kirei

PM

2019-01-23

Kirei 2018:11

Säkerhet vid elektronisk legitimering och underskrift

villaägarna

Sammanfattning

Villaägarnas Riksförbund granskar inom sin verksamhet ”Produktgranskning” sådant som funkar mindre väl, inte alls eller har bristande hållbarhet och därmed är sämre för miljön. Tanken är att småhusägare och andra konsumenter på så sätt ska kunna spara pengar, slippa besvär och göra grönare val.

Många småhusägare och andra konsumenter har drabbats av bedrägerier i samband med elektronisk legitimering och underskrift. Med anledning av att bedragare förhållandevis enkelt har kunnat tillgodogöra sig besparingar på småhusägares och andra konsumenters bankkonton, lyckats med att ta banklån i deras namn etc. samt att antalet bedrägerier och bedrägeriförsök är högt, ansåg Villaägarnas Riksförbunds chefsjurist Ulf Stenberg att något måste göras åt saken. Fredrik Ljunggren på IT-säkerhetsföretaget Kirei anlitades för att få säkerhetsproblemen utredda och även få klarlagt vilka åtgärder som kan vidtas för att öka säkerheten och därmed minska problemen.

I media har fokus framför allt legat på brister i säkerheten för mobilt bank-ID, trots att det primära säkerhetsproblemet – så som framgår av förevarande rapport - egentligen ligger på andra plan, främst avsaknad av tillräckliga rimlighetsspärrar och manuella kontroller vid banktransaktioner med högre risk. Möjligheten att smidigt kunna genomföra banktransaktioner har i mångt och mycket prioriterats på bekostnad av sådana säkerhetslösningar.

Förslag till åtgärder för att minska risken för bedrägerier vid elektronisk legitimering och underskrift

1. En person som beter sig konstigt på ett bankkontor och vill genomföra en rad riskfyllda transaktioner kommer att nekas detta eller i vart fall utsättas för särskilt ingående extra kontroller. När motsvarande riskfyllda beteende äger rum med BankID, fungerar emellertid det automatiserade tillvägagångssättet på samma sätt som vid en transaktion som inte präglas av särskilda risker. De riskfyllda transaktionerna släpps igenom. Genom väl avvägda rimlighetsspärrar och manuella kontroller även vid automatiserad behandling och användande av BankID, minskar risken för att bedrägerier kan genomföras. Rimlighetsspärrar och manuella kontroller kan förhindra att bedragare med t.ex. stöd av en helt nyutfärdad e-legitimation kan länsa ett sparkonto genom överföringar till ett flertal nya och annars okända mottagare, som kunden tidigare aldrig har gjort överföringar till. Att ett bankkonto töms på det sättet, är helt enkelt inte ett rimligt användningsmönster.

2. Genom införande av liknande rimlighetsspärrar och manuella kontroller, kan myndigheter försvåra till exempel bolagskapningar, oriktiga utbetalningar av sociala förmåner, utbetalningar från skattekonton m.m.

3. Ytterligare och mer sofistikerade automatiska kontroller skulle också kunna införas om mer information om legitimeringen förmedlas från utfärdaren till förlitande part. Detta skulle kunna utformas som en poängsättning som grundas i en sammanvägd

riskbedömning att en viss e-legitimation missbrukas. Poängsättningen kan fungera på ungefär samma sätt som när försäkringsbolag som försäkrar fordon gör en bedömning baserat på fordonstyp, förarens ålder, skadefria år och hemvist. Transaktioner som utförs med till exempel helt nyutfärdade e-legitimationer kan i sådant fall i högre grad väljas ut för manuella kontroller för att kompensera för en förhöjd risk.

4. Elektroniskt avläsbara fysiska legitimationshandlingar med automatisk spärrkontroll kan öka säkerheten vid fysiska möten högst väsentligt.

