag vill kostnadsföra ett kvitto som redan finns registrerat som en kostnad hos ett annat företag kan det uppstå en möjlighet att detta ska kunna överklagas/ifrågasättas. Vilken process som är bäst lämpad för att hantera detta kan diskuteras.

Finns det ett bevis på betalning, t.ex. en korttransaktion, är en möjlighet att köparen av en vara då ber kvittoutgivaren att avregistrera det föregående kvittot så att den föregående kostnadsförarens verifikation ogiltigförklaras. Eftersom de signerade verifikationerna skickas ut som en nummerserie kan kostnadsföraren inte undvika att lagra denna korrigering utan att det kan upptäckas vid revision.

Finns det inget bevis på betalning kan det bli svårt för den som önskar kostnadsföra ett redan använt kvitto att motivera att få ut ett kvitto. Det bästa är sannolikt om denna bevisning av vem som är den rättmätige köparen kan regleras mellan parterna dvs. säljaren och köparen. Parterna får bevisa sin rätt inför varandra och det kommer rimligen att vara sällsynt att vilja driva denna fråga för kvitton. För det fall det vid skatteutredning upptäcks att ett företag kostnadsfört ett kvitto som är incheckat av någon annan i hashregistret så kan företaget förklara för Skatteverket att det är det som har rätt till avdraget, dvs. göra sannolikt.

För en faktura kan detta däremot inte ske eftersom en faktura specificerar en mottagare.

De lagkrav som finns på möjligheter att pröva frågor kring personuppgifter kommer givetvis att finnas. Detta gäller såväl myndigheten som ansvarar för hashregistret och det gäller detta privata aktörer som agerar ca. Saklig grund kommer att finnas och hanteringen kan troligen främst lösas mellan den utfärdare av fakturor/kvitton och den kostnadsförare av fakturor/kvitton och deras ca. Beträffande verifikationshashregistret är det ett myndighetskontrollerat register med lagstöd varför överklaganden bör bli ovanliga.

**Kreditfakturor**
När det gäller fakturor är det vanligt att det blir fel av något slag. Det fakturerade företaget vill ibland ha en kreditfaktura. Systemet med verifikationshashregistret behöver därför kunna hantera dessa fel. Det vanligaste är att fakturamottagaren ifrågasätter fakturan innan den kostnadsförs. Den kommer med andra ord aldrig att registreras i verifikationshashregistret som kostnadsförd, bara som utgiven. Verifikationshashregistret kommer därför aldrig att skicka någon signerad bekräftelse på att det finns en motpart som godtagit fakturan till utgivaren.

Skickas en kreditfaktura behöver det troligen inte registreras i verifikationshashregistret. Ska en kostnadsförd faktura krediteras är det lämpligt att kreditfakturan också registreras i hashregistret av såväl utfärdare som mottagare.

**Personuppgiftsbehandling**
För att registreringarna inte ska vara helt oidentifierbara behövs dessutom unika avsändare av hasharna. Det behövs därför ett system som registre-

rar användarna och kan koppla dessa till respektive företag. De kommer därför att behövas privata och publika nyckar eller företagsspecifika koder för detta (eller något annat digitalt identifieringssystem.) Dessa koder kommer sannolikt att betraktas som personuppgifter.

Det måste finnas en analys som visar om systemet kring digitala kvitton resp. registraturen av digitala kvitton innebär någon personuppgiftsbehandling. Personuppgiftsbehandlingen kan avse såväl utställare av kvitton såväl som mottagare eller andra. Om det förekommer någon personuppgiftsbehandling ska den beskrivas. En ev. personuppgiftsbehandling måste ha en rättslig grund, jmf. art. 6 EU:s dataskyddsförordning och det finns antal principer för personuppgiftsbehandlingar som måste beaktas bl.a. uppgiftsminimering och relevans, jmf. art. 5 i samma förordning. Även tidsaspekten på lagring av personuppgifter omfattas av art. 5.

Om det kan förekomma personuppgiftsbehandling inom registraturen, antingen i registret eller i den omgivande handläggningen av uppgifter som finns i registret, ska det finnas en analys av personuppgiftsansvaret och vem eller vilka som bör anses som personuppgiftsansvariga.

Den personuppgiftsansvarige måste också säkerställa lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, (artikel 5.1 f EU:s dataskyddsförordning). En analys av vilka skyddsåtgärder som måste vidtas för uppgifterna i verifikationshashregistret samt omkringliggande handläggning behöver redovisas.

**Sekretess och anonymisering**
Uppgifter i en registratur som hålls av en myndighet kommer att vara en allmän handling. Allmänna handlingar är som utgångspunkt tillgängliga för alla och envar, jmf. andra kapitlet tryckfrihetsförordningen. Behovet av sekretess för uppgifter i registraturen och i ev. sidoordnade system, t.ex. identitetsuppgifter hos ca, behöver utredas och beskrivas. Här bör man också betänka att data som avser försäljnings- resp. inköpsnivåer, motparter m.m. kan vara skyddsvärda.

I den föreslagna lösningen kommer det inte att finnas möjlighet att återskapa försäljnings- och inköpsnivåer eftersom denna data inte registreras eller lagras på något annat ställe än idag, dvs. hos utgivaren och kostnadsföraren. Det finns däremot en möjlighet att komma åt uppgifter om antal verifikationer – vilket kan ge en indikation om försäljningsvolym samt uppgifter om motparter. Bedömningen i projektet är att denna data därför bör betraktas som skyddsvärd och åtkomst för allmänheten ej medges, på samma sätt som momsdeklarationer eller liknande uppgifter som rapporteras till SCB.

Ambitionen är att minimera hanteringen av personuppgifterna i hash-registratorn samt att anonymisera dessa. Det är tekniskt möjligt att göra transaktionerna helt anonyma, exempelvis med nya krypteringsnycklar för varje transaktion. Det är emellertid ett kostsamt och krångligt system och förslaget är därför att anonymisera data i hög utsträckning och begränsa åtkomst och handläggning av uppgifterna i verifikationshashregistret för att uppnå en lösning som sammantaget är kostnadseffektiv, säker och rimligt enkel att implementera.

**Anonymisering**

Frågan om sekretess och anonymisering av personuppgifter är kärnan i den föreslagna lösningen. Till skillnad mot den rådande utvecklingen på området syftar lösningen till att säkerställa verifikationerna med stöd av minst möjliga mängd data och största möjliga skydd av personuppgifter. Ett antal förslag för att ytterligare anonymisera data finns nedan.

1. Företagen kan välja att ha många nycklar och dessa kan dessutom eventuellt lagras hos flera olika ca. Detta försvårar en bedömning av helhetsbilden av det totala antalet kvitton och fakturor som ges ut eller kostnadsförs av ett företag.

2. Företagen kan dessutom skickas in extra transaktioner för att dölja mängden kvitton som registreras. Det vill säga, en utgivare registrerar låtsas-hashar som tillsammans med de korrekta hasharna ger ett jämnt flöde av registreringar vilket försvårar trafikanalys och bedömningar av försäljningsnivåer.

3. Verifikationshashregistratorn kan signera bekräftade transaktioner och skicka tillbaka dessa till kostnadsföraren och till utgivaren. Detta medför att ingen handläggning, revision eller kontroll av själva verifikationshashregistret behöver göras av själva innehållet utan begränsas till teknisk drift av systemet. Inga handläggare får tillgång till känsliga uppgifter.

4. Kortidslagring av data. För att begränsa riskerna med insamlad data kan data i verifikationshashregistret slängas efter en kort tid. Eftersom såväl utgivare lagrar verifierade transaktioner i en obruten serie kan data inte tappas bort utan att riskera en påföljd. Eventuellt kan data slängas med uppgifter om mottagare av en faktura eller kostnadsförare av ett kvitto. På så sätt kan riskerna med den känsliga kopplingen mellan köpare och säljare minska avsevärt utan att möjligheterna till kontroll av utgivningen förstörs.

5. Identifiering och ca. Det är en fördel om Id-hanteringen hanteras separat eftersom det försvårar analys av databasen och eventuella kopplingar till data. Id-hanteringen kan med andra ord skötas av andra aktörer.

Det system som nu är framtaget i den tekniska piloten på www.digitala-kvitton.se samt på Github https://github.com/iTeam1337/digital-receipts Den lösning som där är framtagen möjliggör anonymisering, privata CA och låtsashashar. Den lagreglering som privata CA behöver för att kunna tillhandahålla lösningen i dess nuvarande form behöver utredas vidare. Det är i alla fall mer eller mindre säkerställt att detta går att lösa rent tekniskt.

Det finns en rad olika sätt att ytterligare dölja information, men man ska vara medveten om att detta är enormt mycket säkrare system än vad som etablerats i andra länder. Verifikationshashregistret innehåller mindre komplett och mindre värdefull försäljningsdata än vad många andra länder, inklusive Sverige, Norge och EU är på väg att bygga upp på annat håll.

**Utgivningen**
Kassaregisterkravet är reglerat i skatteförfarandelagen (39 kap. 4-10 §§ och 42 kap. SFL) och skatteförfarandeförordningen (9 kap. 2-4 §§ SFF). Skatteverket har också utgett föreskrifter om bl.a. krav på kassaregister, kontrollenhet och användning av kassaregister (SKVFS 2014:9, SKVFS 2016:1 respektive SKVFS 2014:10).

Vilka ändringar behövs i kassaregisterlagen eller annan lag som reglerar utgivningen och arkivering av kvitton för säljaren? Man kan tänka sig att det blir övergångsregler i flera steg vid ett införande av detta system med ett hashregister. Till att börja med tillkommer sannolikt bara en möjlighet att registrera hashen krävas, för det fall ett företag vill arkivera ett digitalt innehåll i ett annat format än det ursprungliga (företaget vill till exempel spara maskinläsbar data i stället för en Pdf eller ett papperskvitto). I ett andra steg kan en lag finnas som reglerar att en utgivare av kvitton åläggs att registrera hashen om köparen begär det. I ett tredje steg blir det obligatoriskt att registrera alla verifikationer i hashregistret. När det gäller fakturor kan det vara möjligt att hashregistret har starkt stöd internationellt och bland intressenter i Sverige. Det kan därför införas parallellt och även före ett införande av systemet för kvitton.

Förutom att utgivaren av kvitton har ett kassaregistersystem som lagrar den fullständiga kvittoinformationen från kassaterminalerna kan kassaregistersystemet även lagra hashen. Vad som är nödvändigt är att utgivaren lagrar de signerade hasharna av verifikationerna som kommer i retur från verifikationshashregistret. Detta är nödvändigt för att utgivaren inte okontrollerat ska registrera hashar som kan nyttjas av kostnadsförare. Detta förfarande möjliggör också att arkiveringen av hasharna i verifika-

tionshashregistret blir mindre angelägna. Data kan därför slängas tidigare eftersom fullgoda, signerade verifikationer finns arkiverade hos utgivaren. Det behövs därför regleras vilka krav som ställs på lagring av de signerade verifikationerna. Det är emellertid mycket likt det krav som ställs idag i bokföringslagen, dvs. ett krav på att lagra verifikationerna.

Det bör undersökas om det går att stödja företag som vill registrera samtliga hashar för sina kvitton och/eller fakturor. Det är ett antagande att nuvarande kassaregisterlag och krav på utgivning av kvitton i första hand syftar till att säkerställa att skatter betalas enligt lag, dvs. lagstiftaren vill försvåra möjligheten till försäljning sker utan registrering av verifikationer och inbetalning av moms, bolagsskatt osv. Ett ökat krav på lagring av signerade verifikationer borde möjliggöra undantag från kassaregisterlagens krav och kraven på utgivning, givet att systemet fortsatt kan säkerställa skatteintäkter i åtminstone samma utsträckning som idag.

Ett förslag som arbetats fram i den tekniska piloten i projektet är att utgivningen av kvittot/fakturan även innehåller den framräknade hashen. Det underlättar för det kostnadsförande företaget som kan räkna fram hashen och därmed se att den överensstämmer med den som kom från utgivaren. På så sätt slipper man registrera felaktiga hashar, man vet på förhand om man fått fram rätt hash. Får man inte fram den korrekta hashen kan man vända sig till utgivaren på en gång. Denna finess kan eventuellt hanteras utan att den regleras i lag. Förhoppningsvis kommer kostnadsförande företag att förmå sina anställda att välja att göra inköp från utgivare som har en enkel och säker process.

**Anonymisering av kvitton**
I dagsläget är kvitton anonyma, dvs. köparen behöver inte identifiera sig. Eftersom ett stort antal transaktioner idag sker med kortbetalningar, finns en möjlighet till identifiering om kortet är knutet till en identitet, exempelvis ett kundkort hos en butikskedja, men det är fullt möjligt att vara i huvudsak anonym.

