Svenska Bankföreningen
Swedish Bankers' Association

REMISSYTTRANDE
Vår referens: 2019/05/001
Er referens: Ju2019/01281/L4

2019-08-30

Justitiedepartementet
ju.remissvar@regeringskansliet.se
ju-L4@regeringskansliet.se

Bankföreningens synpunkter på betänkandet *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14)

Svenska Bankföreningen har beretts tillfälle att yttra sig över betänkandet *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14) och vill med anledning av det framföra ett antal synpunkter.

Bankföreningen är en branschorganisation för svenska banker och utländska banker med filial i Sverige och har till ändamål att främja medlemmarnas gemensamma intressen genom att bland annat verka för väl fungerande och konkurrensneutrala regelverk såväl nationellt som internationellt. En stabil och säker finansiell infrastruktur utgör en grundförutsättning för säkra och effektiva betalningslösningar men också en möjlighet för kunden att identifiera sig i samband med olika transaktioner och avtal. Alla konton och alla avtal i en bank bygger på fungerande identifiering.

Bankföreningen anser att utredningen är grundlig och genomarbetad.

Bankföreningen är positiv till utredningens slutsatser och rekommendationer som berör föreningens medlemmar som banker, som ägare av samhällsviktig finansiell infrastruktur (Finansiell ID-Teknik BID AB som äger, förvaltar och utvecklar BankID) och som arbetsgivare för tusentals banktjänstemän på ca 1 400 bankkontor runt om i landet.

Förslagen stärker utfärdandet av svenska identitetshandlingar, konsumentskyddet, banksäkerheten och den svenska välfärdsstatens förmåga att stå emot identitetsrelaterad brottlighet. Förslagen kommer också att skapa ännu bättre förutsättningar för förlitande parter (banker, företag och myndigheter) att distribuera sina tjänster digitalt. Förslagen möjliggör också för banker, postombud m fl. att göra en identitetskontroll med högre tillförlitlighet av den fysiska handlingen än vad situationen är i dag.

Besök (Visit):
Blasieholmsgatan 4B
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

t: +46 (0)8 453 44 00

e: info@swedishbankers.se
www.swedishbankers.se

Det finns stora ambitioner att öka digitaliseringstakten i Sverige. Följer man debatten kan man lätt få intrycket att digitalisering på något sätt kommer att kringgå behovet av fysisk identifiering. Bankföreningens uppfattning är att fysisk identifiering och fysiska identitetshandlingar kommer att finnas kvar under överskådlig tid och snarare blir än viktigare i takt med ökad digitalisering och ökad e-handel.

Som läget är idag i Sverige kan inte bankerna förlita sig på den identifiering som staten gör. Bankerna behöver i sin identifieringskontroll vidta ett antal säkerhetshöjande åtgärder som att följa kontrollprocessen i handboken *De 7 Stegen*, att manuellt kontrollera id-handlingen mot utfärdaren via telefon/internet och som ytterligare valbar step-up metod använda scanner-utrustning som läser av id-handlingens optiska säkerhetsdetaljer. Bankernas identitetskontroller bygger på att staten garanterar identiteten och att utfärdaren tillhandahåller verktyg för att kontrollera id-handlingen. Det är mot bakgrund av bland annat dessa brister som utredningens slutsatser och bedömningar är välkomna.

Synpunkterna är indelade i två delar: väsentliga synpunkter och fyra st. bilagor som Justitiedepartementet bör beakta i utvecklingen av lagförslaget.

Bilaga A redogör för de åtgärder bankerna har vidtagit själva och genom BankID och Swish med anledning av de vishing/kundtjänstbedrägerier som till ganska nyligen drabbade svenska konsumenter på bred front. Syftet med redogörelsen är att förse Justitiedepartementet med en inblick i vikten av att även beakta den andra säkerhetsutmaningen med e-legitimationer (att innehavaren vet och förstår värdet av e-legitimationen och vet hur man använder den) och inte endast den första säkerhetsutmaningen (att staten utfärdar fysiska id-handlingar som därefter utfärdare av e-legitimationer kan förlita sig på i sin utfärdandeprocess vilket är det område som ID-kortsutredningen har tittat närmare på). En statlig e-legitimation medför att staten kan tillhandahålla samma information om e-legitimationen till alla medborgare vilket bankerna inte kan på samma sätt. Detta skapar utökade möjligheter för staten att på ett enhetligt och effektivt sätt informera användarna om hur de bäst skyddar sig mot bedrägerier.

Bilaga B visar hur en identitetskontroll på ett bankkontor går till idag samt hur utredningens förslag kan stärka identitetskontrollen. Processen är allmängiltig för alla verksamhetsutövare (banker, postombud, handel m fl.) som vill göra en identitetskontroll.

Bilaga C resonerar om skillnaderna i Bankföreningens självreglering av utfärdare och id-handlingar i Sverige (sammanfattade i handboken *De 7 Stegen*) och Finansinspektionens *föreskrifter om åtgärder mot penningtvätt och finansiering av terrorism FFFS 2017:11*.

Bilaga D består av Bankföreningens remissyttrande för slutbetänkandet *Reboot – omstart för den digitala förvaltningen* (SOU 2017:114) som bifogas för kännedom eftersom det arbetet (se punkterna 1–9) har vissa beröringspunkter med betänkandet *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14).

Väsentliga synpunkter

1. **Att minska antalet utfärdare är den mest prioriterade frågan**

   För att kunna minska antalet identitetshandlingar som butik- och bankanställda ska kontrollera måste Sverige begränsa antalet utfärdare av identitetshandlingar. En minskning av antal utfärdare leder till en minskning av antal id-handlingar. Det ökar möjligheten för butik- och bankanställda att känna igen, granska och kontrollera id-handlingen. Bankföreningens bedömning är att det är den enskilt viktigaste frågan på identitetsområdet i Sverige i dag och den fråga som har störst effekt.

   Att fastställa identiteten är den centrala frågan – inte vilka behörigheter, konton mm som den identiteten kan ha. En behörighet kan t ex vara rätten att framföra ett fordon. En identitet kan vara kontohavare som kan utföra transaktioner på ett konto men med identiteten följer inte per automatik ett konto.

   Bankerna har bedömt frågan att minska antalet utfärdare som så angelägen att de själva under ID-kortsutredningens gång har fattat beslut om att upphöra med att utfärda SIS-kort. Bankerna har därmed redan anpassat riktningen i linje med utredningens direktiv och slutsatser och Bankföreningen förväntar sig att regeringen driver på för att genomföra de lagstiftningsförslag som återfinns i betänkandet.

   Utredningens uppdrag är bland annat att föreslå hur antalet utfärdare kan begränsas. För att snabbare få en enhetlig hantering av identitet och identifiering i Sverige anser Bankföreningen att Skatteverkets id-kort för folkbokförda i Sverige bör ha samma slutdatum på giltighetstiden som de övergångsbestämmelser som föreslås för körkort och SIS-kort, dvs ett år efter den 1 januari 2022. Annars riskerar förändringen att glida onödigt mycket i tiden, ända fram till 2027.

2. **Samma säkerhetsnivå för samtliga identitetshandlingar**

   Problemet är *egentligen* inte att Sverige har många utfärdare. Problemet ligger i att samtliga utfärdare har olika processer och olika krav för att utfärda identitetshandlingar samtidigt som de förlitar sig på varandra och att det

saknas en gemensam infrastruktur för kontroll. Det resulterar i att den utfärdare som har den lägsta säkerhetsnivån sätter nivån för alla utfärdare. Av den anledningen har Bankföreningen efterfrågat att en nationell gemensam utfärdandeprocess av id-handlingar införs. Om en sådan inte kan införas, oavsett anledning, bör antal utfärdare minskas.

Eftersom det inte är troligt att Polisen, Transportstyrelsen, Skatteverket och bankerna (SIS) kommer att kunna enas om ett gemensamt regelverk för ansökan, produktion och utfärdande av id-handlingar (p g a att myndigheterna/utfärdarna har olika uppdrag, lagstiftning och avtal med tillverkare mm) så är den mest lämpliga och kostnadseffektiva vägen framåt att antalet utfärdare minskas.