5. Om folkbokföringsregistret kunde utökas till att även omfatta en frivillig sekretessbelagd uppgift om en persons mobiltelefonnummer, skulle Skatteverket kunna skicka meddelanden till privatpersoner/konsumenter när en e-legitimation har utfärdats, en bankrelation inletts, anmälan om adressändring mottagits eller att en kreditupplysning tagits. Då kan den som är på väg att utsättas för ett bedrägeri, upptäcka detta på ett tidigt stadium.

6. Om bankerna tydligare och mer omfattande – precis som i Storbritannien - informerar sina kunder om riskerna och hur de ska agera om en bedragare tar kontakt, skulle risken för bedrägerier kunna minska.

7. Det saknas reglering av ansvar och aktsamhetskrav vid sådan användning av e-legitimering där betaltjänstlagen inte är tillämplig. Behovet av sådan särreglering behöver utredas.

Så här går bedrägerier med e-legitimationer till

Två vanliga sätt att begå bedrägerier med e-legitimation är följande.

1. Bedragaren tar kontakt med målsäganden via telefon och övertalar målsäganden att genomföra vissa åtgärder på sin internetbank. Bedragarna utger sig ofta att vara från banken, och kontakten sker under förevändning att några obehöriga transaktioner sker på kontot, och att innehavaren måste legitimera sig för att de ska kunna stoppa transaktionerna.

2. Bedragaren tillskansar sig en e-legitimation i någons namn på obehörig väg, t.ex. genom användande av förfalskade fysiska legitimationshandlingar, för att denna väg öppna ett bankkonto och sedan i nästa steg hämta hem ett BankID som kan nyttjas för att ta nya lån eller överföra pengar från konton i annan bank.

Den övervägande delen av alla bedrägerier sker enligt det första av de två tillvägagångssätten. Vad som sällan framkommer är att bedragarna i första hand är inriktade på bankdosorna, även om det förekommer att BankID också används. Med svarskoder från bankdosan kan bedragarna skaffa ett BankID, och kan med hjälp av detta genomföra ett stort antal överföringar till andra konton. Det är också med detta nyutfärdade BankID möjligt att hinna plundra konton, som innehavaren har i andra banker innan kontohavaren förstår vad som är i görningen och hinner spärra e-legitimationen.

Innehåll

1 Bakgrund

Villaägarnas Riksförbund granskar inom sin verksamhet ”Produktgranskning” sådant som funkar mindre väl, inte alls eller har bristande hållbarhet och därmed är sämre för miljön. Tanken är att småhusägare och andra konsumenter på så sätt ska kunna spara pengar, slippa besvär och göra grönare val.

Många småhusägare och andra konsumenter har drabbats av bedrägerier i samband med elektronisk legitimering och underskrift. Det rör sig om att bedragare kontaktar privatpersoner och lurar dem att släppa in bedragarna i deras internetbanker.

Med anledning av att bedragare förhållandevis enkelt har kunnat tillgodogöra sig besparingar på småhusägares och andra konsumenters bankkonton, samt mot bakgrund av det stora antalet bedrägerier och bedrägeriförsök som förekommit, ansåg Villaägarnas Riksförbunds chefsjurist Ulf Stenberg att något måste göras.

Fredrik Ljunggren på IT-säkerhetsföretaget Kirei har anlitats för att få säkerhetsproblemen utredda och även få klarlagt vilka åtgärder som kan vidtas för att öka säkerheten och därmed minska problemen. Förlorar småhusägare och andra konsumenter förtroendet för banksystemet och elektronisk legitimering, kan det negativt påverka den finansiella stabiliteten och effektiviteten i landet. En sådan situation måste undvikas och problemen istället lösas.

I media har fokus framför allt legat på brister i säkerheten för mobilt bank-ID, trots att det primära säkerhetsproblemet – så som framgår av förevarande rapport - egentligen ligger på andra plan, främst avsaknad av tillräckliga rimlighetsspärrar och manuella kontroller vid banktransaktioner med högre risk. Möjligheten att smidigt kunna genomföra banktransaktioner har i mångt och mycket prioriterats på bekostnad av sådana säkerhetslösningar.