För digitala kvitton finns det liksom för papperskvitton ett krav på utgivning. I praktiken innebär detta att en registrering av köparen/konsumenten/arbetstagaren behöver göras i en app eller att denne anger en mailadress dit kvittot skickas. På detta sätt blir det svårare att vara anonym. Det bör undersökas om möjligheten att vara anonym är värd att bevara och kan förbättras. Motsvarande frågan brukar också tas upp i samband med en oro för att kontanter är på väg att försvinna som betalningsmedel, inte minst i Sverige. Frågan om anonyma betalningar och anonyma kvitton hänger därför samman.
Givet att en hash registreras i verifikationshashregistratorn kan man fråga sig om detta fyller samma funktion för att säkra skatteintäkter? Detta bör utredas. Ett alternativ kan också vara att ett kvitto kan publiceras på en terminal och att kvittot kan läsas med en mobiltelefon, t.ex. genom avläsning av en qr-kod. Det skulle möjliggöra anonymisering eftersom kassaterminalen inte behöver få kunskap om en adress till mottagaren.

När det gäller fakturor finns inte möjligheten till anonymisering. Fakturan specificerar mottagaren. Det är därför svårare att kostnadsföra en faktura flera gånger. I synnerhet är det svårt att kostnadsföra samma faktura i flera bolag – det kräver manipulation. Ett kvitto som har en identifierad mottagare eller betalare är därför att föredra om syftet är att minska fusk, men det gör anonymisering svårare.

**Utläggsredovisningen**
De reaktioner som kommit på systemet är så gott som odelat positiva. Den främsta invändningen är hanteringen av internationella kvitton. Ska det införas olika lagstiftning för lagring av svenska och utländska kvitton? Svenskt Näringsliv har exempelvis gjort en hemställan om möjliggörandet av foton av papperskvitton i Sverige, dvs. att överföring till annat medium ska tillåtas från dag ett. Det är naturligt att företagen vill ha en lagstift-

ning som inte försvårar för svenska företag, i synnerhet inte i relation till andra länder. En konkurrensneutral lagstiftning är önskvärd. Ytterligare skäl att tillåta foton av papperskvitton är att varken Skatteverket eller revisorer kontrollerar pappersoriginal, i de fall det finns foton av dessa. Det finns även företag som struntar i lagstiftningen och har slutat lagra papperskvitton, trots att lagen kräver det.

Ett argument som istället talar för lösningen med ett hashregister är att det stimulerar till ett fokus på informationen i kvittot snarare än mediet. Stimuleras företagen till att fokuserar på att organisera informationen i ett förutbestämt format som är maskinläsbart kan automatkontering underlättas. Detta kommer sannolikt att driva på tillämpningen av standarder för kvitton utan krav på lagstiftning.

Detta projekt syftar till att göra en lösning som blir hållbar på sikt. Det går att argumentera för ett möjliggörande av foton av kvitton idag men risken är uppenbar att detta om ett antal år leder till ökat fusk och det bör därför utredas om det föreslagna systemet i så fall ska införas längre fram i tiden. Risken är att ett system med en enkel hantering och lagring av kvitton leder till ökade problem med fusk. Sannolikheten ökar då att Sverige, likt många andra länder ökar takten i insamlandet av känslig data. Om denna, data kommer i orätta händer hotas konkurrensneutralitet och privat företagsamhet i än högre utsträckning. En möjlighet är att se om det går att minska riskerna med fusk med bibehållen möjlighet till digitalisering med ny lagstiftning.

Vilka ändringar i bokföringslagen är nödvändiga för att tillåta detta sätt att lagra verifikationer? Förutom nuvarande möjlighet att arkivera verifikationer behöver det också vara möjligt att spara verifikationer på detta nya sätt. Ett kvitto/faktura/verifikation behöver med andra ord godkän-

nas som att det sparats och arkiverats korrekt om det utöver det lagrade uppgifterna i kvittot/fakturan även den avidentifierade verifikationen är registrerad i hash-registret och den signerade verifikationen från hashregistret sparas i bokföringen.

Enligt gällande lag får ett företag förstöra det som har tagits emot om det överförs till annat medium, dock först från det fjärde året räknat från ett räkenskapsårs utgång. Av förarbetena till bokföringslagen framgår dock att regeln om att det man tar emot ska sparas, ska uppfattas så att den inte förhindrar viss anpassning. Det anges att (något förenklat) ”har företaget tagit emot en elektronisk faktura som vid överföringstillfället inte hade antagit något fysisk form, ska informationen bevaras i elektronisk form så att den kan presenteras på det sätt som det från början var tänkt. Bestämmelsen är inte avsedd att hindra företaget från att anpassa (konvertera) mottagen räkenskapsinformation till sitt eget informationssystem.”.

En lagstiftning som tillåter överföring till ett nytt medium utan nuvarande krav på tidsfördröjning, när den beskrivna processen med verifikationshashregister finns, bör enlig bokföringsnämnden vara relativt enkel att införa.

Givet att det kan ta tid att införa systemet med verifikationshashregistret och att detta inte kommer att tillämpas i all länder under överskådlig tid finns det anledning att se över möjligheterna till lagstiftning som kan införas för att underlätta digitalisering och stimulera automatisering. I synnerhet är det nödvändigt. Att se över hanteringen av internationella kvitton.

Ett förslag är därför att lagstiftaren möjliggör arkivering av foton av kvitton om det kan säkerställas att fotot identifierar en unik rätt till kostnadsförande för företaget, åtminstone i de länder där ett säkerställande av kvittot med ett hashregister eller annan lösning inte finns.

Lagtexten kan alltså fokusera på något i stil med att:
Arkivering ska ske av verifikationen så att eget innehav, mottagande och eller egen utbetalning kan anses styrkt.
I ett förarbete kan lagen förtydligas så att det framgår att det som avses är att acceptera

- Ett papperskvitto i ursprungsutförande (såsom tidigare)
- Ett digitalt kvitto styrkt med mottagande
- Ett digitalt eller papperskvitto styrkt med samtidig utbetalning

**Fakturor och mervärdesskatt, moms**
Vad gäller mervärdesskatt finns en särskild regel i momslagen, ml, om äkthet och integritet. Det gäller utöver bokföringslagen och har till syfte att säkerställa att inga uppgifter förvanskas från det att fakturan utfärdas och under hela bevarandetiden. Detta krav gäller inte bara säljaren utan också köparen. Detta är ett tillkommande krav utöver bokföringslagen med innebörd att fakturan inte får förvanskas under tiden den förs över dvs. från den tidpunkt säljaren utfärdar fakturan till och med den tidpunkt köparen tar emot den. Det är viktigt att säljare och köpare har identiska uppgifter och dessa är en förutsättning för att Skatteverket ska kunna kontrollera att rätt mervärdesskatt har tagits ut av säljaren och att köparen har avdragsrätt för den mervärdesskatt säljaren tagit ut.

Ml:s utökade krav på att uppgifterna i en faktura inte förvanskas kommer med den beskrivna lösningen att vara mycket lättare att säkerställa. Det bör med andra ord betraktas som ett stöd för att införa systemet för fakturor.

**Förfarande vid revision och skatteutredning**
Möjligheten att kontrollera riktigheten i uppgifterna i en faktura eller ett kvitto kan nyttjas av flera olika parter.

*Företaget*
Det kostnadsförande företaget kan säkerställa att uppgifterna i en faktura som kommer från en underleverantör stämmer med de uppgifter som leverantörsföretaget använt i sin redovisning till verifikationshashregistret och bokföring. Görs en kreditfaktura kan denna också registreras i verifikationshashregistret och en ny korrigerad faktura registreras om det behövs.

Företagen kan också kontrollera att ett kvitto för utlägg som kommer från en anställd stämmer med det som registrerats av utställaren, samt att kvittot inte har använts tidigare. Om utgivaren skickar med hashen i kvittot kan företaget göra en förkontroll av uppgifterna innan de skickas till verifikationshashregisteret och notifieras som kostnadsförda.

*Revision*
Vid revision kan revisorn stämma av att alla verifikationer godkänts av verifikationshashregistret. Rent praktiskt använder revisorn då den publika nyckel som verifikationshashregistret publicerar och med vilken det går att kontrollera att verifikationerna är signerade. De arbetsmetoder som idag används för att kontrollera verifikationerna kan därmed förbättras. Vad av dessa förfaranden som ska betraktas som nödvändiga och lämpliga för

att betraktas som ”god redovisningssed” och förfarande vid revision är en bedömning bokföringsnämnden i samarbete med intressenter som exempelvis FAR kan utarbeta.

*Skatteutredning*
På samma sätt som vid revision har en skatterevisor möjlighet att kontrollera verifikationernas uppgifter på ett nytt, säkrare sätt med införande av ett faktura/kvittohashregister.

**Registrering för privatpersoner**
Det skulle kunna vara möjligt att redovisa utlägg som privatperson t.ex. för att samla dessa som utlägg för arbetsresor alternativs som utlägg för investeringar i en fastighet som minskar skatt på kapitalvinst vid försäljning. Denna fråga kan utredas vidare.

# Fullmakter/ombud/behörigheter

Arbetet med fullmakter, ombud och behörigheter har delats upp i dessa tre områden separat. Den lösning som beskrevs i det föregående projektet är främst lämpad för fullmakter som gäller hos flera olika aktörer och den är i grunden den enda lösningen vi kan identifiera för detta syfte. En alternativ med en enklare lösning för behörigheter finns framtagen i detta projekt. När det gäller ombudsfullmakter för myndigheter och banker är frågan säkerhetsmässigt och juridiskt svår och någon självklar lösning har inte identifierats för närvarande.

## Situationen och utmaningarna

Den största nyttan finns sannolikt i att effektivisera och säkra upp arbetet Med fullmakter och behörigheter som delas ut av företag och individer och där fullmakterna gäller hos banker och hos offentliga aktörer. Den vanligaste gruppen fullmaktstagare är sannolikt redovisningskonsulter som utnyttjar sina fullmakter och behörigheter att företräda ett stort antal företag och personer dagligen.

Vidgar vi frågeställningen till att omfatta behörigheter så finns det ännu större användarfall i det att det är mycket vanligt att firmatecknare delar ut behörigheter för anställda att vara behöriga att utföra många aktiviteter, såväl finansiella åtaganden som access till data osv.
Ett stort arbete uppstår också för revisorer, redovisningskonsulter, banker och offentliga aktörer att kontrollera om fullmakter och behörigheter finns och är aktuella samt om de var aktuella vid tidpunkten för ingående av avtal etc.

Eftersom kontrollen över vilka fullmakter och behörigheter som finns är nästan omöjlig att få en överblick över hanterar banker och offentliga aktörer detta system genom att upprätta egna ombuds- och fullmaktstjänster. Det vill säga, var och en av de stora aktörerna bygger sitt eget

system där, i första hand, företagaren/firmatecknaren kan gå in och registrera vilka som ska ges behörighet/fullmakt att företräda företaget och på vilket sätt. Det finns en utmaning för den enskilde företagaren med detta förfarande eftersom användargränssnittet kan skilja sig åt och kan vara svårhanterligt. Den tekniska och juridiska kompetens som krävs för att på ett säkert sätt dela ut behörigheter/fullmakter kan vara en utmaning. Bristande kompetens och tidspress kan leda till att nödvändiga ändringar i utdelade fullmakter/behörigheter inte genomförs. Det är inte ovanligt att en redovisningskonsult har behörigheter som borde slutat gälla för många månader sedan, ibland år.

## Resultatet av projektets fas ett

I det första projektet togs en lösning fram som skulle kunna lösa alla problem som beskrevs. I huvudsak:

- Möjligheten att få en överblick över giltiga fullmakter för såväl fullmaktstagare och fullmaktsgivare, samt i förekommande fall arbetsgivare till dessa.

- Möjligheten att kunna upprätta och avsluta fullmakter för såväl fullmaktstagare och fullmaktsgivare, samt i förekommande fall arbetsgivare till dessa.

- Möjligheten för fullmaktstagaren att kunna bevisa och för tredje part att verifiera fullmaktens giltighet.

Nackdelen med den lösningen var att huvuddelen av fullmakter/behörigheter/ombudsroller hos banker och myndigheter hanteras i avancerade och väl integrerade system hos banker och myndigheter. Det innebär en stor kostnad och risk och kommer att ta tid att ersätta dessa, eller att integrera med dessa. Lösningarna förutsätter att dessa aktörer är beredda att göra sig beroende av externa datakällor vilket är svårt ur många synvinklar.

## Utgångspunkten i detta projekt

I detta andra projekt har vi därför tittat separat på en del olika lösningar. Dessa kan grovt delas i fyra kategorier.

1. Enkla förbättringar som kan genomföras utan samordning av flera aktörer

2. Förbättringar av ombudshantering hos myndigheter – en lösning som om den blir framgångsrik eventuellt skulle kunna integreras med banker

3. En lösning för fullmakter där det idag inte finns en etablerad infrastruktur och där fullmakten gäller hos fler aktörer än en enskild myndighet eller bank. Ett exempel är framtidsfullmakter.

4. Ett system för behörigheter för företag och offentliga aktörer som är helt eller delvis självständigt – dvs. där samordning inte är nödvändigt.

## De behov som finns är i första hand följande

En mjukvara/tjänst och arkitekturför fullmakter/behörigheter kan skapa värde genom att underlätta i följande situationer:

1. En fullmakt/behörighet ska registreras och gälla hos flera banker, alternativt registreras hos flera banker på ett så enkelt sätt som möjligt.