Det är alltså angeläget att det ska vara samma säkerhetsnivå för samtliga id-handlingar som utfärdas till landets befolkning. Sverige bör därför välja den utfärdare som har den mest robusta utfärdandeprocessen. Bankföreningen gör samma bedömning som den utredningen gör dvs att utfärdande av de statliga identitetshandlingarna ska samlas hos Polismyndigheten. Den statliga identitetshandlingen bör därför omgärdas av samma begränsningar som regelverket för pass (kap. 6.2.1), till exempel att antalet pass som kan beviljas till en person sedan 2016 begränsas till tre vanliga pass under en femårsperiod.

3. Utfärdande av de statliga identitetshandlingarna ska samlas hos Polismyndigheten

Av flera skäl är det positivt att utfärdandeprocessen stärks och samlas hos Polismyndigheten:

- I dag kan inte bankerna förlita sig på den identifiering som staten (Skatteverket, Polisen, Transportstyrelen) gör. Anledningen till det är att identitetskedjan från ansökan, tillverkning, utlämnande och den för förlitade parter så viktiga verifieringen av identitetshandlingen mot utfärdaren inte är tillräckligt robust och utfärdarnas skiftande uppdrag. Beslutsstödet som utfärdarna av identitetshandlingar tillhandahåller verksamhetsutövare är dessutom begränsat. En anledning för bankerna är ansvaret som kommer med att vara Sveriges i särklass största utfärdare av e-legitimationer (BankID). Idag har åtta miljoner svenskar ett BankID som möjliggör legitimering och underskrift mot cirka 4 000 förlitande parter. 2018 gjordes cirka 3 miljarder transaktioner i BankID-infrastrukturen vilket är cirka 100 transaktioner per sekund. Det är alltså väldigt många intressenter i det svenska samhället som förlitar sig på den identifiering som banken gör.

- I framtiden skulle bankerna kunna förlita sig på den identifiering som staten gör. En förutsättning för det är att antalet utfärdare av fysiska identitetshandlingar minskas och att utfärdandeprocessen stärks enligt utredningens förslag. Polismyndigheten behöver också fortsätta att tillhandahålla en funktion för kontroll av utfärdade identitetshandlingar online liknande den som lanserades 2018.

  Om staten utfärdar en e-legitimation på den statliga fysiska id-handlingen så stärks identifieringen högst väsentligt.

4. Bankernas kontroller kommer inte att minska, snarare tvärtom

Att enkelt, snabbt och med god kvalitet kunna kontrollera en identitetshandlings äkthet är en förutsättning för att kunna minska identitetsrelaterad brottslighet. För medarbetarna i bankernas kontorsrörelser är det idag svårt att hålla reda på alla de olika versioner som finns (sammanfattade i handboken *De 7 Stegen*) och kunna göra en bra identitetskontroll med god kvalitet med det begränsade beslutsstöd som utfärdarna tillhandahåller verksamhetsutövare. De förfalskningar som bankerna tar är väldigt välgjorda.

Den största förändringen på många år när det gäller giltighetskontroll av identitetshandlingar i Sverige skedde 2017 då Polismyndigheten utvecklade en e-tjänst för giltighetskontroll av svenska pass och nationellt ID-kort. E-tjänsten lanserades i januari 2018 och förser banker och andra med en möjlighet att kontrollera Polisens identitetshandlingar online: https://etjanster.polisen.se/egid/giltighetskontroll/

E-tjänsten innebär stora fördelar för flera parter i samhället:

- För medborgarna: konsumentskyddet stärks, risken för identitetsstöld och identitetsrelaterade bedrägerier minskar och tillgängligheten till Polisens växel (114 14) ökar, eftersom banker och andra inte längre behöver ringa dit för att verifiera id-handlingar.

- För Polismyndigheten: personalresurser frigörs.

- För banken: processen att validera uppgifterna på id-handlingen snabbas upp och säkerheten stärks. Kontroll via växeln tog, i bästa fall några minuter medan kontroll via e-tjänsten bara tar några sekunder. Bankpersonalen är mycket nöjda med Polismyndighetens utvecklade e-tjänst.

Statistiken visade att antal samtal från bankerna till Polisens växelpersonal hade ökat stadigt under ett antal år. År 2017 (innan e-tjänsten fanns) fick Polisens växelpersonal ta emot 186 000 telefonsamtal från bankerna. Det finns ingenting som tyder på att bankernas kontroller (penningtvätt, kundkännedom, bedrägeriprevention, identitetsstöld mm) kommer att minska i omfattning, snarare tvärtom.

Om utredningens förslag blir verklighet kommer antal ID-kontroller från bankerna mot Polismyndigheten förmodligen att tiofaldigas 2022 jämfört med 2017. Den uppskattningen baseras på att det utfärdas drygt tre miljoner id-handlingar årligen i Sverige och att Polismyndigheten utfärdade 276 104 st. nationella id-kort 2018. Passet är otympligt att ha i plånboken och kommer inte att ha en e-legitimation. Därför är det rimligt att tro att över tiden kommer antal utfärdade statliga identitetshandlingar (motsvarande dagens nationellt id-kort) att väsentligt öka. Polismyndigheten bör därför redan nu överväga en back-up lösning till e-tjänsten. I ett läge där e-tjänsten fallerar är det inte hållbart att ha Polisens växel 114 14 som back-up lösning. Vid en sådan händelse skulle bankerna återigen börja ringa Polisens växel 114 14 och det skulle försämra allmänhetens möjligheter att komma i kontakt med Polisen högst väsentligt och det är inte önskvärt.

En annan inneboende utmaning med alla IT-system är utveckling, drift och förvaltning av dessa. Den 9 november 2018 informerade Polismyndigheten att Polisens system för hantering av pass och id-kort skulle migreras till en ny IT-miljö. Det skulle medföra att den e-tjänst som lanserades i januari 2018 – och som främst banker använder sig av för att kontrollera om Polisens utfärdade id-handlingar är giltiga eller inte – skulle ligga nere från klockan 20:00 torsdagen den 29 november till och med söndagen den 2 december klockan 23:59, dvs i drygt tre dygn. Att informera tre veckor innan en planerad förändring och utan en alternativ lösning på plats är för kort framförhållning. Det är dessutom inte ovanligt att migreringar till nya IT-miljöer inte förlöper friktionsfritt och förseningar är vanligt förekommande i projekt- och förändringsarbete p g a komplexitet. Ett längre avbrott för e-tjänsten skulle medföra stora konsekvenser för bankernas kundkontakter. Det är ytterligare ett argument för att Polismyndigheten bör öka robustheten och tillhandahålla alternativa lösningar för giltighetskontroll av sina utfärdade id-handlingar. Den 19 november informerade Polismyndigheten att de måste skjuta på uppgraderingen och det tidigare aviserade driftstoppet var då inte längre aktuellt.

Eftersom utredningens uppdrag består i att analysera hur verifieringen av äktheten och giltigheten kan förbättras anser Bankföreningen att en skyldighet för Polismyndigheten att tillhandahålla en funktion/verktyg för

kontroll av utfärdade identitetshandlingar för verksamhetsutövare att använda sig av (som den e-tjänst som lanserades 2018 eller liknande) bör skrivas in i lag eller förordning. Verktyget som Polismyndigheten bör tillhandahålla kan t ex vara en e-tjänst på en hemsida (som den e-tjänst som redan finns), en app eller ett API.

Utredningens förslag är att Polismyndigheten även ska överta utfärdandet av id-handlingar för folkbokförda. Om Polismyndigheten övertar det ansvaret från Skatteverket bör de även tillhandahålla en effektiv kontrollmöjlighet för verksamhetsutövare av de id-handlingarna (som den e-tjänst som lanserades 2018 eller liknande).