2 Säkerhet vid elektronisk legitimering och underskrift

Under det senaste decenniet har det vuxit fram breda lösningar för elektronisk identifiering som används av allmänheten för åtkomst till såväl privata som offentliga e-tjänster.

Sedan tekniken för elektronisk legitimering med stöd av mobilt BankID infördes år 2011 har användningen av e-legitimering ökat närmast explosionsartat. Under 2017 använde 7,6 miljoner personer mobilt BankID för att genomföra 2,5 miljarder transaktioner mot över 600 e-tjänster. Med en sådan spridning och användning, och med de nyttor som uppstår denna väg, får e-legitimationen idag anses vara en samhällsbärande infrastruktur. Det är således från ett samhällsperspektiv av yttersta vikt att säkerheten och tilltron till e-legitimationer åtnjuter ett grundmurat förtroende hos såväl de som ska använda den för att legitimera sig och de som ska förlita sig på legitimeringarna.

Denna PM syftar till att från säkerhetssynpunkt och utifrån ett konsumentperspektiv beskriva de utmaningar som är förknippade med elektronisk legitimering. Promemorian inleds med en genomlysning av området, bland annat vad kvalitetsmärket Svensk e-legitimation innebär, vilka säkerhetskravställningar som finns och hur de tillämpas samt vilken rättslig reglering som finns och som planeras inom området.

3 E-legitimering i Sverige

I Sverige har utfärdande av legitimationshandlingar aldrig varit en ren myndighetsuppgift. Dåvarande Postverket och bankerna tog huvudsakligen på sig uppgiften att förse invånarna med legitimationshandlingar, eftersom de hade intresse av att deras kunder hade sådana handlingar. Sedan 2005 har det nationella ID-kortet börjat utfärdas av Polismyndigheten till följd av det europeiska rörlighetsdirektivets införande. Även Skatteverket utfärdar sedan 2009 legitimationshandlingar för att kunna förse de invånare som varken är svenska medborgare (och därför inte kan erhålla det nationella id-kortet) och inte heller är kund i någon bank, en inte alldeles ovanlig situation för en person som flyttar till Sverige.

Motsvarande struktur kan sägas gälla för utfärdande av e-legitimationer. Dessa har en stark koppling till banksektorn, som via det samägda bolaget Finansiell ID-teknik AB tillhandahåller de lösningar som går under namnet BankID. Finansiell ID-teknik startades 2002 för att möta den efterfrågan som uttryckts, inte minst från myndighetshåll, att kunna legitimera medborgare på distans. Man började tala om 24-timmarsmyndigheten och e-förvaltning, och e-legitimering var och är en grundförutsättning för att realisera de målsättningar man hade för att effektivisera och höja servicegraden inom den offentliga sektorn gentemot medborgaren.

Banksektorn hade genom de många internetbankerna ett flertal identifieringslösningar på plats. De kunde redan då identifiera 2,7 miljoner svenskar på ett tillförlitligt sätt denna väg. För att underlätta de tekniska integrationerna och kunna identifiera medborgaren på ett enhetligt sätt lanserades produkten BankID år 2003.

Därtill fanns ytterligare elektroniska legitimationer från bl.a. Nordbanken, Telia och Posten. Postens satsning på chipförsedda legitimationshandlingar till allmänheten lades ner tidigt. Nordbanken, sedermera Nordea, har sedan 2011 gått med i BankID-samarbetet, vilket lett till att drygt 7 miljoner svenskar idag kan skaffa BankID via sin internetbank. Därtill finns sedan 2009 Skatteverkets ID-kort som även innehåller e-legitimation.

I en internationell jämförelse ligger Sverige idag i yttersta framkant vad beträffar utbredning, genomslag och användning av e-legitimering och den samhällsservice som erbjuds via internet.