2. En fullmakt/behörighet ska registreras och gälla hos flera myndigheter, alternativs så enkelt som möjligt.

3. En fullmakt/behörighet ska registreras och vara allmänt giltig – t.ex. gälla för ett visst belopp oberoende av var inköpet sker. Kontrollen av fullmaktens giltighet behöver då vara tillgänglig för allmänheten. Denna möjlighet är bra även i (1) och (2) men inte nödvändig eftersom den aktör hos vilken

fullmakten/behörigheten gäller kan ha kontroll över detta, beroende på lösningens utformning.

4. Revisorn begär ut en fullständig lista på fullmakter för att kontrollera att inköp, betalningar, avtal m.m. har tecknats av behöriga personer. Detta är revisorn skyldig att göra vid revision.

5. En person vill bevisa att vederbörande har en fullmakt och att fullmakten är giltig men även att personer får företräda/agera ombud i en given situation.

6. Redovisningskonsulten, företaget, eller banken, vill få en översikt över vilka giltiga fullmakter som finns för egen del eller bland sina anställda, vem som är fullmaktstagare och vem som är fullmaktsgivare.

7. En fullmakt/behörighet ska avslutas, till exempel för att en person avslutar sitt arbete som redovisningskonsult för ett företag, eller för att en fullmakt ska dras in.

8. En redovisningskonsult ska gå på semester och behöver överlåta sina behörigheter att företräda sina kundföretag på någon annan.

9. Internt utdelade behörigheter/fullmakter i ett företag. En nyanställd VD vill få en överblick över vilka behörigheter som finns bland de anställda. Hur skapas en översikt över vilka fullmakter och behörigheter som finns?

10. Sannolikt med koppling till ovan hur upprättas och hur skapas en överblick över ställningsfullmakter/behörigheter som följer med en viss anställning/position.

11. En konsument vill upprätta en fullmakt på papper. Fullmaktens giltighet behöver sedermera kontrolleras av en bank,

myndighet eller privatperson. Kontrollen behöver ske på distans – dvs. digitalt.

12. En framtidsfullmakt som är upprättad aktiveras av fullmaktstagaren. En avisering eller notifiering av att detta har skett synliggörs för andra inblandade, exempelvis fullmaktsgivaren.

13. Ett dödsbo behöver få tillgång till dödsboets tillgångar, access till system, samt kunna underteckna i dödsboets namn.

## Ombudsfullmakter

Ombudsfullmakter är det område som bedöms svårast och projektet har inget tydligt förslag på lösning för dessa. Frågan om fullmakter och behörigheter har berörts i en rad arbeten genom åren i Sverige. Digitaliseringsrättsutredningen lyfter tanken att det kanske kan finnas en möjlighet att använda blockkedjeteknik och ställer sig frågande till om det går att hantera med en central aktör. I DIGGs rapport ”säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn” är ”mina ombud” är ett av 5 prioriterade byggblock. Någon konkret lösning har vad vi känner till inte presenterats. I slutet av detta kapitlet finns några projekt och aktörer exemplifierade men en mer grundlig genomgång behövs.

Några huvudalternativ finns dock:
Bolagsverket har i dialog med DIGG och andra myndigheter ett pågående arbete kring ombud och behörigheter. Man har gjort en behovsanalys för att kartlägga behoven hos kommuner, myndigheter och privata aktörer och tagit fram en konceptuell arkitektur. Konceptet bygger på federerad lagring av digitala fullmakter (där fullmakterna lagras hos betrodda parter) men omfattar i detta läge inte användning av blockkedjor.

När det gäller en central aktör kan detta vara två alternativ:

1. Den myndighet som samlar information skickar en förfrågan till de myndigheter fullmakten ska gälla via ett api. Respektive myndighet hos vilka fullmakten/fullmakterna gäller skickar en förfrågan – i praktiken via mobilt bankid eller Freja ID och får svar från om registreringen är godkänd av fullmaktsgivaren.

2. Störst säkerhetskrav skulle sannolikt ställas på en lösning som är helt centraliserad. Den myndighet som samlar information skickar en förfrågan om signering direkt till mobilt bank ID eller Freja ID och får svar om fullmakterna signerats. Meddelande om vilka fullmakter som blivit signerade skickas därefter till respektive myndighet där fullmakten/fullmakterna gäller. En gissning är att detta förfarande blir svårare i fallet med deklarationsombud eftersom det måste godkännas av Skatteverket, men det är intressant att veta för olika typer av fullmakter.

En utmaning med det huvudsakliga användarfall som beskrivs ovan, dvs. redovisningskonsulters ombudsroll i system hos banker och myndigheter förutsätter ett incitament från de senare att göra tekniska ändringar och sannolikt dela ansvar med andra aktörer för hanteringen. Blir arbetet för komplext kan det fördröja en möjlig implementering i många år. Förutom att utreda dessa frågor dvs. juridik och säkerhetsfrågor finns det anledning att titta på enklare lösningar för delar av problemen som en väg framåt.

**Enkla förbättringar för att avsluta fullmakter**

Ett identifierat problem med fullmakter som ej är avslutade eller går att avsluta gäller redovisningskonsulters ombudsfullmakter hos myndigheter och banker. Ett alternativ är att fullmakter alltid kan avslutas av fullmaktstagaren, dvs. inte bara fullmaktsgivaren vilket ofta är fallet idag. Juridiskt och tekniskt bör detta vara en enkel lösning. När det gäller myndigheter kan krav på detta komma från regleringsbrev, föreskrift eller liknande. Skatteverket har redan en sådan lösning. När det gäller bankerna kan det finnas en konkurrensfördel. Redovisningskonsulterna och revisorerna kan också förstärka denna effekt. Redovisningskonsulterna som har stor fördel

av denna funktionalitet kan rekommendera sina kunder att välja den eller de banker som erbjuder ett förenklat förfarande för att avsluta fullmakter, alternativt erbjuda lägre priser.

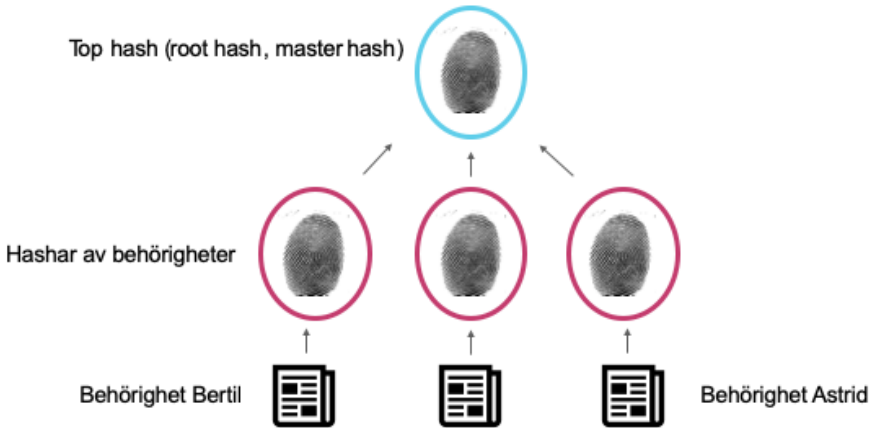
**Enklare upprättande av ombudsfullmakter hos banker och myndigheter**
Om själva upprättandet av fullmakterna sker på en annan plats än i respektive bank och myndighets system uppstår en fråga om vem som bär ansvaret om den samlade lösningen hackas eller oriktiga uppgifter registreras av olika skäl, eller om det finns en konflikt mellan uppgifter i den nya portalen och det egna systemet hos banken/myndigheten.
Banker och myndigheter har också lagstiftning att förhålla sig till på området. En myndighet kan inte göra sig beroende av externa it-system utan förbehåll. En bank kan inte avsäga sig sitt ansvar för kontroll av sina kunder.

Givet att problemet främst syftar till att göra det enkelt få en överblick kring hur fullmakter upprättas och vilka som bör upprättas kan systemet eventuellt upprättas på en lägre säkerhetsnivå. Det vill säga det kan exempelvis vara en länklista till de platser där fullmakter behöver upprättas. Andra lösningar kan vara att hantera frågan med enkla instruktionsvideos och/eller att skriva en lathund till företagarna.  I dagsläget försöker redovisningskonsulter ofta göra detta på distans och göra sina egna checklistor osv. Det går att förenkla detta.

## Behörigheter inom en organisation

Om fokus är på fullmakter, behörigheter inklusive ställningsfullmakter som ett företag ger till sina anställda går det att upprätta en arkitektur motsvarande den som beskrevs i den föregående rapporten på företagsnivå

och som finns längs ner i detta dokument. Ett sådant system kan upprättas helt i respektive företags eget system men där publicering av hela eller delar av det sk Merkleträd som förhindrar ändringar i behörigheterna görs publikt – t.ex. på hemsidan eller annan plats. Rent tekniskt kan en ”förankring” av datan i Merkleträdet göras på en extern plats på säker plats så att säkerhetsriskerna minimeras. Det betyder att en så kallad top hash registreras på en annan säker plats, något som kan vara relevant för ett mindre företag, eller ett företag med en hemsida som kan hackas för lätt, eller organisationer som vill höja säkerheten. En enkel illustration och beskrivning ser ut som följer.




Företaget vill dela ut behörigheter till tre anställda. Var och en av dessa har en fil som beskriver respektive persons behörigheter. Hasharna av dessa filer publiceras på ett intranät. Alla hasharna slås samman och bildar en top hash. Top hashen omöjliggör nu ändringar av alla underliggande filer. En av de anställda, Bertil, kan nu gå till t.ex. en leverantör och bevisa att han är behörig att företräda organisationen. Han visar då sin fil, visar att filen ger upphov till en hash och att hashen tillsammans med ett antal andra hashar kan skapa top hashen. Eftersom top hashen är publikt

tillgänglig kan Bertil inte ljuga. Systemet syftar till att ge leverantörer och anställda bevis för behörigheter. Det ger dem trygghet.

För företaget som sätter upp systemet ställs det givetvis krav på att de vet vad de gör, men det är inte komplicerat. Andrahandsuppgifter som framkommit i projektet är att skl har menat att det går att komma relativt långt med att bara kunna säkerställa att en person är anställd. För detta syfte kan systemet vara väldigt lämpligt. Givet att det framgår att enbart anställningsbevis finns att verifiera är det inte lika känsligt ur säkerhetssynvinkel. Företaget kan också lätt ändra sin top hash till exempel dagligen om de önskar. Det blir lite som ett bevis för ”vår sanning idag”.

För myndigheter saknas en ansvarig registerhållare motsvarande Bolagsverket roll för privata företag och organisationer. Det finns därför ingen källa till en motsvarighet till firmatecknare hos myndigheter och därför inga behörigheter som delas ut av en firmatecknare. En möjlighet är därför att myndigheten upprättar ett sådant register självständigt enligt principen ovan. De definierar därmed själva sin ”firmatecknare” och firmatecknarens delegerade behörigheter.

## Extern fullmaktstjänst inklusive framtidsfullmakter

Om vi bortser från de fullmakter som upprättas i ett slutet system idag, dvs. hos banker och myndigheter är det ”enklaste” att låta en enskild aktör registrera och hålla kontroll på vilka fullmakter som gäller. För enklare fullmakter med ett begränsat syfte går detta att lösa på motsvarande sätt som fullmaktskollen som beskrivs nedan. När det gäller mer generella fullmakter kommer den aktör som erbjuder tjänsten att bli samhällskritisk eftersom fullmakter kan ge väldigt långtgående befogenheter till fullmaktstagaren. I det fallet framstår den lösningen som föreslogs i den föregående rapporten vara den mest rimliga. Det finns andra varianter på

systemet med mycket likande funktionalitet och arkitektur som är open SOUrce på Github https://github.com/google/trillian. Det systemet använder tre Merkleträd. En av fördelarna med dessa lösningar är att den mest kritiska delen av processen ur säkerhetsynvinkel, dvs. upprättandet av fullmakten, inte kontrolleras av systemet. Upprättandet kan, som idag, ske med digitala underskrifter och e-IDentifiering eller på papper.

Det är också möjligt att använda lösningen för att skapa värdefulla tilläggstjänster, inte minst för framtidsfullmakter. En framtidsfullmakt kan tas i bruk av fullmaktstagaren när fullmaktstagaren bedömer fullmaktsgivaren oförmögen att agera på egen hand. Det kan vara rimligt att fullmaktsgivaren kan få en avisering om att detta har skett (och kanske göra en annan bedömning). Det går bra att göra med föreslagen arkitektur.

Behovet av en lösning för framtidsfullmakter har identifierats i projektet, även fullmakter för gode män och personal i hemtjänsten har nämnts.

När det gäller frågan om framtidsfullmakter har vi inte lyckats få klarhet i om digitala signaturer är godkända. Framtidsfullmakter ska bevittnas men i övrigt är det oklart. Det är inte. Ens säkert att det går att fastställa. Digitaliseringsrättsutredningen skriver:

”Författningskrav på underskrift kan betecknas med ett antal olika termer, varav underskriven, undertecknad och namnteckning är några. Ibland kompletteras de olika termerna med ordet ”egenhändig”. Exakt vad dessa krav innebär är emellertid inte helt klart.” Det är med andra ord inte alltid möjligt att utifrån laxtext och förarbeten klargöra vad som gäller. Det krävs att detta fastslås i domstol.