Ett ytterligare alternativ för Polismyndigheten att öka robustheten kan vara att undersöka möjligheterna att utveckla ett API mot RES-systemet. Ett API fungerar som en brygga för olika system att utbyta data mellan varandra. För bankerna är API:er idag ett väletablerat sätt att kommunicera bankerna emellan. Syftet och fördelen med ett API är att bägge parter (sändare och mottagare av data) är identifierade (part A vet alltså att part B är part B och vice versa). Det ansvaret är inte lika tydligt över internet. Ett API skulle kunna fungera som ordinarie lösning för förlitande parter medan den befintliga e-tjänsten då skulle kunna fungera som parallell (back-up) lösning. Ett sådant initiativ skapar effektivitetsvinster för både Polismyndigheten och de som vill göra en identitetskontroll.

5. API:er är bra för utfärdare, förlitande parter och konsumentskyddet

Ett API kan skapa bättre spårbarhet och högre säkerhet för Polismyndigheten. Ett API kan också möjliggöra för utfärdaren att tillhandahålla ytterligare information till verksamhetsutövare som kan minska risken för att banken utnyttjas för penningtvätt, förbättra bankernas möjlighet att kontrollera kunders identitet och stärka bedrägeripreventionsarbetet. Utfärdaren vet dessutom vilken data som har tillhandahållits till vilken part och vid vilken tidpunkt.

Svenska Institutet för Standarder (SIS) verkar i de internationella nätverken ISO och CEN som skapar standarder. SIS har skapat en teknisk standard för webbaserad giltighetskontroll av identitetshandlingar (teknisk specifikation SIS/TS 45). Standarden möjliggör verifiering av fysiska identitetshandlingar oberoende av utfärdare. Bankföreningen ser en potential i standarden eftersom den kan möjliggöra identitetskontroll mot fler utfärdare av fysiska identitetshandlingar inom till exempel EU (utanför denna utrednings scope). Standarden skulle också kunna fungera som ett automatiserat maskin-till-maskin API för maskinella/automatiska kontroller mot Polismyndighetens RES-system.

Bankföreningen och bankerna är därför intresserade av att fördjupa dialogen med Polismyndigheten avseende frågan om ett eventuellt API mot Polisens RES-system.

6. Staten bör utfärda en e-legitimation

Bankföreningen är positiv till att staten utfärdar en e-legitimation på den statliga fysiska id-handlingen av de skäl som utredningen framför. Det finns ett antal argument som talar för att staten bör utfärda en e-legitimation samt ett antal områden som Justitiedepartementet bör beakta i det fortsatta beredningsarbetet.

- Förslaget innebär att en stark gemensam utfärdandeprocess införs med nödvändig koppling mellan fysisk och digital identitet. Genom att en (1) myndighet ges ansvaret för den viktiga identifieringen garanteras säkerhet och kvalitet.

- En statlig e-legitimation ger bättre skydd för svenska identiteter, dvs ett stärkt konsumentskydd. E-legitimationen utfärdas på eIDAS nivå 4 vilket stärker tillförlitlighet och identifiering.

- En nationell infrastruktur för legitimering och underskrift innebär att staten kan tillhandahålla samma information om e-legitimationen till alla medborgare vilket bankerna inte kan på samma sätt. Detta ger exempelvis utökade möjligheter för staten att på ett enhetligt och effektivt sätt informera användarna om hur de bäst skyddar sig mot bedrägerier.

- Andra utfärdare av e-legitimationer (t ex BankID) bör kunna förlita sig på eIDAS4 (högsta tillitsnivå). En gemensam utfärdandeprocess medför också att säkerheten stärks och att konkurrensen mellan andra e-legitimationsutfärdare bör öka.

- Banker bör, om förslaget blir verklighet, i större utsträckning kunna förlita sig på statens identifiering, både fysiskt och elektroniskt.

- Infrastruktur mot utfärdaren (Polismyndigheten) för giltighetskontroll av fysiska identitetshandlingar online finns redan.

- Samhällets digitalisering gör det nödvändigt att landets befolkning ges tillgång till e-legitimationer. Svenska myndigheter använder sig mer och mer av BankID som identifieringsmetod och förlitar sig på att det

finns en e-legitimation. Samtidigt är det inte alla konsumenter som vill ha en privat e-legitimation och det finns en grupp som inte kan få ett BankID. Det är därför rimligt att staten utfärdar en e-legitimation.

- Hotbilden förändras löpande och motåtgärder behöver därför snabbt komma på plats. De eventuella riskerna med social engineering på tillitsnivå eIDAS4 behöver beaktas och konsekvenserna analyseras. Kan t ex konsumentskyddet påverkas? Staten behöver hänga med vid till exempel ett behov av förändring av säkerhetsdosa/kortläsare (som med utveckling av vishing/kundtjänstbedrägerier, se resonemang i bilaga A).

- Mobila enheter har blivit väldigt populära på kort tid och det är därför angeläget att utfärdaren beaktar den snabba tekniska utvecklingen. Tillverkare av datorer, läsplattor och smartphones släpper löpande nya modeller. Utvecklingen verkar gå mot mobila enheter med allt färre sladdingångar och stort fokus på appar vilket kan påverka en nationell eID-lösning som kan vara baserad på kort/kortläsare.

Givet de områden som bör beaktas är Bankföreningens sammanvägda bedömning att staten bör utfärda en e-legitimation på den statliga fysiska id-handlingen.

7. Området för obehörigt användande av e-legitimation bör bli föremål för en särskild utredning

E-legitimationer fyller en samhällsviktig funktion då ett stort antal intressenter måste kunna förlita sig på e-legitimationers legitimitet. Det förekommer att e-legitimationer likväl som fysiska legitimationer utfärdas och används av obehöriga personer, trots utfärdares avtalsvillkor och säkerhetsåtgärder. Det obehöriga användandet sker ofta på sätt som leder till ekonomisk skada för såväl ursprungliga innehavaren av e-legitimationen som den som förlitat sig på legitimationen. E-legitimationer kan användas som betalningsmedel, men även på andra sätt. Ett stort antal statliga och kommunala myndigheter, privata och statliga institut, föreningar och företag tar emot ansökningar och beviljar ersättning bidrag och lån. I detta sammanhang är e-legitimationer en urkund enligt brottsbalken 14:1.

De skador som kan uppstå vid obehörig användande av e-legitimation som urkund är därmed till exempel felaktigt utbetalda skattemedel i form av bidrag, utebliven återbetalning av statliga och privata lån samt andra felaktigt utbetalda benefika ersättningar. Vad gäller kontohavares ansvar för obehöriga transaktioner på konton gäller lag (2010:751) om betaltjänster. För avtal ingångna före den 1 maj 2018 gäller alltjämt lag (2010:738)

transaktioner med betalningsinstrument. Betaltjänstlagen reglerar vilket ansvar som åligger den som möjliggör en obehörig betalningstransaktion på ett grovt oaktsamt eller särskilt klandervärt sätt. Ansvaret sträcker sig som högst till det belopp som överförts från kontoinnehavarens konto genom obehöriga transaktioner. Det kan dock ifrågasättas om lagens tillämpningsområde sträcker sig utöver obehöriga betalningstransaktioner från ett konto. Området för obehörigt användande av e-legitimation bör bli föremål för en särskild utredning. I utredningen kan det vara lämpligt att utreda frågan om den enskildes ansvar för den skada som uppstått efter att denne hanterat uppgifter på ett klandervärt sätt och detta lett till att en e-legitimation använts med ett bedrägligt syfte.

8. **Tillgång till id-handlingens uppgifter får inte begränsas**

   Det är viktigt att tillgången till informationen (till exempel MRZ-koden, det digitala certifikatet (ett elektroniskt signerat dokument som innehåller uppgifterna som finns på kortet samt en större bild) i pass och nationellt id-kort mm) som förlitande parter kan använda sig för att verifiera uppgifterna på id-handlingen inte begränsas. Det är också viktigt att Sverige inom ICAO inte verkar för att begränsa de datapunkter som finns på handlingen som kan hjälpa förlitande parter att verifiera handlingen på.