3.1 Den offentliga sektorns användning av e-legitimationer

Sedan början av 2003 har myndigheter via ramavtalsupphandlingar kunnat avropa e-legitimering av nämnda leverantörer. Genom förändringar i upphandlingsreglerna blev det efter den ramavtalsupphandling som genomfördes 2008 inte längre möjligt att upphandla flera leverantörer på samma sätt som tidigare. Vid denna tid hade man från myndigheternas sida även identifierat det tydliga leverantörsberoende som e-förvaltningen kommit att få till Finansiell ID-teknik AB. De tekniska lösningar som tillhandahölls vid den tiden var dessutom kostsamma att införa och underhålla. Under 2010 tillsattes en utredning för att förbereda och genomföra bildandet av en nämndmyndighet för samordning av den offentliga sektorns användning av e-legitimationer.

Utredningen föreslog att inrätta ett valfrihetssystem som upphandlingsform för den

framtida försörjningen av e-legitimationer till den offentliga sektorn. Detta skulle främja en mångfald genom att det blev möjligt för nya leverantörer att tillhandahålla likvärdiga tjänster som BankID på samma villkor. Genom denna modell blev det möjligt att på ett enkelt sätt nyttja tjänster från olika leverantörer utan att varje myndighet skulle behöva teckna nya avtal och genomföra nya tekniska integrationer.

Kopplat till valfrihetssystemet blev även en enhetlig säkerhetskravställning, kallad tillitsramverk, som varje tillhandahållare av e-legimationslösning behövde uppfylla för att kunna teckna avtal och leverera inom ramen för valfrihetssystemet.

E-legitimationsnämnden bildades 1 januari 2011, och började arbeta för att inrätta den modell som utredningen föreslagit. Lagen (2013:311) om valfrihetsystem i fråga om tjänster för elektronisk identifiering trädde i kraft 1 juli 2013, och vid denna tid fanns i praktiken hela den struktur på plats som krävdes för att såväl myndigheter som leverantörer skulle kunna samverka denna väg.

Det kom dock att dröja ytterligare 5 år innan den första godkända leverantören av e-legitimering vid sidan om BankID kunde teckna anslutningsavtal. Verisec Freja eID AB har tecknat avtal om att börja leverera e-legitimeringar till offentliga sektorn så sent som 30 augusti 2018, dagen innan E-legitimationsnämnden avvecklades och verksamheten övergick till Myndigheten för digital förvaltning.

Tillitsramverket för Svensk e-legitimation

Tillitsramverket för Svensk e-legitimation syftar till att etablera gemensamma säkerhetskrav för alla utfärdare av Svensk e-legitimation. Kraven för att utfärda en Svensk e-legitimation är högt ställda och vilar på internationella standarder och erkända och etablerade principer. Endast de aktörer som lever upp till kraven får tillåtas att leverera elektroniska legitimeringstjänster och bära kännetecknet för Svensk e-legitimation. Myndigheten för digital förvaltning, och tidigare E-legitimationsnämnden, granskar därför utfärdare ingående mot denna kravställning innan anslutning sker, och följer därefter löpande upp kravuppfyllnad.