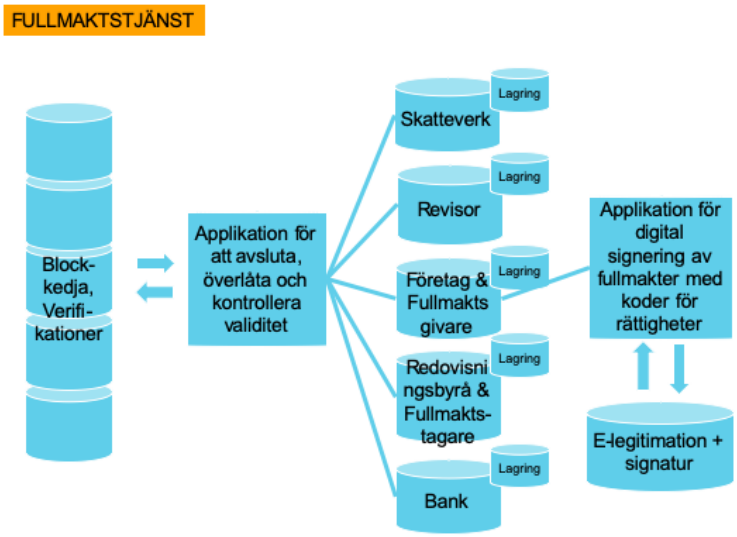
Alldeles innan detta skrivs har vi fått uppgift om att det finns en pågående statlig utredning om att möjliggöra digitala framtidsfullmakter. Det ger anledning att tro att digitala underskrifter inte är giltiga enligt lagens

förarbeten. Detta får utforskas närmare. Helt klart är att det finns stora fördelar om framtidsfullmakter kan kontrolleras med den föreslagna arkitekturen.

**Värde och kostnad**

Frågan om giltigheten hos en digitalt signerad fullmakt gäller framtidsfullmakter. När det gäller tekniken är det i vilket fall fullt möjligt att genomföra detta. Det är inte dyrt. Däremot uppstår en fråga om vem som ska äga lösningen. Ska giltigheten säkras över tid kan det vara svårt för privata aktörer att lösa uppgiften. I så fall återstår offentliga aktörer och ett regeringsuppdrag. Lösningen är i stort densamma som beskrevs i det föregående projektet.

## Övergripande arkitektur



**Teknik**
Rent tekniskt kan ovanstående arkitektur byggas med några kompletteringar genom att utgå ifrån googles trillian project. Projektet är open SOUrce och kod finns publicerad på github. Det finns redan en framtagen en lösning för elektroniska löpande skuldebrev enligt denna teknik och det finns inga större skäl att tvivla på teknikens kvalité eftersom den stöds av google och kan granskas av alla som vill. Lösningen gör det möjligt att säkerställa versionshistorik samt en ägare till en digital fil anonymt. Lösningen kan vara distribuerad så att vem som vill kan lagra verifikationsträden/Merkleträden. I detta fall är det tre träd för olika delar ägare, filidentitet, version som håller det samman och säkerställer att det är anonymt.

**Process**
Upprättandet av fullmakterna sker på vanligt sätt i den digitala världen, dvs. en digital fil med innehållet i fullmakten signeras med ett digitalt ID och en digital signatur knyts till fullmakten. Fullmakten är nu giltig. Tanken är här att giltigheten samtidigt styrs av ett externt register i blockkedjan. Fullmakten är giltig om och endas om nödvändig status på fullmakten är registrerad i blockkedjan. Detta formuleras i fullmakten, dvs. vilka publika nycklar som har rätt att avsluta fullmakten, samt till vilka publika nycklar fullmakten kan överlåtas (om någon).

**Steg 1**
Fullmakten upprättas digitalt, vilket inkluderar giltighetstid, vem som är fullmaktstagare, vem som är fullmaktsgivare, omfattningen på fullmakten dvs. vad den kan användas till. Såväl fullmaktsgivaren som fullmaktstagaren fyller också i varsin publik nyckel som ger behörighet att avsluta fullmakten. Eventuellt registreras flera publika nycklar, eftersom det kan finnas intresse av att ge fler personer och organisationer rätt att avsluta och eller överlåta fullmakterna.

Fullmakten kan även upprättas fysiskt. På samma sätt som med en digital fullmakt behöver användning och villkor för giltighet regleras i fullmakten om den är fysisk, dvs. avslut av fullmakten kan ske digitalt även om fullmakten upprättas fysiskt. Ska fullmakten kunna kontrolleras behöver den registreras digitalt det innebär emellertid inte att registreringen är likvärdig med upprättandet av fullmakten.

**Steg 2**
Fullmakten signeras digitalt med en godkänd eID t.ex. Mobilt bankid eller Freja eID och en godkänd underskrift t.ex. från CGI knyts till fullmakten.

**Steg 3**
Fullmakten registreras i blockkedjan för fullmakter men endast som en hash, dvs. ett digitalt fingeravtryck för fullmakten. Bredvid hashen finns de publika nycklar som har rätt att avsluta fullmakten, vilka åtminstone bör finnas hos fullmaktsgivaren och fullmaktstagaren. Processen är nu klar och fullmakten kan användas.

Användarfall:

*1. Revisorn begär ut en fullständig lista på fullmakter för att kontrollera att inköp, avtal m.m. har tecknats av behöriga personer. Detta är revisorn skyldig att göra vid revision.*

Lösning:

Revisorn begär ut en lista på alla fullmakter som företaget har och deras digitala fingeravtryck, hashar. Hasharna för fullmakterna kontrolleras mot blockkedjan via ett enkelt API som bara behöver kontrollera att fullmakterna inte avslutats. Har de avslutats i blockkedjan behöver revisorn kontrollera när det gjordes och att fullmakterna endast användes när de var giltiga.

*2. En person vill bevisa att vederbörande har en fullmakt och att fullmakten är giltig men även att personer får företräda/agera ombud i en given situation.*

Lösning:

Ombudet visar upp fullmakten – t.ex. för banken. Banken gör en slagning i blockkedjan via ett enkelt API och kan bekräfta att den finns och att den fortfarande är giltig.

*3. Redovisningskonsulten, företaget, eller banken, vill få en översikt över vilka giltiga fullmakter som finns, vem som är fullmaktstagare och vem som är fullmaktsgivare.*

Lösning:

En förutsättning är att de anställda har förberett förfrågningar kring fullmakter och deras giltighet genom att skicka in de publika nycklar som respektive redovisningskonsult, bankanställd, företagsanställd m.fl. har registrerat i fullmakter. Respektive organisation kan välja om även de privata nycklarna ska sparas centralt. På organisationsnivå kan man då kontrollera samtliga giltiga och avslutade fullmakter som är registrerade.

*4. En fullmakt ska avslutas, till exempel för att en person avslutar sitt arbete som redovisningskonsult för ett företag, eller för att en fullmakt ska dras in.*

Lösning: den som vill avsluta fullmakten går in i ett gränssnitt som är uppkopplat till blockkedjan och registrerar den privata nyckel som tillhör den publika nyckel som finns knuten till fullmakten i blockkedjan. Den som har den privata nyckeln har rätt att avsluta fullmakten och den är därför registrerad som avslutad och kan därefter inte användas. Observera att denna rätt att avsluta fullmakten kan finnas hos flera personer och organisationer. Det kan exempelvis vara möjligt att avsluta en fullmakt för såväl en redovisningskonsult som dennes arbetsgivare.

*5. En redovisningskonsult ska gå på semester och behöver överlåta sina behörigheter att företräda företaget på någon annan kollega.*

Lösning:

Det finns lite olika sätt att lösa detta. Vanligtvis vill en redovisningskonsult kunna överlåta en fullmakt under t.ex. sin semester för att därefter kunna bli fullmaktstagare igen efter semestern. Det krävs en lite annan logik i denna situation eftersom den privata nyckeln inte kan publiceras och sedan användas igen. Redan i fullmaktens upprättande är det troligen nödvändigt ur juridisk synvinkel att tilldela rollen som möjlig framtida fullmaktstagare. Med andra ord, det bestäms vilken person som kan bli fullmaktstagare under semestern redan vid upprättandet. En publik nyckel även till denna person knyts då till hashen av fullmakten i blockkedjan. Dessa personer kan i sin tur sedan överlåta fullmakten mellan sig. Det går att lösa med kryptering även utan att avslöja den privata nyckeln. En väldigt viktig egenskap är att detta möjliggör att säkerställa vilken person som har fullmakten att företräda bolaget vid varje tillfälle och att det endast är en person i taget. Givet att fullmakten redan vid upprättandet har flera fullmaktstagare är det inte att betrakta som en traditionell överlåtelse av en fullmakt. Eventuellt kan därför fullmakter för deklarationsombud aktiveras för en annan person trots att en överlåtelse enligt lag i dagsläget inte är tillåten. Det beror på att det inte är en överlåtelse utan snarast en aktivering av en inaktiv fullmakt. Givetvis får detta inte ske om det betraktas som ett kringgående av lagstiftningen. Bedömningen är att lagstiftaren har haft för avsikt att begränsa överlåtelser av fullmakter till personer som fullmaktsgivaren inte accepterat eller godkänt. I detta fall har fullmaktsgivaren godkänt fullmaktstagaren på förhand och även fastställt villkoren för detta.

Lösningen kan som synes tillföra funktionalitet även för ombudsroller men som tidigare nämnts kräver det att myndigheter och eller banker accepterar att göra sig beroende av att kontrollera sina uppgifter med en extern databas.

# Governance juridik med mera

**Governance**
Det centrala i arkitekturen är att själva fullmakterna skiljs från blockkedjan. I blockkedjan finns ett Merkleträd som sparar giltighetsinformation om fullmakterna. Eftersom informationen i blockkedjan inte går att identifiera, varken vem som äger de privata nycklarna eller innehållet i fullmakterna är governancefrågan flexibel.
Det är tänkbart att företag, banker, redovisningskonsulter, erp-systemleverantör m.fl. Kan tänkas tillhandahålla denna arkitektur som en tjänst.
Det viktiga i arkitekturen är att säkerställa att data inte kan manipuleras.
Det finns fortsatt fördelar med att hantera databasen som en blockkedja eftersom det är blockkedjan som skapar redundans och minskar risken att någon enskild skaffar sig ett monopol med databasen som grund.

**ID**
En väldigt viktig del i lösningen är att skilja på upprättandet och avslutandet av fullmakter. Upprättandet av en fullmakt kräver mycket hög säkerhet. Vi vill inte att det skapas fullmakter av obehöriga. För detta syfte behövs säker identifiering och signaturer. För de privata nycklar som används är säkerheten inte lika avgörande. Den enda användningen av de privata nycklarna är att avsluta fullmakten. Det behövs därför inte någon CA certificate authority för hanteringen av de publika och privata nycklarna i blockkedjan. Hanteringen av fullmakternas giltighet, dvs. aktivering, avaktivering och avslut kan däremot hanteras med privata nyckar som genereras lokalt. Denna hantering kan banker och redovisningskonsulter se som affärskritisk och hantera med hög säkerhet, men för enskilda fullmaktsgivare är det ingen fara om en publik nyckel som är kopplad till en fullmakt kommer i orätta händer. Fullmakten kan avslutas, men den kan inte användas på annat sätt än den var tänkt.

**Lagring**
Lagring av fullmakterna, dvs. själva originalinformationen, kan göras väldigt flexibel. Det går att lagra dessa i en molntjänst, på en vanlig dator eller i en struktur för fullmakter hos professionella aktörer med många fullmakter.

Lagringen av själva databasen med verifikationer bör vara ett Merkleträd och gärna en blockkedja.

Långtidsarkiveringen av digitala filer, som fullmakter, är ett problem, men det är också ett problem för det mesta. Ett system kommer att komma långt med att möjliggöra att uppdatera nya signaturer och identiteter när säkerhetskraven höjs över tid, i takt med att datorernas beräkningskapacitet och ökar och nya algoritmer utvecklas.

## Bakgrundsinformation och andra projekt

Det finns ett antal andra projekt på området som identifierats. Kunskapen om dessa är för låg för att vi ska beskriva dessa mer i detalj men följande är några av de viktigaste:

- Bolagsverkets projekt kring ombudsroller
- Fullmaktskollen
- De nordiska bankernas bolag kring kyc
- En statlig utredning kring digital signering av framtidsfullmakter
- EU-projektet Semper
- Privata initiativ

# Företagsuppgifter

I det föregående projektet identifierades företagsuppgifter som ett intressant område för nya tjänster. Under projektet blev det samtidigt tydligt att det är många områden och frågeställningar. Huvuduppgiften i detta projekt dvs. fas två har därför varit att strukturera upp frågeställningen och göra den hanterbar.