9. **Vid återkallelse av e-legitimation p g a säkerhetsskäl bör Polismyndigheten informera bankerna om det kan förhindra finansiell brottslighet**

   Angående återkallelse (kap. 12.15) är utredningens förslag att e-legitimationen ska kunna återkallas om det är nödvändigt av säkerhetsskäl. Bankföreningen har i många år efterfrågat en fungerande informationsström från Polisen till bankerna och frågan aktualiseras återigen när det gäller återkallelse av e-legitimationen av säkerhetsskäl. Bankföreningen anser att Polismyndigheten ska vara skyldig att förse bankerna med information (om sådan finns) som kan hjälpa bankerna att förhindra finansiell brottslighet. Har Polismyndigheten kännedom om identiteter och e-legitimationer som återkallas på grund av misstanke om penningtvätt, bedrägerier, identitetsstöld, falska identiteter mm måste bankerna få den informationen från Polisen.

   Sådan information är väsentlig för bankernas arbete mot penningtvätt och finansiering av terrorism samt annan brottslighet och bildar underlag både för bankens verksamhetsövergripande riskbedömningar, riskbedömningen av den individuella kunden samt för utredning av misstänkta transaktioner och aktiviteter.

SVENSKA BANKFÖRENINGEN

Hans Lindberg

Peter Göransson

Bilaga A – om vishing/kundtjänstbedrägeri och e-legitimationer

Svenska konsumenter är utsatta för en mängd olika bedrägeriförsök. Det största hotet mot svenska konsumenter det senaste året har varit så kallade kundtjänstbedrägerier/vishing. Modus är en person som blir uppringd av en bedragare och itutad en hopkokt historia. Ofta framstår bedragaren som en ”trevlig banktjänsteman” eller en ”trevlig polis”. Bedragare är väldigt skickliga på att via olika former av social engineering-knep få det att framstå som att det är banken eller polisen som ringer. Syftet är att förmå kunden att tro på den påhittade historien för att i slutändan lämna ifrån sig koder från sin säkerhetsdosa eller att använda Mobilt BankID. Det allvarliga med kundtjänstbedrägerier/vishing är att konsumenter lämnar ifrån sig sina digitala identiteter vilket riskerar att skapa stora konsekvenser för individen. Bankerna har utmaningar med att nå fram med information som förändrar kunders beteende på internet. För Sveriges fortsatta digitaliseringssträvanden är det synnerligen viktigt att svenska folkets motståndskraft att stå emot den här typen av bedrägeriförsök stärks.

Frågan aktualiseras om Polismyndigheten, enligt utredningens förslag, ska utfärda en e-legitimation på högsta tillitsnivå, enligt eIDAS. Digitalisering av tjänster skapar mycket positivt i form av hållbarhet, tillgänglighet och effektivitetsvinster men det skapar också informationssäkerhetsrisker.

Om vishing/kundtjänstbedrägeri

Ett stort antal konsumenter har drabbats över hela landet. Utvecklingen av vishing nådde sin peak hösten 2018. Med anledning av brottsutvecklingen har bankerna vidtagit ett antal åtgärder i BankID och Swish och Polisen initierade en så kallad nationell särskild händelse i augusti 2018. Det är än så länge för tidigt att blåsa faran över och per augusti 2019 är scenariot med vishing fortfarande kvar. Antal försök mot kunder är antalsmässigt högt men förlustmässigt lågt. Bankerna följer frågan hela tiden.

Vishing bygger på social engineering och vår vilja att som människor hjälpa till. Det finns inga identifierade tekniska sårbarheter i BankID eller bankernas säkerhetsdosor. Det finns en mängd olika modus operandi för vishing-bedrägerier men det typiska upplägget har följande ingredienser:

1. Bedragaren ringer upp en kund. Bedragaren utger sig för att vara från ”polisen” eller ”banken”. Bedragaren har sedan tidigare tagit reda på kundens personnummer. Uppgifterna om personnummer och inkomst kan man få genom att ringa till exempel Skatteverket eller genom att söka på internet. Från ett informationssäkerhetsperspektiv är det olämpligt att svenska folkets

personnummer är så lättillgängliga eftersom personnumret är den första delen i legitimeringen (inloggningen) i ett e-legitimationssystem.

2. Bedragaren berättar för kunden att det pågår någonting på kundens konto men att ”banktjänstemannen” eller ”polisen” ska hjälpa kunden med den påstådda händelsen. Men, det gäller att agera snabbt. Kunden känner sig pressad, här gäller det agera. Bedragaren frågar därefter kunden om denne har sin säkerhetsdosa eller Mobilt BankID tillgänglig.

3. Bedragaren har innan dess förberett en inloggning genom att mata in kundens personnummer på ett antal bankers hemsidor eller under samtalet lyckats ta reda på vilken bank kunden har. Personnumret är det identitetsbegrepp som Sverige har enats kring och det får banker, handel m fl. förhålla sig till. Bankerna har ett antal identifieringsmetoder, de vanligaste fungerar enligt följande:

    - Mobilt BankID – finns på en app i en smartphone. Modus är att bedragaren ber kunden att legitimera sig mot sin bank. Kunden får då upp rutan i Mobilt BankID och tror att det är mot banken kunden legitimerar sig hos.

    - säkerhetsdosa/digipass – en fysisk dosa. Modus är att bedragaren ber kunden att lämna ifrån sig koder.

4. Eftersom bedragaren redan har förberett en legitimering (inloggning) med kundens personnummer blir bedragaren inloggad på sin PC i stället för kunden.

5. Bedragaren har nu tillgång till att titta på kundens engagemang i banken. Bedragaren nöjer sig inte med det, bedragaren vill flytta pengarna från kundens konto till en målvakts konto. Bedragaren behöver övertala kunden att signera ett uppdrag till exempel att skapa ett nytt Mobilt BankID (för banken har ”spärrat” det gamla eller det är något som ”strular”) eller signera en Swish-betalning.

6. När kunden därefter övertalas att göra en ny ”inloggning” med sin säkerhetsdosa/Mobilt BankID, för att något till exempel ”krånglat vid legitimeringen”, har bedragaren förberett så att kunden signerar ett uppdrag, till exempel en överföring, ett nytt Swish-avtal osv.

För att motverka detta har bankerna utvecklat och implementerat specifika lösningar som QR-koder för Mobilt BankID. QR1 (legitimering och underskrift) lanserades i september 2018 och QR2 (utfärdande av Mobilt BankID) lanserades i november 2018 i BankID-infrastrukturen. En del banker har infört QR1 och QR2 för samtliga flöden, andra banker i färre flöden. En del banker har inlett arbetet med att byta ut säkerhetsdosan. QR-koderna hjälper mot ovan beskrivet vishing-modus. Säkerhetsdosan kommer att vara en större utmaning för bankerna när modus

utvecklar sig. Andra åtgärder har vidtagits inom Swish som beloppsbegränsning, krav att ha apparna BankID och Swish på samma enhet mm.

I vishing-modus är det kunderna själva som gör transaktionerna. Det innebär att det är väldigt svårt för banken att utifrån monitoreringen stoppa transaktionen. Från bankens sida ser legitimeringen, autentiseringen och signeringen ut som den ska.

Bankerna kan begränsa limiter, fördröja nyanslutning av Swish-avtal och utveckla QR-koder för att knyta tjänsten närmare BankID men det finns egentligen ingen teknisk lösning på utmaningarna med social engineering. Kunderna å sin sida vill naturligtvis inte att bedragare ska komma över deras pengar men de blir i dessa situationer omkullpratade och lurade att göra saker som de inte vill.

Det är alltså angeläget att svenska folkets motståndskraft mot den typen av bedrägeriförsök stärks. Regeringen bör därför ge uppdrag till MSB att årligen delta i den europeiska informationssäkerhetsmånaden (oktober varje år) samt ge Polismyndigheten SC3 ett uppdrag att årligen delta i Europols EC3:s årliga EMMA-kampanjer (European Money Mule Action week) samt öka resurstilldelningen till Polisens nationella bedrägericentrum och Polisens olika bedrägerisektioner.