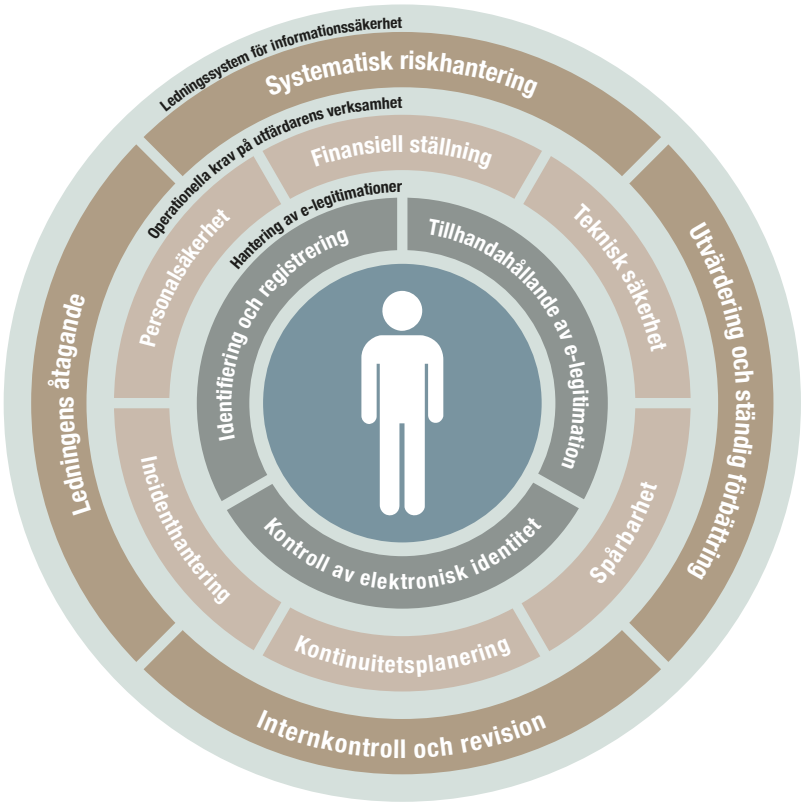
Tillitsramverkets beståndsdelar

För att olika tekniska lösningar från olika utgivare ska kunna betraktas som likvärdiga från ett säkerhetsperspektiv, och därmed kunna läggas till grund för anslutning till valfrihetssystemet, fordras en heltäckande, långsiktig och teknikneutral kravställning.

Kraven formuleras enligt en allmänt vedertagen modell för elektronisk identifiering, där hanteringen av e-legitimationen delas in i tre olika faser;

1. Ansökan och fastställande av sökandens identitet;
2. Utfärdande och tillhandahållande av e-legitimationshandling; och
3. Verifiering av e-legitimation och utställande av identitetsintyg.

I var och en av dessa faser krävs särskilda åtgärder för att upprätthålla den angivna skyddsnivån för hanteringen av e-legitimationer. De områden inom vilka krav ställs redovisas översiktligt i följande figur.



Figur 3.1 – Tillitsramverkets beståndsdelar

Tre tillitsnivåer

I elektroniska miljöer är säkerhet och användbarhet storheter som vanligen står i motsatsförhållande till varandra. En alltför säker lösning riskerar att bli oanvändbar för de allra flesta. Utgångspunkten vid utformning av en säkerhetskravställning för e-legitimationer bör därför vara att den elektroniska identifieringen ska vara tillräckligt säker för det ändamål och i det sammanhang den skall brukas. Riskerna ska begränsas till acceptabla nivåer, och det är inte befogat att till exempel ställa mycket högre krav när ett ärende hanteras via en it-baserad tjänst än när det genomförs på traditionellt sätt på papper.

Infrastrukturen för svensk e-legitimation ger av denna anledning utrymme för e-legitimationer med olika säkerhetsegenskaper. Kraven i Tillitsramverket är fördelade på tre olika skyddsklasser – tillitsnivåer – som svarar mot olika grader av säkerhet i den resulterande elektroniska legitimeringen. Nivåindelningen motsvarar även den som följer av Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS) och genomförandeförordningen (EU) 2015/1502 om fastställande av tillitsnivåer.

De faktiska krav som blir tillämpliga på de olika tillitsnivåerna bestäms genom en samlad riskbedömning där förekomster av hotbilder vägs mot tillgänglig teknik, kostnader, användbarhet och andra nyttor.

I utarbetandet av tillitsramverket har särskild hänsyn tagits till att etablera en teknikneutral kravställning som ger långsiktighet, kostnadseffektivitet och förutsebarhet, samtidigt som det blir möjligt att genom varsamma förändringar möta förändrade hotbilder.

Det är tillhandahållaren av e-tjänsten som väljer vilken tillitsnivå som ska krävas för

en viss transaktion. Denne bör då tillämpa ett riskbaserat förhållningssätt, där den aktuella transaktionens art och den hotbild som existerar styr valet.