## Tillgängliggöra uppgifter respektive inlämning

Till att börja med har vi tittat på två typer av situationer. Dels hur vi kan få tillgång till, verifiera och dela uppgifter om företag med lämplig nivå på säkerhet och anonymisering. Dels möjligheter till förenkling för inlämning av företagsuppgifter till myndigheter som Skatteverket, SCB, Bolagsverket m fl.

## Verifiera och dela uppgifter

Uppgifter som ska verifieras är många och det har därför varit angeläget att börja dela upp uppgifterna/datan i olika kategorier.

**Egen data**
Uppgifter som ett företag är skyldigt enligt lag att registrera och spara men där dessa uppgifter inte skickas in till någon myndighet. Det kan också vara uppgifter som företaget inte är tvingade enligt lag att hålla i något register men uppgifter som likafullt kan vara intressanta att verifiera för andra personer och organisationer. Exempel kan vara: fakturor, kvitton, löpande bokföring, lägenhetsförteckning i bostadsrättsförening, personalliggare, aktiebok, behörigheter att företräda företaget, vanliga avtal.

**Rapporterad data**
Uppgifter som ett företag är skyldigt enligt lag att registrera och spara men där dessa uppgifter dessutom skickas in till en myndighet. I de flesta fall har uppgifterna lagtekniskt inte överförts – dvs. är årsredovisningen som skickats in till Bolagsverket felaktig är det fortsatt företagets årsredovisning som gäller. Väljer en bank att låna ut pengar till ett bolag med oriktig omsättning i den inlämnade årsredovisningen får banken problem. Företaget kan bli skadeståndsskyldigt men de juridiskt bindande uppgifterna är de som företaget har. Det kan fortsatt vara intressant för andra intressenter att ta del av dessa uppgifter från en myndighet. Samma förhållande gäller arbetsgivardeklarationer på individnivå som till exempel skickas till försäkringskassan som underlag till beslut. Skatteverket kan emellertid inte veta om uppgifterna stämmer. Exempel kan vara: årsredovisning till bv, arbetsgivardeklarationer till skv, prisnivåer till SCB.

**Myndighetsregisterdata**
Uppgifter som är att betrakta som ”sanning” när de blir registrerade hos en myndighet. Som huvudregel har alltså dessa uppgifter företräde i juridisk mening. En person som påstår sig heta anna men i folkbokföringen heter angelica heter som huvudregel i juridisk bemärkelse angelica. En person som är gift är det som huvudregel i juridisk mening först när det är regist-

rerat i folkbokföringen. En bank som låtit en behörig firmatecknare ta ett lån för ett företag har ett gott skydd om det är en firmatecknare som är registrerad hos Bolagsverket. Om företaget har andra uppgifter är det i första hand deras problem, även om banken också kan få problem. Exempel kan vara: stadgar och uppgifter om firmatecknare hos Bolagsverket, fastighetsregistret och pantregistret hos Lantmäteriet och personuppgiftsregistret hos Skatteverket, Authorised Economic Operator hos Tullverket.

**Uppgifter om företag som ägs av tredje part**
Uppgifter om ett företag som samlats in, prioriterats och analyserats för att sedan säljas. Antingen tar man betalt för upprättandet av analysen från företaget som analyseras eller från de företag som önskar information om andra företag. Exempel kan vara: UC, Allabolag, Datcha, Esri.

## Tankar om lösningar för att tillgängliggöra uppgifter

Indelningen i de olika typerna av data ger en tydlig insikt. När det gäller den första gruppen data, egen data, finns det ett flertal lösningar som är beskrivna i denna rapport. Lösningar för behörigheter, personalliggare, löpande bokföring, fakturor etc. hamnar alla inom denna kategori. En insikt är därför att den teknik som är grunden i många av lösningarna i första hand hashar och Merkleträd, (digitala fingeravtryck och trädstrukturer av fingeravtryck) sannolikt kan lösa mångas problem inom denna kategori data. Det innebär att om vi identifierar en typ av data som kan klassificeras som egen data kan den sannolikt förbättras med liknande teknik.

I kategorin ”myndighetsregisterdata” finns det förutom fiskala intressen från myndigheterna även säkerhetsfrågor som vi inte har grävt djupare i än. Det vill säga det kan finnas ett samhällsintresse av att inte sprida dessa uppgifter för friktionslöst av säkerhetsskäl. Myndigheter som Lantmäte-

riet och Bolagsverket tar också betalt för hanteringen av dessa uppgifter, de kan till och med vara tvingade till detta.

Det är troligen möjligt att bygga ett system som kan underlätta hanteringen och därmed kostnaden för handläggning. Ett bortfall i intäkter kan då delvis kompenseras. Det förutsätter emellertid att säkerhetsaspekterna är tydliga och kan hanteras.

För rapporterad data gäller i stort sett samma som ”myndighetsregisterdata”. En möjlighet kan uppstå att säkerställa underlaget till denna data, till exempel att säkerställa att omsättningen inte kan manipuleras utan bygger på verkliga siffror. Inget av dessa användarfall har analyserats närmare. För ytterligare begrepp kring data som berör myndigheter kan man läsa denna rapport från DIGG.[5]

Beroende på affärsmodell kan tredjepartsdata vara attraktivt att distribuera och säkra på nya sätt. Det enklaste är när man tar betalt av den som analyseras. Ett företag som tar betalt för att göra en analys eller en certifiering , t.ex. bolagsanalys av en bank eller en iso-certifiering kan med fördel distribuera sina analyser säkert, digitalt, verifierbart och med lämplig nivå på anonymisering. I situationer där den som gör analysen tar betalt av den som vill kontrollera någon annan kan det vara svårare att hitta en affärsmodell med en teknik för verifiering. Det ligger ofta i den sammanställande organisationens intresse att kunna sälja samma analys flera gånger och då vill man inte att spridning och kontroll ska ske för lättvindlit.

## Samordnad inlämning av uppgifter till myndigheter

I den föregående rapporten nämndes TOOP, the once-only principle. Tanken med detta är att det ska vara lättare för företag att rapportera in data till myndigheter. Det finns också ett EU projekt som arbetar med

frågan the once-only principle project. Idag begär myndigheter in data i många olika plattformar och format är tanken att detta ska samordnas för att underlätta för företagen.
En utmaning är att det är väldigt många myndigheter i Sverige och naturligtvis mångdubbelt fler inom EU. Att samordna alla dessa myndigheter för att samla in data i samma format är mycket svårt, i det närmaste omöjligt, utan tvingande lagstiftning på väldigt detaljerad nivå.

Ett alternativ som diskuteras är att myndigheterna ska hämta data mellan varandra. Återigen är detta synnerligen komplicerat. Det finns ingen generell infrastruktur för att dela data mellan myndigheter i Sverige och än mindre inom EU.

Det finns exempelvis processer för data som skickas mellan skattemyndigheter inom EU men det är inte vanligt med sådan infrastruktur. Nordic Smart Government arbetar med att underlätta detta i framtiden.

Estländska X-road som numera hanteras av Nordic Institute for Interoperability Solutions, NIIS, är ett alternativ. Varje myndighet har då en ”security server” som kan identifieras och kopplas upp för att hämta data från en annan myndighets ”security server”. Den centrala administrationen kan i denna lösning inte läsa vad som skickas.

I Norge finns istället alltinn som samlar in all data och fördelar ut den till myndigheter. Det närmaste exemplet i Sverige är verksamt.Se. Det är dock en mindre fullständig lösning än den i Norge.

Inget av dessa alternativ är enkelt att införa utan det krävs omfattande arbete och lagkrav på införandet för varje myndighet som ska omfattas av systemet.

**Samverkan en utmaning**
Den svenska regeringen gick våren 2018 ut och talade om en ambition att underlätta för företagen att skicka in uppgifter till myndigheter. Näringsminister Mikael Damberg var samtidigt ödmjuk och menade att ”det är en oljetanker som ska vända”.

Förutom den tekniska utmaningen är en orsak till att detta är svårt är att myndigheter är självständiga i Sverige och inte får fatta beslut på oklara grunder.

I utredningen om grunddata står att läsa:

*Generella regler för samverkan finns i förvaltningslagen, myndighetsförordningen och förordningen om statliga myndigheters elektroniska informationsutbyte. Samverkan som syftar till att följa riktlinjerna måste hålla sig inom ramen för dessa regler. Förenklat uttryckt gäller följande:*

- *Myndigheter kan inte genom samverkan åta sig nya uppgifter som inte kan härledas till befintliga regler som styr myndighetens verksamhet. Beslut som fattas av myndigheter som ingår i samverkan utgör självständiga myndighetsbeslut och kan inte innebära tvingande handlingsregler för någon annan part utanför samverkan. Samverkan får inte leda till att sekretessbelagda handlingar röjs eller att hantering av personuppgifter sker i strid med gällande dataskyddslagstiftning. Införande av uppgifter i författningsreglerade statliga register kräver författningsändringar och kan inte beslutas i samverkan.*

*De riktlinjer som rör myndigheternas samverkan om grunddata ska läsas mot bakgrund av ovan beskrivna rättsliga ram. Det bedöms inte föreligga hinder för Bolagsverket, Lantmäteriet, Skatteverket och DIGG att samverka i syfte att standardisera myndigheternas grunddata.*

En tolkning av detta är att en myndighet inte kan avhända sig beslutsrätt till ett samverkansarbete. Hänsyn till andra myndigheters intressen utöver det egna uppdraget kan också vara svårt att motivera.
Det kan låta märkligt men alternativet kan också leda till oklarheter. En myndighet som börjar driva sin verksamhet i hög utsträckning för att stödja andra myndigheters uppdrag får en oklar roll.

En slutsats av detta är att det läggs ett större ansvar på regering och riksdag att formulera tydliga uppdrag för att myndigheterna ska kunna agera konstruktivt när samarbeten mellan myndigheter är värdefulla.

En andra slutsats är att det finns anledning att vara försiktig med förhoppningar om vilka standarder myndigheter kan samordna sig kring. I dagsläget kan två myndigheter ha problem med att enas om hur ett enhetligt format för personnummer ska se ut (tio eller tolv siffror, bindestreck eller inte t ex). Inom vården finns det ett stort värde av att kunna läsa patientjournaler från andra landsting. Enligt en företrädare från skl finns det fyra stora leverantörer av patientdatasystem i Sverige. I dessa finns över 270 olika klassificeringar av patientdata. Ingen klassificering är likadan i två system. I flera decennier har det därför ägnats mycket tid och många miljarder åt att omklassificera patientdata för att passa i andra system utan en lösning i sikte.

En tredje slutsats är att det är enklare att styra myndigheterna med uppdrag till var och en snarare än med samarbeten.

## Lösningsförslag inlämning av företagsuppgifter

Ett förslag till lösning för att snabbare inleda arbetet med enklare inlämning av företagsuppgifter är att fokusera på teknisk tillgänglighet snarare än standardiserat innehåll och kommunikation mellan myndigheter. En

bra inspiration kan vara andra betaltjänstdirektivet, mer känt som PSD2, direktiv (EU) 2015/2366.

I PSD2 specificeras att banker och olika betaltjänstaktörer är tvingade att tillgängliggöra ett antal uppgifter om sina kunder till tredje part – om kunden som uppgifterna gäller har gett sitt medgivande. Nordea kan be en kund Lars Larsson om godkännande för att hämta uppgifter om hans affärer i SEB. SEB är då tvungna att tillgängliggöra lars larssons uppgifter (inte alla uppgifter men de som definieras i PSD2). Syftet är att möjliggöra ”open banking”, en bättre konkurrens och nya möjligheter att utveckla nya och bättre tjänster.

För att tillgängliggöra uppgifterna ska bankerna och andra betalningsförmedlare tillhandahålla ett API som andra banker och aktörer kan ansluta sig till för att hämta och dela uppgifter på ett effektivt sätt. Intressant är att EU inte har ställt hårda krav på API:erna. Det är alltså många olika varianter hos olika banker. Det är emellertid inte något stort problem. Nu när API:erna är på plats har det snabbt uppstått flera lösningar för att integrera med olika API:er. En bank som vill hämta in uppgifter kan därför vända sig till en integrationsplattform som har den tekniska integrationen med flera aktörer och hämtar in uppgifter från dessa. På detta sätt behöver inte alla skapa relationer till alla motparter, något som är helt nödvändigt för att systemet inte ska bli för komplext.

En liknande tanke har framförts när det gäller elektroniska fakturor. Det vill säga, istället för att harmoniera teknik och innehåll kan en växlingsmotor hantera detta. Där har emellertid kravet på att uppgifter i en faktura inte får förvanskas varit ett av skälen till att projektet bromsats. Eftersom samma krav inte finns för företagsuppgifter bör det vara möjligt att genomföra.

Ett förslag är att DIGG får i uppdrag att ta fram en likande öppen teknisk specifikation för hur information ska skickas in till myndigheter som i fallet med PSD2. Regeringen ger parallellt ett uppdrag till berörda myndigheter att ta fram dessa API:er (för att ta emot den data de enligt lag ska samla in). Eftersom detta inte kräver någon samordning mellan myndigheterna är det lättare att skriva ett tydligt uppdrag till dessa var och en. I praktiken blir det gissningsvis samma eller ett mycket likartat uppdrag till alla berörda myndigheter.