Det är flera parter som har bidragit till att vända vishing-utvecklingen. Media har beskrivit och uppmärksammat problemet och vad man bör och inte bör göra på ett bra sätt. Bankerna har vidtagit ett antal säkerhetshöjande åtgärder i sina kanaler. Bankföreningens uppfattning är att det är Polisens insatser genom den särskilda nationella händelsen som har varit den enskilt viktigaste komponenten i att vända vishing-utvecklingen.

Polisens statistik avseende antal fall uppdelat per säkerhetslösning (säkerhetsdosa och BankID) visar att majoriteten (ca 75%) av antal anmälda brott härrör från konsumenter som blir avlurade koder från sin säkerhetsdosa. Säkerhetsdosan är alltså en större utmaning medan BankID är en säkerhetslösning med lägre frekvens av bedrägerier. Förklaringen till det kan vara att säkerhetsdosan inte skapar samma kontext som Mobilt BankID gör eller att äldre personer i större omfattning använder sig av säkerhetsdosa och BankID på kort framför Mobilt BankID eller att bedragare ser säkerhetsdosan som mer angelägen att komma åt.

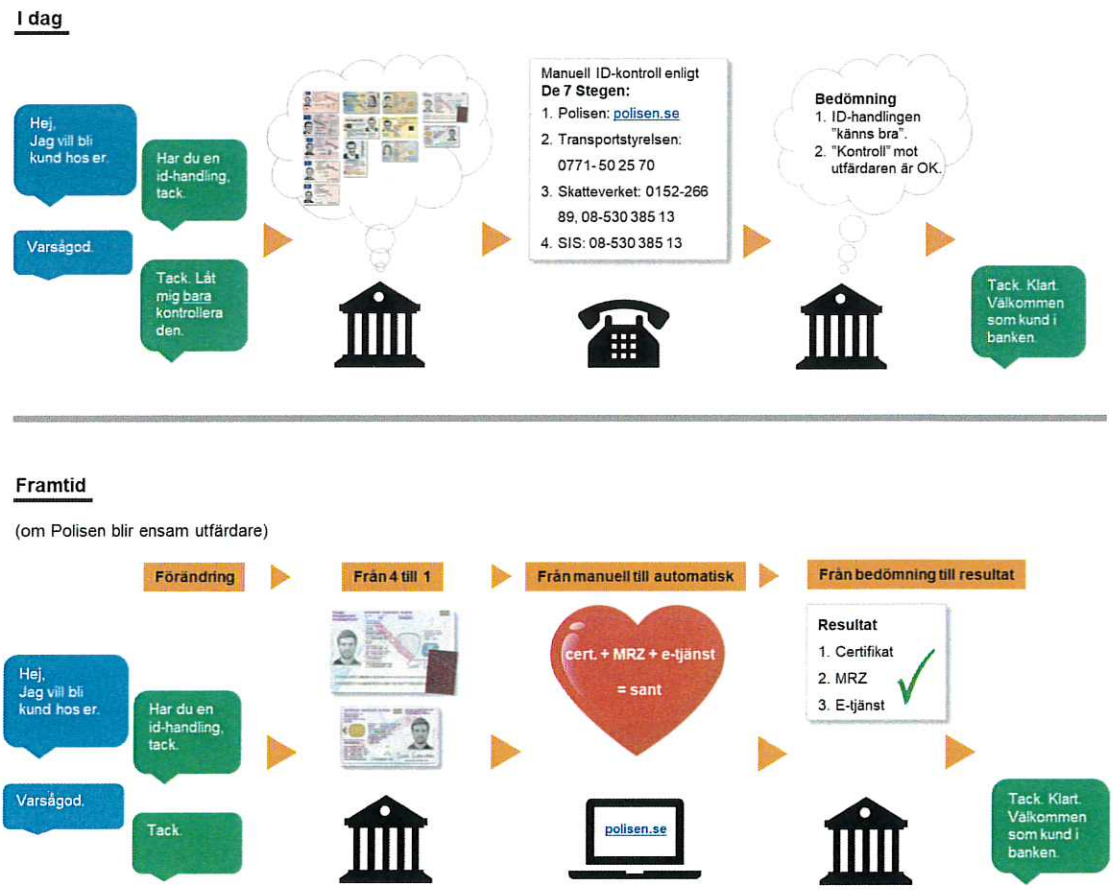
Eftersom utredningen gör ställningstagandet att staten ska utfärda en e-legitimation på högsta tillitsnivå kommer e-legitimationen att finnas på en fysisk bärare (förmodligen ett kort) vilket kräver en (kort)läsare. Som beskrivet ovan är säkerhetsdosan en större utmaning för bankerna att hantera när vishing-modus utvecklar sig. Säkerhetsdosa och BankID på kort kan ha likheter med en statlig e-legitimation på högsta tillitsnivå och utmaningarna kan därmed vara liknande. Det är därför angeläget att Justitiedepartementet och utfärdaren (Polismyndigheten)

funderar på hur svenska folket ska kunna hantera och förstå hur sin e-legitimation ska användas. Det är alltså synnerligen viktigt att svenska folkets motståndskraft att stå emot den här typen av bedrägeriförsök stärks.

Bilaga B – identitetskontroll på bankkontoret idag och i framtiden

I bilaga B åskådliggörs hur en identitetskontroll på ett bankkontor går till idag samt hur utredningens förslag kan stärka identitetskontrollen i framtiden. Bilden är allmängiltig för alla verksamhetsutövare som vill göra en identitetskontroll.

Hur går en ID-kontroll till på bankkontoret i dag och i framtiden?



Utredningens förslag stärker genomgående statens skydd av våra personliga identiteter. Fördelarna är dock inte avgränsade till det som åskådliggörs i bilden ovan, dvs färre utfärdare och effektivare kontrollmöjligheter för verksamhetsutövare.

Många förbättringar återfinns tidigare i ”identitetskedjan”, delar som inte finns med i bilden ovan, dvs i ansökan, tillverkning och utlämnande av identitetshandlingar. Även om effektivitetsvinsterna och säkerhetsförbättringarna i de delarna är svåra att kvantifiera så bör förändringarna i de delarna väsentligt stärka den svenska välfärdsstatens förmåga att stå emot grov identitetsrelaterad organiserad brottslighet.

Bilaga C – Vem bestämmer vilka utfärdare och därmed identitetshandlingar i Sverige som ska anses vara godkänd identitetshandling?

Det finns två aktörer som har uttalat vilka utfärdare (och därmed identitetshandlingar) som ska användas i kontakt med bank och vilka åtgärder som ska vidtas för att kontrollera identiteten: Bankföreningen genom handboken *De 7 stegen* och Finansinspektionen genom *föreskrifter om åtgärder mot penningtvätt och finansiering av terrorism FFFS 2017:11*. I 3 kap 2 § anges att "ett företag ska kontrollera identiteten hos en fysisk person genom svenskt körkort, svenskt pass eller identitetskort utfärdat av en svensk myndighet eller ett svenskt certifierat identitetskort."

Skrivelsen i FFFS 2017:11 som anger att banker ska kontrollera identiteten baserat på "…identitetskort utfärdat av en svensk myndighet…" är problematisk. Det finns för närvarande ca 340 st. svenska myndigheter under regeringen och många myndigheter utfärdar tjänstekort till sina anställda. En vanlig missuppfattning är att anställda på myndigheter kan använda sitt tjänstekort för att legitimera sig i kontakt med bank.

Den 1 januari 2014 upphörde bankerna att godta tjänstekort som identitetshandling. Detta mot bakgrund av dels den osäkerhet som råder kring administrationen av tjänstekort, dels svårigheten för bankerna att kontrollera tjänstekortens giltighet och äkthet. Det finns ingen praktisk möjlighet för bankerna att kontakta ca 340 st. olika svenska myndigheter för att kontrollera deras utfärdade tjänstekort.

Mot denna bakgrund godkänner bankerna endast identitetshandlingar som utfärdas av 3 st. svenska myndigheter: Polisen, Skatteverket och Vägverket/Transportstyrelsen samt bankerna själva (SIS). Där finns etablerade möjligheter att göra fördjupade kontroller av id-handlingen via telefon och internet enligt kontrollprocessen i handboken *De 7 Stegen*.