Eventuellt krävs ingen lagändring. En myndighet bör på eget initiativ kunna utveckla ett API som det går att ansluta sig till och ställa krav på de som kopplar upp sig. Skulle tillräckligt många myndigheter göra detta skulle systemet eventuellt kunna uppstå utan nya regeringsuppdrag.

Beträffande de standarder som arbetas fram kring företagsfakta inom exempelvis EU och Nordic Smart Government kommer dessa att behöva hanteras kontinuerligt. Det vill säga, det är inte nödvändigt att vänta tills standarderna är klara. Respektive myndighet kommer att behöva anpassa sig till dessa standarder i vilket fall och det kommer inte att vara en slutlig standard utan sannolikt kommer nya anpassningar över tid. Det arbetet kan därför pågå parallellt.

När alla myndigheter gjort sina API:er klara kommer det naturligt att uppstå ett intresse från affärssystemleverantörer och andra att skapa integrationer mot de olika API:er som myndigheterna tillhandahåller. Ett fåtal tekniska plattformar kan då agera mellanhand och lösa integrationerna samt se till att data skickas i de tidsintervall som respektive myndighet önskar.

För företagen är det viktiga inte att myndigheterna begär in uppgifterna en gång eller i ett gränssnitt utan att företagen kan skicka in och registrera uppgifterna endast en gång.

# Personalliggare

Ett lagkrav på personaliggare har införts i en rad branscher i Sverige. Syftet har varit att minska förekomsten av svart arbetskraft. Rapporten från den första fasen i detta projekt (blockkedjeinspirerade lösningar för redovisning, revision och skatt) beskrev en tänkt lösning för hur personalliggaresystemet kan förbättras. I det förslaget fanns en blockkedja med som ett alternativ. I detta projekt har en del enklare alternativ tagits fram som kan underlätta en implementering. Stora utvärderingar av systemet har också presenterats under året, vilka visar på ett behov av förbättringar.

## Nyligen genomförda utvärderingar

Sedan rapporten presenterats har bland annat skatteutskottet respektive handelns forskningsinstitut, på uppdrag av Svenskt Näringsliv, gjort rapporter med utvärderingar av personalliggare. (En utvärdering av personalliggarsystemet ISSN 1653-0942, ISBN 978-91-88607-77-5, Riksdagstryckeriet, Stockholm, 2019) (hur påverkas företagen av kravet på personalliggare, HFI forskningsrapport 2019:02)

Utvärderingarna visar på brister i systemet. Skatteutskottets utvärdering visar att de som är kritiska framför följande synpunkter.

- Skatteverket lyckas inte nå de oseriösa företagen.
- Skatteverket borde genomföra fler kontroller.
- Systemet med personalliggare anses vara för lätt att lura.

I skatteutskottets rapport finns också många synpunkter som visar på nyttan med systemet.

Handelns Utredningsinstitut framför bland annat följande kritik.

- Företagen tvivlar på att systemet lyckas identifiera fusk eftersom ”Skatteverket inte gör någon kontroll mot faktiska löneutbetalningar”.

- Det finns bland en del svarande en uppfattning att det är en kontrollavgift som snarast belastar seriösa företagare.

- Det finns en kritik mot kravet på registrering av egna barn och ägaren i personalliggaren.

I båda rapporterna finns en oklarhet i hur stor effekten är på faktiska löneinbetalningar är. I handelns forskningsinstituts rapport drar man slutsatsen att den effekten är mycket liten, om något. De drar slutsatsen att personalliggare bör avskaffas. Skatteutskottets utredning konstaterar att det finns skäl att se över systemet utan att tydligt ta ställning för eller emot.

Svenskt Näringsliv, Visita och Handelns forskningsinstitut arrangerade ett seminarium den 9 oktober 2019 där rapporten från Handelns Forskningsinstitut presenterades. Under seminariet fick vi som åhörare intrycket av att kritiken mot personalliggare är större i restaurangbranschen än i byggbranschen. Ordföranden i skatteutskottet gav ett färskt exempel på hur ett av Sveriges största företag upptäckt svart arbetskraft på ett av deras upphandlade byggen. Underentreprenörer till huvudentreprenören visar sig ha anlitat svart arbetskraft. Sveriges byggindustrier har enligt andrahandskällor framfört önskemål till regeringskansliet om att Skatteverket ska samla in ännu mer uppgifter för att stävja fusket på byggarbetsplatser.

## Vad kan förbättras

I denna rapport tar vi inte ställning till om systemet ska vara kvar. Fokus ligger istället på hur systemet kan förbättras. Fyra exempel på förbättringar är:

1. I båda utvärderingarna framgår att det är en mycket stor andel av företagen som gör fel med personalliggarna. Av de företag som uppger att de blivit kontrollerade (54%) uppger 47% att de fått betala en kontrollavgift. I skatteutskottets utvärdering anges hur stor andel av de kontrollerade företagen som handläggarna på Skatteverket bedömer gjort fel, inklusive fel som inte leder till kontrollavgift. Medianuppfattningen bland handläggarna är att CA 40% av företagen har gjort fel.

   Slutsats: omfattningen på felaktigheter är ett stort problem och det ligger inte i linje med visionen om att ”det ska vara lätt att göra rätt” eller ”compliance by design”. Det bör vara möjligt att förbättra väsentligt.

2. Om kontroll på restaurang skriver skatteutskottets utredning följande:
   ”När kontrollanterna har gått in i lokalen och legitimerat sig frågar de direkt efter personalliggaren och den som är ansvarig på plats. De försöker få kontroll över personalliggaren så fort som möjligt så att den inte kan manipuleras. Om näringsidkaren måste gå och hämta liggaren följer kontrollanten med.”

   Slutsats: skrivningen ger anledning att tro att det förekommer att personalliggaren manipuleras vid kontroller. Förslaget i denna rapport innebär att manipulation vid kontrollbesök blir i det närmaste omöjlig.

3. En personalliggare kan föras manuellt (i bokform). Den ska då vara inbunden/limmad, och sidorna ska vara förnumrerade. Det betyder att man inte kan använda lösa papper eller exempelvis ett spiralblock. Det är inte heller tillåtet att använda blyertspenna. Skatteverket har tagit fram en manuell personalliggare som man kan använda, men en personalliggare kan också föras elektroniskt. Det är samma krav på vad som ska antecknas i den elektroniska personalliggaren som i den manuella. I programmet måste alla händelser loggas, så att det framgår vem som har gjort en ändring och när. Systemet måste även vara utformat på ett sådant sätt att Skatteverket ska kunna granska uppgifterna bakåt i tiden.

Slutsats: i praktiken är kraven på loggar av ändringar omöjliga att säkerställa eftersom det inte finns några formkrav på elektroniska personalliggare. Det går bra att använda vanliga program som excel och word för den som önskar. Detta går och bör förbättras för att göra det tillräckligt svårt att manipulera.

4. Under seminariet den 9 oktober menade restaurangägaren som var representerad i panelen att personalliggaren inte kunde fylla någon funktion. Skälet som framfördes var att vid kontroll jämförde kontrollanten inte uppgifterna mot löneinbetalningarna och det blev därför bara en närvarokontroll. I samtal med Skatteverket framhålls istället att personalliggaren fyller en funktion att se om det är värt att göra en större utredning och att det kan finnas värdefulla uppgifter som kan meddelas polisen till exempel. I skatteutskottets utredning framgår att det är lite olika hur personalliggaren används vid utredning/kontroll. Det kan dels bero på utredarens erfarenhet och förmåga men det beror också på att det finns olika

begränsningar i hur personalliggaren får kontrolleras och vad den kan användas till.

Slutsats: det behöver naturligtvis klargöras vad personalliggaren kan användas till och vilka privata intressen, integritet, datasäkerhet m.m. som behöver skyddas. Givet att det finns en kritik från skötsamma företag i restaurangbranschen att personalliggaren inte fyller sin funktion för att den inte används tillräckligt finns det anledning att tro att det går att förbättra och bredda användningen. När syftet och användningen fastställts är det viktigt att uppgifterna inte går att förvanska, till exempel om polisen vill kontrollera en uppgift vid ett senare tillfälle. Det är mer rättssäkert om varje enskild uppgift säkerställs, till exempel en personalliggare, snarare än att en stor grupp osäkra data ska analyseras för att göra en riskbedömning.

5. I skatteutskottets utredning är ett förslag på förbättring av personalliggarsystemet fler kontroller av Skatteverket. Utredningen visar på ett kraftigt sjunkande antal kontroller.

Slutsats: fler kontroller är ett kostsamt förslag på förbättring både för företagen och Skatteverket. Finns det system att göra kontrollerna riktade mot de som inte registrerat någon personalliggare eller där det finns skäl att misstänka fusk är det en fördel. Skatteverket arbetar idag framgångsrikt med maskininlärning för att göra mer precisa riskbedömningar av företag och därigenom öka sannolikheten att upptäcka fusk med samma antal skatteutredningar. Givetvis är det intressant om en liknande riskbedömning kan bli bättre även för personalliggare.

## En mjukvara/tjänst och arkitektur för personalliggare

Tanken med lösningar för personalliggare i det föregående projektet kan anses ha fått starkare stöd i utredningarna. Det är angeläget att göra förbättringar. Ett enkelt sätt att förbättra systemet är att registrera personalliggaren direkt hos Skatteverket. Arbetsgivarinlämning på individnivå, agi, är ett exempel på hur insamlingen av mer data gör det svårare att fuska. I skatteutskottets utredning menar nära nog samtlig handläggare att agi kommer underlätta arbetet med att identifiera fusk. Väljer lagstiftaren att samla in även personalliggare blir det givetvis ännu enklare att identifiera fusk och svårare att fuska.

Den enkla lösningen för att minska fusk är som alltid att samla in mer data. Personalliggaren kan också skrivas in direkt i ett register hos Skatteverket. Det är emellertid ett större hot mot integritet och en större risk och större kostnad för Skatteverket, om de blir registerhållare. Utmaningen ligger i att identifiera lösningar som minskar möjligheten till fusk utan att kompromissa för mycket med integritet och risker för att känslig data kommer i orätta händer.

## Förslaget

Lösningsförslaget bygger på att dela anonymiserad information. Syftet är att göra det svårare att göra fel och lättare att göra rätt. Detta innebär är att det i princip blir omöjligt att fuska med personalliggarnas innehåll samtidigt som alla uppgifter i personalliggarna förblir anonyma, dvs. omöjliga att dekryptera.

- Processen är i första hand tänkt att skapa en rutin för att registrera digitala verifikationer av personalliggarna, oavsett format. Själva personalliggaren kan vara analog men verifikationerna behöver vara digitala.

- Syftet är att göra det svårare att göra fel och lättare att göra rätt. Detta innebär är att det i princip blir omöjligt att fuska med personalliggarnas innehåll samtidigt som alla uppgifter i personalliggarna förblir anonyma, dvs. omöjliga att dekryptera.

- Ytterligare en fördel är att det kan bli lättare att kontrollera historiken i personalliggarna vid skattekontroll.

- En notifiering om en utebliven registrering kan också skickas till företag redan samma dag om det är önskvärt, vilket minskar risken att glömma registreringen. I dagsläget straffas en ägare av en restaurang om en anställd missköter sig med till exempel personalliggare, otillåten dans eller rökning vilket ifrågasattes på seminariet. Med ett elektroniskt system kan det gå att kontrollera hur många som är registrerade i personalliggaren t.ex. i en restaurang. Vill man göra detta anonymiserat är det också möjligt, dvs. att veta hur många som är där men inte vilka. Det kan också finnas en notifiering om att t.ex. nu är sex personer på plats.

- Värdet av lösningen består också i att eventuellt fusk med svart arbetskraft kan minskas och att det blir lättare att skilja på situationer med felaktig rapportering som bygger på rena misstag till skillnad från medvetet fusk.

- Skulle det finnas intresse och mandat att titta på personalliggaren vid andra tillfällen, eller av andra, t.ex. Polisen, går den inte att manipulera.

**Process**
Steg 1: Upprättande av personalliggare
Varje dag fylls personalliggaren i på samma sätt som idag. Givetvis är det en fördel om personalliggaren är digital men det går bra att ha en vanlig anteckningsbok, dvs. valfritt format kan fortfarande accepteras enligt de befintliga lagkraven.

Steg 2: Registrering av en verifikation
Från restaurangens affärssystem, beläggningsplanering, eller liknande där personalliggaren hämtas publiceras vilka som arbetar och när. Det går också att lösa detta i de fall personalliggaren är analog. I det fallet används en app i en telefon. Med den tas ett foto av personalliggaren varje dag. En verifikation, dvs. en hash, av filen/fotot registreras tillsammans med en kod som kan identifiera den som registrerar verifikationen. Registreringen görs med en anonym hash till en förutbestämd blockkedja, ett Merkleträd hos tredje part, på företagets hemsida eller direkt till en myndighet. Alternativet med publicering på en egen hemsida är med andra ord liknande det som beskrivs för i denna rapport under rubriken behörigheter med tillhörande illustration.

Steg 3: Notifiering
Notifieringen kan ske på olika sätt. Finns det digital integration finns många möjligheter. Då kan en utebliven registrering av personalliggaren notifieras valda personer på företaget. Behöver det göras ändringar i personalliggaren därför att någon är sjuk eller det behöver tillkallas mer personal görs uppdateringar i personalliggaren. Det går att bygga ett system som automatiskt kontrollerar vilka som är på plats och registrerar det via t.ex. wifi i mobiltelefoner, scanning av qr-koder, kameror. Det kan anses vara integritetskränkande och det kan anonymiseras till exempel vilka personer som är där, bara antalet. Uppgifterna registreras dessutom inte utanför restaurangen. Tekniskt och juridiskt är detta naturligtvis mer komplicerat men fullt möjligt.

Steg 4: Kontroll
Om Skatteverket ska göra en kontroll av personalliggaren kan mobilen eller mjukvaran som registrerat verifikationerna enkelt kontrolleras. Behovet av att få kontroll över personalliggaren så snabbt som möjligt som

skatteutskottets utredning beskriver är borta. Stämmer inte personalliggaren med den verifikation som är publicerad på hemsidan eller på annan plats har den ändrats.

Den personalliggare som har en verifikation på hemsidan (eller på annan vald extern plats) är den som jämförs med den personal som arbetar på restaurangen. Det är omöjligt att manipulera personalliggaren eftersom den då inte stämmer överens med verifikationen. Det är också lätt att kontrollera till exempel den senaste månadens registreringar, dvs. det är lättare att bedöma om det är ett olycksfall i arbetet att en registrering missats eller om det är systematiskt. Eventuellt kan skattekontrollerna styras till de företag/restauranger som inte gjort registreringar, det förutsätter dock att platsen med personalliggarverifikationerna (hasharna) är tillgänglig i någon form på hemsida, hos en myndighet, i ett merkle träd.

**Governance juridik mm**
Det centrala i denna lösning är att beskattningen av personalen säkras i de digitala informationskedjorna med den fullständiga informationen enbart hos de skattskyldiga själva, men samtidigt att risken att uppgifter manipuleras minskar ytterligare.
Är det externa tredje parter som håller verifikationerna är ett krav att dessa har rutiner för att säkerställa vilka restauranger de håller verifikationer åt. Det vill säga det räcker med att det inte finns risk för flera olika register för samma restaurang. Ägandet av lösningarna kan därför vara helt privat. Restaurangerna behöver heller inte dela med sig av personalliggarna till registerhållarna, enbart krypterade verifikat.

**ID**
Registreras hasharna på en hemsida eller. Hos en myndighet behövs ingen id-hantering.
Det är möjligt för restauranger att göra flera registreringar av verifikationer samma dag. Till exempel om någon blir sjuk och en ersättare sätts in. Minst en registrering per arbetsdag behöver dock ske. För att säkerställa att endast en registrering per företag sker behövs ett ID som är kopplat till det specifika företaget. Detta ID kan överenskommas med företaget som samlar registreringarna, t.ex. kan en publik nyckel skickas från applikationen medan den privata nyckeln behålls. Stjäl någon nyckeln är det enkelt att göra en ny.

**Lagring**
Lagring av originalfilerna måste ske digitalt, men behöver endast ligga lokalt. Personalliggaren kan göras på papper men fotot som tas av liggaren behöver vara digitalt. Detta foto är också det som behöver sparas. I detta fall kan en översyn av bevaranderegelrna av personalliggaren behöva göras.

**Digitalt först**
När det gäller analoga personalliggare finns det formkrav och Skatteverket säljer personalliggare i papper. När det gäller digitala personalliggare finns däremot inte några formkrav och Skatteverket tillhandahåller inga lösningar. Det är valfritt vilket digitalt format som används. Det är olyckligt.

Ett förslag är därför att det upprättas formkrav på digitala personalliggare, dvs. någon form av lagstiftning eller regelverk. I detta fall syftar lagstiftningen till att säkerställa att det är rätt version av personalliggaren. Det intressanta är inte om det finns flera exemplar, om det är ett ursprungsutförande eller om det finns flera innehavare av personalliggaren. Lagstiftaren bör säkerställa att personalliggaren är den senaste versionen och att tidigare versioner kan kontrolleras i efterhand.

Det kan ske genom:

1. En verifikation av aktuell version sparas tillgänglig för allmänheten t.ex. på företagets hemsida
2. En verifikation av aktuell version skickas till en myndighet
3. En verifikation av aktuell version skickas till en tredje part som håller dessa i en icke-manipulerbar serie som är externt verifierbar (ett Merkleträd).

Ett förslag är att Skatteverket eller en annan myndighet får i uppdrag att ta fram en open-SOUrce mjukvara eller annan tjänst som företagen kan använda sig av gärna utan kostnad. Det ligger i lagstiftarens intresse att digitala alternativ som de som föreslås väljs och de kan därför vara gratis.

# Bilaga 1: Tekniska förklaringar

För att förstå de lösningar som beskrivs i rapporten är det några tekniska begrepp som är värdefulla att känna till. Dessa beskrivs  översiktligt nedan. För mer djupgående analys av tekniken är det lämpligt att utgå ifrån begreppen nedan, PKI, certificate authourity, merkle tree, hash osv och söka sig vidare på internet. En välskriven bok om kryptering är The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography av Simon Singh. Det är med andra ord ett förslag och en rekommendation att börja med att förstå kryptering och först därefter blockkedjan. Något mer utförliga beskrivningar av blockkedjetekniken och dess tillämpningar från svenska projekt finns här.
https://chromaway.com/papers/blockchain_landregistry_report_2017.Pdf
https://www.Kairosfuture.com/se/publikationer/rapporter/blockchain-use-cases-for-food-tracking-and-control/

## Privata och publika nycklar

Traditionell kryptering har byggt på tanken att det finns ett dokument, t.ex. ett avtal, som krypteras med en krypteringsnyckel. Resultatet blir ett oidentifierbart meddelande. Den som på ett eller annat sätt får tag på krypteringsnyckeln, eller knäcker koden, kan återskapa ursprungsmeddelandet. Denna krypteringsteknik kallas synkron. Den som har kunskap om krypteringsnyckeln kan dekryptera meddelandet.

Privata och publika nycklar är ett vanligt sätt att generera koder med ytterligare en finess. Vi kan veta att någon har en krypteringsnyckel – utan att visa upp den för oss. Den som krypterar har då inte samma krypteringsnyckel som den som dekrypterar. Denna teknik kallas asynkron och har revolutionerat användandet av digital teknik, till exempel internet. I

väldigt många sammanhang i den digitala världen vill vi veta vem som agerar på andra sidan nätverket, någon form av elektronisk identifiering, eid, behövs oavsett om det är ett internt nätverk eller internet.

Privata och publika nycklar är en lösning på det problemet. Den som ska identifiera sig har då tillgång till en privat nyckel, dvs. en kod med siffror och bokstäver. Till den privata nyckeln hör en speciell publik nyckel. Den publika nyckeln kan delas ut fritt, till exempel på internet. Om Astrid vill identifiera sig kan Bertil veta att det är just Astrid som skrivit ett meddelande, gjort en signatur på ett dokument, eller liknande. Bertil vet det eftersom ett meddelande som krypteras med den privata nyckeln kan dekrypteras med den tillhörande publika nyckeln. Med andra ord kan Bertil dekryptera meddelandet med den publika nyckeln. Om dekrypteringen är lyckad vet han att det måste ha varit en person med tillgång till Astrids privata nyckel som har krypterat meddelandet – i annat fall skulle det inte gå att dekryptera med Astrids publika nyckel. Tekniken fungerar också åt andra hållet, dvs. Bertil kan kryptera ett meddelande med Astrids publika nyckel – och bara Astrid kan läsa det med den privata nyckeln. Bertil kan däremot inte dekryptera sitt eget meddelande, trots att han gjorde krypteringen med Astrids privata nyckel.

Eftersom det är lätt att generera nya privata och publika nycklar föreslår vi den tekniken i några av lösningarna i rapporten.

## Certificate Authority, CA

Ett problem kvarstår emellertid i exemplet ovan. Hur vet Bertil att den publika nyckeln han kan få tillgång till verkligen tillhör Astrid? En annan person, vi kan kalla honom Edvin, kanske har lagt ut en publik nyckel och påstår att det är Astrids? För att garantera att den publika nyckeln tillhör Astrid finns en certificate authority, ofta kallad CA. Denne har till upp-

gift att hålla ordning på vilka publika nycklar som tillhör vilken individ. Observera att CA:n inte behöver kunna Astrids privata nyckel. CA:n kan däremot påstå att en annan nyckel är Astrids och därmed lura Bertil. Om någon hackar CA:n är det därför ett stort problem eftersom denne kan påstå att alla andra har felaktiga nycklar. Säkerheten kopplad till CA:n är därför central. Den infrastruktur som omfattar privata och publika nycklar, CA m.m. kallas ibland public key infrastructure (PKI).

I Sverige är det vanligast med identifiering med mobilt Bank-ID, och företaget Finansiell ID-teknik är CA för dessa eID. Det finns emellertid flera legitimationer som kan användas av privatpersoner för att identifiera sig, dvs. de har lagstöd som e-legitimationer, exempelvis e-legitimation från Telia. Nu finns även ett myndighetsgodkännande som kan ges i form av att bli godkänd som svensk e-legitimation, vilket Freja eID blivit.

Per den 29 september 2018 är EIDAS, EU:s lagstiftning för e-legitimationer och betrodda tjänster bindande för EU:s medlemsländer. Detta medför att alla e-legitimationer som blivit godkända enligt EIDAS kommer att behöva accepteras i alla länder inom EU som godkända e-legitimationer. För att det ska bli praktiskt möjligt att integrera tiotals, kanske hundratals godkända ID-lösningar, har EIDAS ålagt varje land att inrätta en form av id-växling. Den nyinrättade myndigheten för digital förvaltning, DIGG, har fått ansvar för e-Legitimationsnämnden och har också byggt denna typ av växlingstjänst. I växlingstjänsten ingår två delar, en för utgående eID dvs. identifiering som gjorts med ett svenskt eID och ska användas i ett annat land. Den andra tjänsten finns för att inhämta ett godkännande av eID från ett annat land som använder en svensk tjänst. I praktiken är arbetet med att sätta upp dessa växlingstjänster inte alls färdigt i den utsträckning eu-lagstiftningen egentligen kräver. Ett tiotal medlemsländer verkar dock vara på god väg med att upprätta systemet.

Utöver de funktioner där det redan finns ansvariga myndigheter finns det ett värde av att kunna säkerställa mer information om individers roller och befogenheter.

Detta område omfattar frågor som behörigheter, befogenheter, ombud, fullmakter, ställningsfullmakter och kyc (know your customer) av individer. I denna rapport har vi tagit fram ett förslag på lösning för fullmakter. Det finns ett antal andra pågående arbeten kring dessa frågor utöver EIDAS. Några exempel är:

- Frågan om behörigheter hanteras vanligen av dagens it-system för respektive organisation.

- Frågan om kyc är något som är särskilt värdefullt för banker och kreditinstitut. Där finns ett pågående projekt mellan de nordiska bankerna med blockkedjeteknik som stöd för att upprätta detta.

- Hantering av ombud är en fråga som nu ska utredas i ett myndighetsgemensamt projekt.

- I mars 2019 ska en utredning presenteras som ska utreda frågan om ett nytt svenskt myndighetsägt ID som väntas ersätta körkorten, men det är alltså tillsvidare inte ett eid

- Det finns ett nordiskt samarbete kring ID, NOBID.

## Underskrifter och betrodda tjänster

EIDAS reglerar förutom eID även betrodda tjänster eller digitala signaturer. Förutom att göra en identifiering av en person så behövs det ibland ett bevis på att en person blivit identifierad, skrivit under och att det beviset kan knytas till ett dokument, i praktiken en digital fil. För detta syfte behövs en signeringstjänst.

## En hash, ett digitalt bevis

Den kanske viktigaste tekniska komponenten i det som idag kallas blockkedjeteknik är möjligheten att skapa unika verifikationskoder av digitala filer, dvs. foton, transaktionslistor, register, avtal, videofilmer, patent m.m. Verifikationer kan skapas av allt som går att lagra som en digital fil. Verifikationerna gör det möjligt att fastställa att digitala filer inte har ändrats, en funktion som är oerhört central. Detta är viktigt eftersom det inte finns några tillförlitliga sätt att veta om en digitalfil har ändrats, med mindre än att krypteringsteknik används som innehavaren av den digitala filen inte själv kontrollerar.

Med hjälp av en avancerad ”fingeravtrycksalgoritm” kan vilken digital fil som helst få en unik verifikationskod. Tekniskt kallas detta för en kryptografisk hash. Ett exempel på en algoritm som skapar kryptografiska hashar är sha256. Denna algoritm tar alla ettor och nollor som beskriver ett digitalt dokument och räknar om dessa enligt ett bestämt, men oförutsägbart mönster. Oberoende av vilken datamängd ursprungsfilen har är resultatet alltid en mindre kod som alltid har samma format, dvs. antal tecken.