Det är olyckligt att Bankföreningens handbok *De 7 stegen* och Finansinspektionens föreskrifter om kundkännedom inte överensstämmer med varandra i delen som listar utfärdare som bankerna ska förlita sig på. Det är därför angeläget att Finansinspektionens föreskrifter om kundkännedom justeras enligt utredningens förslag.

Bilaga D – remissyttrandet för slutbetänkandet *Reboot – omstart för den digitala förvaltningen* (SOU 2017:114)

2018-04-23

Bankföreningen har beretts tillfälle att yttra sig över rubricerat slutbetänkande och vill med anledning av det framföra ett antal synpunkter.

Bankföreningen är positiv till utredningens slutsatser och rekommendationer som direkt eller indirekt berör föreningens medlemmar som banker och ägare av samhällsviktig finansiell infrastruktur, bland annat e-legitimationsfrågorna. Vi anser att förslagen kan skapa effektivitet och förenklingar inom e-legitimationsområdet som stärker konsumentskyddet och offentlig förvaltning. Bankföreningen är också positiv till att infrastrukturen Mina meddelanden öppnas upp för privata aktörer som avsändare.

Det har varit en krokig väg för e-legitimationsfrågan i Sverige. Bankföreningen vill därför understryka behovet av en snabb beredning av förslagen för att ge tydliga förutsättningar för leverantörer och myndigheter för att Sverige inte ska tappa i konkurrenskraft. På e-legitimationsområdet behövs förutsägbarhet, stabilitet och långsiktighet.

Finansiell ID-Teknik BID AB som äger, förvaltar och utvecklar BankID, har fattat beslut om att de kommer att anmäla BankID till kvalitetsmärket Svensk e-legitimation. BankID-bankerna har därmed anpassat riktningen och Bankföreningen förväntar sig att regeringen driver på för att genomföra de lagstiftningsförslag som återfinns i reboot-betänkandet.

Bankföreningen lämnar endast synpunkter på de delar som vi bedömer berör bankernas verksamhet:

1. Eftersom BankID är ett miljardprojekt vill Bankföreningen säkerställa att det finns en avsikt att genomföra de lagförslag som återfinns i reboot-betänkandet och en intention att tillskjuta de resurser som krävs för att utveckla och förvalta infrastrukturen för ett statligt e-legitimationssystem. Infrastrukturen består, något förenklat, av tre delar (och är utförligt beskrivet i utredningen på sidan 179…): 1) utfärda elektroniska identitetshandlingar till konsumenter, 2) att konsumenter är medvetna om det ansvar som åligger dem och använder den mot en förlitande part och 3) att den förlitande parten accepterar och kontrollerar den uppvisade elektroniska identitetshandlingen mot utfärdaren. Fördelen och styrkan med e-legitimationer är att det finns en infrastruktur för kontroll i realtid av e-legitimationens giltighet och innehavare vilket saknas för de fysiska identitetshandlingarna.

Om det statliga åtagandet avgränsas till att utfärda en e-legitimation på en fysisk bärare, som andra utfärdare av e-legitimationer ska kunna förlita sig på för att i sin tur utfärda t ex en mobil elektronisk identitetshandling, behöver staten ändå tillhandahålla en infrastruktur för giltighetskontroll gentemot utfärdaren av e-legitimationen för förlitande parter. Det finns flera länder i Europa där staten har utfärdat mängder med e-legitimationer men där användandet av dessa e-legitimationer är begränsat. Eftersom det kan vara kostsamt att utveckla och förvalta en infrastruktur (testmiljöer, kortläsare, säkerhetsuppdateringar, patchning, olika operativsystem, supportfrågor mm) är en sådan utveckling inte önskvärd. Det är helt enkelt inte kostnadseffektivt eftersom kostnaden inte står i paritet med nyttan.

2. Bankföreningen tillstyrker utredningens resonemang och tankar kring grundidentifiering. En fungerande process för att identifiera personer och fastställa fysiska personers identitet stärker förutsättningarna för att utfärda elektroniska identitetshandlingar oavsett vem som är utfärdare. Principerna för grundidentifiering (sid. 175) bör kompletteras med ”tagande av fingeravtryck”, dvs de befintliga kraven för pass.

3. Bankföreningen tillstyrker utredningens bedömning och förslag att staten inte ska utfärda mobila elektroniska identitetshandlingar och att statliga elektroniska identitetshandlingar ska vara på den högsta tillitsnivån (12.7.2) samt förslaget i 12.8.

4. Svenska banker har inga planer på att endast förlita sig på mobilt BankID. BankID på kort och andra fysiska säkerhetsdoslösningar kommer att finnas kvar under överskådlig tid. Det kan förvisso bli någon annan teknik över tiden men som kund får man alltid en säkerhetsdosa (från de större bankerna) som grundidentifiering. Ur ett kontinuitetsperspektiv kan inte bankerna endast förlita sig på BankID även om infrastrukturen under tjugo år har visat sig vara säker, stabil och har haft mycket hög tillgänglighet med redundans på både säkerhet och drift. Bankernas uppfattning är att säkerhetsdosor kommer att fortsätta att vara en del av bankernas infrastruktur för legitimering och underskrift för sina kunder. I dagsläget är säkerhetsdosan bankernas ordinarie back-up lösning för sin bank och sina kunder för det fall BankID inte skulle fungera. Utöver ordinarie back-up lösningar undersöker svenska banker ytterligare back-up lösningar som en del i arbetet att stärka sektorns robusthet. Bankerna diskuterar olika scenarier och förmodligen blir det någon form av gemensam back-up lösning, dvs inte avgränsad till utfärdande banks kunder.

5. Svenska konsumenter är idag utsatta för en mängd bedrägeriförsök. Eftersom säkerhet byggs underifrån behöver konsumenternas

medvetandegrad (awareness) höjas i Sverige. Bankföreningen vill därför understryka behovet av att staten engagerar sig mer i frågan om att höja svenska folkets kunskaper i informations- och cybersäkerhet. Att höja informationssäkerheten är en förutsättning för fortsatt digitalisering. Bankföreningen ser inte att staten är särskilt närvarande på området informationssäkerhet, i alla fall inte på den så viktiga konsumentnivån. Det är en grundläggande skillnad mellan den fysiska världen och den digitala världen och en del konsumenter har svårigheter att förstå de nya tjänsterna och de nya kraven. Svenska banker kommer att fortsätta sitt arbete med att höja kundernas medvetandegrad. I sammanhanget är det positivt att regeringen har givit MSB och Polisens nationella bedrägericenter ett uppdrag att bidra till att öka allmänhetens kunskap om informationssäkerhet (Ju2018/01866/SSK). Bankföreningen ser gärna att bankerna och BankID ges möjlighet att bidra med input i det arbetet. För att inte tappa ytterligare momentum bör regeringen redan nu uppdra åt MSB att säkerställa att Sverige varje år uppmärksammar och deltar i den europeiska informationssäkerhetsmånaden (oktober varje år). Det kan ske genom seminarier, hemsidor, samverkan med konsument- och privata organisationer, närvaro i sociala medier mm. Embryot till detta finns redan inom MSB och Polisen.

Det finns stora politiska ambitioner att öka digitaliseringen av offentlig sektor. Myndigheter kommer att möta motsvarande utmaningar som svenska banker har gjort ju mer digitaliserade tjänsterna blir. Om vi tar Riksbankens initiativ e-kronan som ett illustrativt exempel så har frågan utretts under en tid, och frågan utreds fortfarande. Det dröjde inte länge förrän det på internet dök upp ”erbjudanden” att köpa e-kronor (några e-kronor finns inte att köpa eftersom frågan fortfarande utreds av Riksbanken) men det visar på den genomslagskraft som internet har. Den myndighet och företag som distribuerar sina ”produkter” via e-tjänster behöver hantera dimensionen internet, det handlar förmodligen framför allt om utbetalande myndigheter t ex Försäkringskassan, Skatteverket, CSN m fl. Det kan handla om operativ informationsdelning, övervakning av vissa forum på internet, nedtagning av bedrägliga hemsidor, awareness, trojanmonitorering, transaktionsmonitorering mm. Allt detta har banker erfarenhet av och samarbeten runt sedan många år.