Hashen uppfanns redan på 50-talet men användningen har tagit fart på senare tid. Den allra viktigaste egenskapen hos en hash är att den inte kan backas. På samma sätt som det inte går att återskapa en människa från den begränsade information som finns i ett fingeravtryck går det inte att återskapa en digital fil från en hash. Till skillnad från den krypteringsteknik som i flera tusen år varit den enda kända är det alltså inte möjligt ens för den som känner till krypteringsalgoritmen att förstå hur ursprungsfilen ser ut. Jämfört med synkron och asynkron kryptering finns det för hashar ingen dekryptering alls. Det går inte att återskapa ursprungsfilen.

Hashen kan bestå av 64 tecken, vilket är alldeles för lite information för att förstå hur en bokföringsfil med en årsredovisning ser ut. Om bokföringsfilen omfattar flera megabyte kan det inte återskapas med ett fåtal siffror och bokstäver.

Antalet kombinationer hashar är samtidigt ett större tal än en etta med 64 nollor efter (eftersom det innehåller bokstäver också). Sannolikheten att två hashar av en tillfällighet blir likadana är därför i praktiken noll. Det betyder att den som har ursprungsfilen kan återskapa hashen, dvs. fingeravtrycket, men ingen annan. Samtidigt kan ägaren av filen inte göra en ändring utan att det märks för någon som har den ursprungliga hashen.

Denna egenskap är helt avgörande för de lösningar som beskrivs i denna rapport. Fullmaktsgivaren och fullmaktstagaren kan exempelvis dela med sig av en hash avseende sin fullmakt utan att avslöja innehållet i fullmakten. Givet att innehållet i ett digitalt kvitto är tillräckligt omfattande går det inte att utifrån en hash som ligger i ett kvittoregister förstå kvittots innehåll. Möjligheten att vara anonym är avgörande i dessa fall.

## Merkleträd

Låt oss anta att en fullmaktstagare och fullmaktsgivare vill att det ska finnas ett bevis för fullmaktens innehåll och att detta inte är manipulerat. De kan då låta en tredje part förvara en hash av fullmakten. Nackdelen med detta är naturligtvis att denna tredje part, eller någon anställd hos denna kan manipulera hashen. För att eliminera detta problem läggs hasharna in i en ordningsföljd där varje hash som ska läggas till utgör en del i en ny hash. I exemplet med fullmakten tar vi den första hashen nr 1 av fullmakt nr 1. När det kommer en ny hash av fullmakt nr 2 tar vi dessa två

hashar 1 och 2 och gör en ny fil och gör en ”kombinationshash” hash 1+2 av den nya filen. När det kommer en tredje fullmakt tar vi ”kombinationshashen” slår ihop den med den nya fullmaktshashen nr 3 och skapar en ny ”kombinationshash” (1+2)+3.

Resultatet av detta förfarande leder till att den sista kombinationshashen låser all underliggande information. Ändras någon av fullmakterna 1, 2 eller 3 kommer denna hash och kombinationshasharna inte längre att stämma.

Eftersom alla nya hashar som kommer in i Merkleträdet använder den sista kombinationshashen får vi dessutom en tidsordning för all information. Vi vet att den sista fullmakten nr 3 kommer att få sin verifikation sammanslagen med en kombinationshash som innehåller hänvisningar till alla tidigare fullmakter. Hash 1 och 2 måste därför ha registrerats före hash nr 3.

Tidsordningen eller tidsstämplingen som den ibland kallas, är värdefull eftersom vi kan veta vilken fullmakt och vilken information om fullmakten som är den senaste. I fallet med personalliggare är det också värdefullt att veta när personalliggarna registrerats. Görs det en uppdatering vet vi vilken version som gäller. Har det gjorts registreringar av personalliggare varje dag den senaste månaden är detta lätt att kontrollera. Det är heller inte möjligt för den som tillhandahåller Merkleträdet att göra ändringar, givet att kombinationshasharna publiceras, åtminstone en gång per dag till exempel. En av de mest använda aktörerna på denna arena är guardtime som samarbetar med de estländska myndigheterna, usas försvarsdepartement, ericsson, verizon etc. De publicerar sin kombinationshash, också kallad tophash, i financial times en gång i månaden.

## Blockkedja

Det som vanligtvis avses med en blockkedja är att Merkleträdet också ska vara säkert för manipulation och inte vara beroende av en enda databas. Ytterligare ett skäl är att det kan finnas en möjlighet att ägaren av Merkleträdet prioriterar inkommande hashar för egen vinning, något som är väldigt värdefullt på finansmarknaderna. Om någon fick en möjlighet att registrera sin handel med aktier före andra skulle det vara oerhört värdefullt. Givet att kombinationshashen hålls hemlig under ett par dagar kan det också vara möjligt att göra ett nytt träd och stoppa in nya hashar och därmed göra en ny tidsordning mm. För att undvika detta problem kan det därför vara viktigt att ordna databaserna i en distribuerad struktur där fler aktörer kan säkra ordningsföljd av datan, att den följer uppsatta regler, att den inte förstörs osv. Det innebär att det finns flera databaser som alla innehåller samma Merkleträd. Olika system för blockkedjor använder sig av särskilda algoritmer för att säkerställa att alla databaser är synkroniserade, dessa algoritmer kallas konsensusalgoritmer. Genom att låta flera aktörer ha en synkroniserad databas med Merkleträdet ökar förtroendet för den.

Inledningsvis byggdes blockkedjeteknik eller ”distributed ledger technologies” för att efterlikna publika blockkedjor, i första hand Bitcoin. Tanken var då att alla rättigheter skulle vara ilka för alla noder. I praktiken har detta frångåtts och det blir vanligare att låta noder få olika rättigheter. Förslag på ändringar av mjukvara, mottagande av inkommande transaktioner, validering är exempel på vad som kan vara förbehållet en eller ett fåtal noder. Eftersom syftet i grunden handlar om att skapa förtroende för processer och motparter är det inte nödvändigt att i alla system låta alla rättigheter vara lika, varken tekniskt eller juridiskt. Det är en avvägning mellan kostnad, risk, enkelhet med mera.

**Publika blockkedjor**

De blockkedjor som framför allt förknippas med kryptovalutor kallas publika blockkedjor. Denna teknik används inte i de förslag som beskrivs i denna rapport. Ett par problem som ibland lyfts fram med publika blockkedjor är därför inte relevanta. Exempel på problem som ofta tas upp i samband med blockkedjor, men som alltså inte är aktuella i våra exempel i denna rapport är t.ex. :

1. Energiåtgång – publika blockkedjor använder ofta en teknik som kallas proof of work. Den tekniken kräver stora mängder energi.

2. Skalbarhet – publika blockkedjor har kapacitetsbegränsningar. Det går inte att registrera för stora mängder data i dessa.

3. Transaktionshastighet – publika blockkedjor har svårigheter med snabbheten att registrera hashar och annan information.

4. Radera uppgifter – i publika blockkedjor går det inte att radera gammal information. Det beror på att blockkedjor som används till kryptovalutor behöver vara tydliga med hur många kryptovalutor som skapats sedan blockkedjan startade. Det finns juridiska överväganden om möjligheten att använda blockkedjor med hänsyn till exempelvis GDPR, exempelvis denna från Europaparlamentet.

https://www.europarl.Europa.eu/regdata/etudes/stud/2019/634445/eprs_stu(2019)634445_en.pdf

Eftersom utredningen är gjort utifrån den strikta beskrivningen av en blockkedja som projektet sällan arbetar med är det viktigt att vara försiktig med att dra slutsatser av dessa

juridiska slutsatser. Mer relevant kan vara juridiska överväganden för annan teknik såsom X-road.

5. Stölder och förluster – stulna eller borttappade privata nycklar kan innebära att stora belopp går förlorade. Det är möjligt att förlora privata nycklar även i de beskrivna lösningarna, men förlusterna är i dessa fall små eller obefintliga. Ibland talas det om ”self sovereign identities”. Dessa är inte nödvändiga för att lösningarna som beskrivs ska fungera.

6. Parallella sanningar – i publika blockkedjor kan olika delar av nätverket hamna efter i kunskap om vad som är den aktuella statusen. Det kan därför uppstå två parallella sanningar. Dessa kallas ”fork", gaffel. Detta kan i praktiken inte hända i privata blockkedjor eftersom antalet medverkande noder är känt och begränsat.

7. SSI, self sovereign identities – i diskussioner om blockkedjor framförs ibland ett behov av self sovereign identities. Detta behov kan finnas för publika blockkedjor samt i vissa privata blockkedjor. Eftersom lösningar för detta endast är i sin linda är det tillsvidare ingenting projektet vill göra sig beroende av. Ingen av lösningarna som föreslås behöver därför dessa.

Blockkedjan har beskrivits som en trustless-teknik, dvs. en teknik där du inte behöver lita på andra. I praktiken har detta sitt ursprung i publika blockkedjor som Bitcoin eller Ethereum där en enskild individ eller organisation inte kan ändra registreringar som gjorts av systemet. Om du har sålt dina Bitcoin finns det inget sätt att ta tillbaka pengarna eller ta bort registreringen. Det kan göras en ny transaktion men den gamla kan inte göras ogjord. Den som kontrollerar den privata nyckeln som har tillgång till respektive Bitcoin kan spendera dessa och när det är gjort är det någon

annan som har kontrollen. I slutändan betyder det att var och en måste lita på sig själv när det gäller förvaringen av de privata nycklarna, vilket är riskabelt. Få människor vill att deras pension går förlorad bara för att de tappat bort en personlig kod, datorns hårddisk blir hackad eller går sönder. I fallet med Bitcoin använder därför de flesta ett förvaringsinstitut, någon organisation som tar ansvaret för att lagra dessa privata nycklar, vilka i sin tur kontrollerar Bitcoin. När ett förvaringsinstitut hackas av någon på insidan eller utsidan, vilket har hänt, vill ägarna ha ett system för tvister för att få tillbaka sina pengar. Detta gör att de rättmätiga ägarna till kryptovalutor har ett stort behov av någon form av försäkring, brottsbekämpning eller annat skydd, vilket, åtminstone idag, förutsätter institutioner i den övriga världen.

# Referenslista

1 https://github.com/I§team1337/digital-receipts
2 https://www.cbsnews.com/news/amazons-jeff-bezos-looks-to-the-future/
3 https://www.svenskhandel.se/nyhetscenter/nyheter/2018/standard-for-elektroniska-kvitton-framtagen/
4 https://www.lantmateriet.se/contentassets/50c7b8feec4744e5a0fa2ffaf0ea07ec/519-2018_2889-bilaga-2-ekonomisk-nytta-rattelse-190514.pdf
5 https://www.DIGG.Se/globalassets/slutrapport---uppdrag-om-saker-och-effektiv-tillgang-till-grunddata.Pdf

FAR är branschorganisationen för revisorer, redovisningskonsulter, skatterådgivare, lönekonsulter och specialister. FAR bidrar till branschens utveckling genom rekommendationer, utbildning och remissverksamhet. FAR arrangerar utbildningar, ger ut böcker, regelverk och digitala tjänsten FAR online, samt två tidningar - Balans och Resultat. FAR:s uppdrag är att hjälpa branschen att göra nytta för näringsliv och samhälle. Detta sker främst genom: Utveckling av god yrkessed, Kompetensutveckling, Opinionsbildning .Våra medlemmar, cirka 5 100, är auktoriserade och godkända revisorer, auktoriserade redovisningskonsulter, skatterådgivare, auktoriserade lönekonsulter och andra specialister, exempelvis inom hållbarhetsredovisning.

Skatteverket är till för alla i samhället. Vi vill att det ska vara lätt att göra rätt – till exempel när du betalar skatt, säljer eller köper bostad, startar och driver företag, flyttar eller gifter dig. Vårt uppdrag från regeringen består av tre delar: Bidra till ett väl fungerande samhälle för privatpersoner och företag, Bidra till att säkra finansieringen av den offentliga sektorn, Motverka brottslighet. Det innebär att vi arbetar med skatter, folkbokföring, äktenskapsregistret, fastighetstaxering, bouppteckningar, id-kort och att utreda skattebrott. Vi är också borgenär åt staten. Vi har drygt 10 000 medarbetare och har verksamhet i hela landet.

Bolagsverket ska skapa förutsättningar för ett näringsliv där man kan lita på varandra. Kärnan i vårt uppdrag är att registrera och tillgängliggöra företagsinformation, som skapar värde för samhället. Bolagsverket har cirka 550 anställda och ligger i Sundsvall.

Kairos Future är ett internationellt konsult- och analysföretag som hjälper företag att förstå och forma sin framtid. Genom trend- och omvärldsanalys, innovation, strategi och mjukvarustöd för AI-driven analys, omvärldsbevakning och innovation, hjälper vi våra kunder att omsätta de stora sammanhangen till konkret handling. Kairos Future grundades 1993, vårt huvudkontor finns i Stockholm och vi har egna kontor eller samarbetspartners över hela världen.

Kairos Future AB | P.O. Box 804 | S-101 36 Stockholm | Sweden
Phone: +46 (0) 8-545 225 00 | www.kairosfuture.com