Säkerhet på internet handlar för banken mycket om att konsumenten skyddar sin identitet och använder bankens säkerhetslösningar. Det är mycket ovanligt att de tekniska aspekterna av en säkerhetslösning eller betalinstrument fallerar men vanligare att kunder luras av bedragare att lämna ifrån sig koder till sin säkerhetsdosa eller luras av en ”trevlig banktjänsteman” eller ”trevlig polis” som ringer upp och uppmanar kunden att

logga in med sitt BankID. Medvetandehöjande åtgärder kan stärka konsumentskyddet i Sverige. Bankerna har utmaningar med att nå fram med budskap som förändrar konsumenternas beteende på internet. Här krävs någon form av samlad informations- och utbildningsinsats och utredningen för ett resonemang om detta i avsnittet om användning (22.4). Bankföreningen är positiv till samtliga initiativ som kan stärka informationssäkerheten och som ökar konsumenters förståelse för vad internet är.

6. Bankerna utfärdar idag BankID till personer som är folkbokförda (finns med i SPAR), som har svenskt personnummer och som har en svensk ID-handling. Det förekommer ofta synpunkter på varför bankerna inte utfärdar BankID till utländska medborgare, personer som inte kan uppvisa giltiga identitetshandlingar eller personer med samordningsnummer. Anledningen till avgränsningen är att personnumret är det identitetsbegrepp som Sverige har enats om. Det är bara på personnumret och folkbokföringen som en person kan anses vara grundidentifierad och det är bara då det finns förutsättningar för att utfärda ett BankID eftersom banken intygar identiteten till flera tusen förlitande parter (företag, myndigheter och banker). BankID är en e-legitimationslösning som hela tiden utvecklas och förändras beroende på hotbilden. Även om namnet är oförändrat så är det på intet sätt en statisk säkerhetslösning, det sker en ständig förflyttning, utveckling och löpande analyser.

   Ett område som kommer att bli ännu svårare att hantera är gruppen utlandssvenskar. De medborgarna vill fortsätta att använda e-tjänster i Sverige men bristande information om kunderna gör att bankens utfärdande av BankID försvåras. Efter ett antal år så finns denna grupps personuppgifter inte längre med i SPAR-registret. För bankernas utfärdande av BankID så skulle det underlätta om denna grupps uppgifter finns tillgängliga i SPAR mer än tre år.

   För kunder som inte är folkbokförda och som saknar svenskt personnummer utfärdar svenska banker idag ett s k BxID. Tekniskt sett fungerar ett BxID som ett BankID och BxID finns både på kort och mobilt. Skillnaden är att ett BxID endast fungerar mot utfärdande part medan ett BankID fungerar mot samtliga förlitande parter.

7. Det finns, så vitt Bankföreningen kan se, inget mervärde med att ändra begreppet ”e-legitimation” till ”elektronisk identitetshandling” eller ”förlitande part” (på engelska: relying party) till ”förlitande aktör” trots förklaringen (sid. 171). Vi har samtidigt inget större behov av att hålla fast vid den nuvarande begreppsapparaten om staten anser att det är angeläget att ändra den. ”E-

legitimation" och "förlitande part" har som begrepp inarbetats under tjugo år vilket gör att begreppsapparaten riskerar att bli stökig.

8. Författningsförslag 17 § – "Om en statlig elektronisk identitetshandling spärras ska den utfärdande myndigheten informera de utfärdare av elektroniska identitetshandlingar, som har använt den statliga elektroniska identitetshandlingen som underlag om detta".
   Bankföreningen anser att en spärrtjänst är nödvändig. En bank kan dock inte automatiskt spärra ett utfärdat BankID om en fysisk id-handling har förkommit, det är två olika saker. Tilltron till fysisk-elektronisk identitet kräver inte en sådan kedja vilket man skulle kunna tro (sid. 204). Händelser i den fysiska världen (som att en identitetshandling tappas bort och därmed behöver förlustanmälas och spärras) behöver inte resultera i motsvarande åtgärder i den digitala världen (för utfärdare av elektroniska identitetshandlingar). Fysiska identitetshandlingar kan förkomma/bli obrukbara på en mängd olika sätt: kvarglömd i tvättmaskin, borttappad, stulen osv. I samtliga fall bör innehavaren kontakta utfärdaren för att få handlingen spärrad och därefter inleda ansökan om få en ny handling utfärdad. Så länge den fysiska identitetshandlingen spärras är risken liten för att den urkunden ska användas som identifiering av en utfärdare av elektroniska identitetshandlingar. Om den statliga elektroniska identitetshandlingen spärras behöver den utfärdande myndigheten informera andra utfärdare av elektroniska identitetshandlingar om *orsaken* till varför den har spärrats. Det är endast vid ett felaktigt utfärdande (helfalsk identitet eller identitetsstöld) som detta torde vara aktuellt och det är endast då som den utfärdade elektroniska identitetshandlingen bör spärras oavsett utfärdare.

9. Det är angeläget för förtroendet för digitala tjänster att samtliga utfärdare av elektroniska identitetshandlingar håller en hög tillitsnivå. Om man bortser från den infrastruktur och skydd som omger den elektroniska identitetshandlingen, hur patch management går till och hur testmiljöer mm hanteras så landar man i att det är utfärdandeprocessen som är nyckeln till den digitala identiteten. BankID utfärdas idag genom dualitet av två banktjänstemän som följer kontrollprocessen i handboken De 7 stegen med krav på giltighetskontroll av den fysiska identitetshandlingen mot utfärdaren via telefon/internet. E-legitimationsnämnden har en viktig roll att säkerställa att samtliga utfärdare av elektroniska identitetshandlingar, som har kvalitetsmärket Svensk e-legitimation, uppfyller denna säkerhetsnivå så att förtroendet för digitala tjänster upprätthålls.

10. Bankerna har tillsammans med de större distributörerna av digitala dokument alltsedan mitten av 1990-talet verkat för en digital nationell infrastruktur med fokus på fakturor. Möjligheten att ta emot och betala digitala fakturor i

internetbankerna redan 1997 var mycket framsynt då man kan ta i beaktande att internetbankerna som sådant lanserades bara några år tidigare.
Den svenska e-fakturainfrastrukturen är tillsammans med våra nordiska och baltiska grannländers lösningar fortfarande ur ett europeiskt perspektiv ett framgångsexempel. De europeiska initiativ som tas idag med sikte på att främja utvecklingen av distribution av digitala fakturor över landsgränser för konsumenter och småföretag bygger på samma lösningar och tankesätt som etablerats i Norden och Baltikum, dvs s k EIPP-lösningar, E-invoicing Payment and Presentment. Ett enkelt sätt att titta på och betala en faktura digitalt. Volymen e-fakturor växte långsamt i början då marknaden inte var tillräckligt digitalt mogen men efter ett uthålligt arbete i ca 20 år är nu Sverige, Europa och många andra delar av världen redo för digitala fakturor och digital post. Vi såg en tillväxt i Sverige på 14 % för e-fakturor till konsumenter 2017 i den bankgemensamma infrastrukturen till ca.140 miljoner fakturor.

11. Bankföreningen är tveksam till beskrivningen av personuppgiftsansvaret inom Mina meddelanden i relation till fakturor och dess vidare bearbetning. En leverantör av brevlådetjänster är inte enligt infrastrukturens definition en betaltjänstleverantör. Dagens brevlådeoperatörer kan erbjuda betalningslösningar, men gör detta baserat på bankernas betalningslösningar som t ex autogiro. Betalningsinstitut står under tillsyn av Finansinspektionen, lyder under andra lagar och regler och kan inte och bör inte regleras indirekt även i denna lag om digital post. Detta särskilt med beaktande av att personuppgiftsansvaret inom Mina meddelanden föreslås att särskilt regleras i lag. Inom bankernas tjänst ”Banksamverkan e-faktura” anses den bank som har avtal med avsändaren ta över personuppgiftsansvaret då denne godkänt mottagandet av den digitala fakturan, detta i båda de fall då det enbart är en avisering (om autogiro, kreditfaktura) utan koppling till betalning eller en faktura med koppling till betalning. Att en avsändare ska bibehålla sitt personuppgiftsansvar längre än efter ett godkänt mottagande kan få märkliga konsekvenser för betalningstjänstleverantörerna. Vidare skrivs att personuppgifter i registret bara ska få behandlas om det behövs för att förmedla digital post i syfte att kunna utföra en arbetsuppgift inom en författningsreglerad verksamhet hos någon av de som anslutit sig till infrastrukturen. Omfattas samtliga föreslagna avsändare av författningsreglerad verksamhet?

12. Bankernas internettjänster är i mångt och mycket redan etablerade digitala brevlådetjänster där bankernas egna samt andra aktörers information presenteras. Bankerna erbjuder externa parter tjänsterna distribution och presentation av e-fakturor och e-lönebesked i sina internettjänster sedan många år tillbaka. Digitala dokument som är relaterade till en betalningstjänst. Merparten av Offentlig sektor är idag ansluten till bankernas

infrastruktur för digitala fakturor. Genom avtal med en bank når man 13 internetbanker plus ett 50-tal Sparbanker.

Bankföreningen ifrågasätter om att begränsningen att en mottagare bara kan ha en (1) adress i förmedlingsregistret innebär att bankernas digitala fakturor automatiskt kommer styras bort från bankinfrastrukturen. Bankerna skulle kunna ansluta sig till infrastrukturen som brevlådetjänst under förutsättning att typ av dokument på motsvarande sätt som i Min Myndighetspost kan begränsas. Bankföreningen är av övertygelsen att mottagaren önskar hålla isär sin ekonomi och viktiga papper med övrig information som t ex direktadresserad reklam.

Med tanke på att Mina meddelanden kommer att vara anslagsfinansierad för offentlig sektor och privata utförare visavi de kommersiella brevlådorna kommer inte bankerna att kunna konkurrera på samma marknadsmässiga villkor. Bankföreningen ser ett hot mot att den infrastruktur bankerna byggt upp under 20 år avseende digitala fakturor automatiskt kommer styras bort från bankinfrastrukturen genom den adresseringsmetod som föreslås i kombination med det anslagsfinansierade upplägget. Detta kan inte vara lagstiftarens avsikt.

13. Under förutsättning att en mottagare kan ta emot digital post och digitala fakturor för betalning i olika brevlådetjänster, dvs ha fler än en adress i förmedlingsregistret, samt att samtliga avsändare inom infrastrukturen Mina meddelanden, även avsändare av allmänt intresse, kan skicka post till Min Myndighetspost, ser Bankföreningen möjligheter för bankerna att delta i och främja en framgångsrik utveckling av den nationella infrastrukturen för digital post, Mina meddelanden. Bankerna skickar idag fortfarande stora volymer papperspost till kunder där man ej har en huvudkundsrelation och där kunderna har sin internettjänst hos en annan bank. Många banker kan säkert önska ansluta sig som en brevlådetjänst i infrastrukturen under förutsättning att man inte tvingas ta emot all möjlig post som t ex direktreklam.
Många banker kan säkert även tänka sig agera som förmedlare för sina kunder för att underlätta deras distribution av post för vidarebefordran till kommersiella brevlådor och Min myndighetspost.

14. Bankföreningen anser att det är viktigt att en infrastruktur för digital post i Sverige reglerar ett minimum av det som behöver regleras för att marknaden ska svänga över till digital post. Vi ser att erbjudanden som att kunna arkivera, sortera, kommunicera, betala, m.m. är tjänster som i så stor utsträckning som möjligt bör ligga inom det konkurrensutsatta området. Krav på enhetliga funktioner i infrastrukturen bör hållas till ett minimum.
Bankföreningen anser också att skickad post ägs av mottagaren och att

denne kommer välja den brevlådetjänst som bäst tillgodoser dennes önskemål och krav. Sund konkurrens kommer driva på utvecklingen av bra tjänster. Den främsta hämskon för bankernas infrastruktur för digitala fakturor har varit att man inte kan få samtliga fakturor digitalt. Detta har i första hand berott på att företagen som skickar fakturor har vaknat ganska sent när det gäller att ställa om till digitala fakturor. Från och med april 2019 kommer det vara lag på att alla leverantörer till offentlig sektor ska skicka e-fakturor vilket kommer driva på volymutvecklingen för e-fakturor till konsument genom att fler företag har lösningar för att skicka e-fakturor. Även företagen vill hantera alla sina fakturor på samma sätt, dvs antingen digitalt eller på papper. Ett villkor om att avsändaren måste ha avtal med en eller alla leverantörer av brevlådetjänster för digital post kan vara marknadsmässigt svårt då det alltid är en bilateral förhandling. Om man inte kan enas om pris nekas en sådan avsändare tillträde till infrastrukturen. Bankföreningen anser att en sund marknadsplats bygger på största möjliga konkurrens och att infrastrukturmässiga funktioner som begränsad adresseringsmöjlighet och olyckliga prisincitament inte ska styra bort digitala fakturor och andra dokument från redan etablerade och väl fungerade lösningar.

15. Bankföreningen rekommenderar att ytterligare arbete genomförs avseende aktörerna och deras roller i infrastrukturen Mina meddelanden. Några exempel:
    - Eventuellt kan beskrivningen tolkas som att avsändare av allmänt intresse kan eller inte kan skicka post till Min myndighetspost. Vi utgår att syftet med att tillåta nya avsändargrupper, som privata utförare och företag av allmänt intresse, är att dessa kan skicka digital post till brevlådan Min Myndighetspost.
    - Bankföreningen ser inte hur rollen förmedlare kan innehas av en individ dvs. fysisk person. Innebär lagen att samtliga avsändare, inklusive av allmänt intresse, kommer anslutas via Skatteverkets förmedlare (distributörer) eller kommer varje avsändare själv distribuera den digitala posten alternativt upphandla en förmedlare.
    - Vad kallas den del av kedjan som distribuerar posten till brevlådan, dvs. länken mellan avsändaren och leverantör av brevlådetjänsterna. Bankföreningen utgår från att det är förmedlaren (i det fall avsändaren själv inte upprätthåller rollen)?
    - Bankföreningen ser inte hur rollen som leverantör av brevlåda kan innehas av en individ dvs. fysisk person.

SVENSKA BANKFÖRENINGEN

Hans Lindberg

Peter Göransson

Svenska Bankföreningen
Swedish Bankers' Association

REMISSYTTRANDE
Vår referens: 2019/05/001
Er referens: Ju2019/01281/L4

2019-09-10

Justitiedepartementet
ju.remissvar@regeringskansliet.se
ju-L4@regeringskansliet.se

Bankföreningens kompletterande synpunkt på betänkandet *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14)

Bankföreningen har den 30 augusti lämnat ett remissvar på betänkandet och skulle nu vilja komplettera detta med ytterligare en synpunkt.

I förslaget till ändring av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, 3 kap. 7 §, föreslås ett nytt tredje stycke. Där anges att en person som är personligt närvarande ska kontrolleras bland annat, om det bedöms lämpligt, med en **statlig** e-legitimation. Så som förslaget är skrivet exkluderas möjligheten att, när kunden är närvarande, använda en annan e-legitimation än en statlig, till exempel BankID. Detta anser Bankföreningen vara olyckligt och förslår att skrivningen ändras till att medge även andra e-legitimationer än en statlig.

SVENSKA BANKFÖRENINGEN

Hans Lindberg

Peter Göransson

Besök (Visit):
Blasieholmsgatan 4B
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

t: +46 (0)8 453 44 00

e: info@swedishbankers.se
www.swedishbankers.se