För att underlätta denna bedömning och att samordna den med en lämplig tillitsnivå utgår definitionen av tillitsnivåerna från en konsekvensbaserad modell för riskbedömning som bland annat framgår av den internationella standarden ISO/IEC 29115:2014 (dock ursprungligen definierad av den amerikanska budget- och förvaltningsstyrningsbyrån (OMB) år 2003 genom en PM benämnd M-04-04). Modellen är indelad i graderna begränsade, måttliga, betydande och allvarliga. Valet av tillitsnivå för en e-tjänst görs genom en avvägning utifrån sex riskområden och vad en felaktig legitimering skulle kunna föra med sig för negativa konsekvenser.

Tabellen ska läsas så att respektive tillitsnivå möter en viss riskprofil, där riskerna inom vart och ett av de angivna områdena inte får överstiga den angivna konsekvensgraden. Risker kan naturligtvis förekomma inom flera områden, och det är inte osannolikt att en felaktig identifiering kan leda till negativa konsekvenser inom flera områden. Det blir då det område inom vilket de svåraste konsekvenserna kan förekomma som blir styrande för vilken tillitsnivå som krävs. Förekomst av flera risker inom olika områden avses alltså som huvudregel inte räknas som kumulativa.

Figur 3.2 – Tillitsnivåer och riskprofiler

Konsekvensgraderna överensstämmer även med de nivåer som Myndigheten för samhällsskydd och beredskap (MSB) definierat i skriften Modell för klassificering av information. Till dessa nivåer har emellertid i riskbedömningsmodellen tillförts den lägre graden begränsade konsekvenser, i syfte att helt överensstämma med de internationella och vedertagna principer som råder inom området. Av samma anledning förekommer i modellen tillitsnivå 1 som svarar mot en elektronisk identifiering där användarens verkliga identitet inte är verifierad. Denna tillitsnivå har ingen motsvarighet i tillitsramverket för Svensk e-legitimation, då den inte utgör en legitimation i verklig mening.

Tillitsnivå 2, som något förenklat avses motsvara det skydd en personlig engångskod förmedlad via reguljär postgång ger, ska kunna användas vid enklare ärenden där personlig kod i många fall redan idag används. Exempel på sådan enklare identifiering är godkännande av deklaration via telefon eller mobilapplikation, ställa av eller på fordon, se sammandrag av trängselskattebeslut, etc. Tillitsnivå 2 är också utformad för att kunna användas av

minderåriga inom till exempel skolväsendet.

För Svensk e-legitimation av tillitsnivå 3 är avsikten att den ska ge motsvarande skyddsnivå som den traditionella fysiska legitimationshandlingen, samtidigt som en sådan e-legitimation ska kunna tillhandahållas och användas på ett så effektivt sätt som möjligt. Det är också denna nivå av tillit som de e-legitimationer som tillhandahålls genom Finansiell ID-teknik AB (BankID) normalt uppfattas nå upp till.

För tillitsnivå 4 tillkommer ytterligare krav på skydd vid utgivning och hantering i övrigt, och avses svara mot de allra högsta skyddsbehoven. De centrala delarna av denna tillkommande kravställning är att utgivning eller förnyelse av e-legitimationen aldrig kan ske på distans, särskilt stringenta krav på utfärdarens internkontroll tillämpas samt krav på fysiskt skydd av e-legitimationshandlingen (t.ex. koddosa eller aktivt kort).

Kontroll av efterlevnad

Allt eftersom användningen och spridningen av e-legitimationer har ökat, och samhällets beroende till denna infrastruktur har kommit att bli allt mer kritisk, har frågan aktualiserats hur det kan säkerställas att e-legitimationsutfärdare efterlever de uppställda säkerhetskraven. Detta är avgörande för att samhällets aktörer, vare sig de verkar inom den offentliga sektorn eller är privata aktörer, ska kunna fästa och upprätthålla en tillit till infrastrukturen.

Mer omfattande säkerhetsincidenter kan, beroende på incidenternas art, drabba tilltron till hela infrastrukturen för e-legitimering och snabbt undergräva förtroendet bland såväl invånare som förlitande parter. Myndigheten för digital förvaltning, i rollen som upphandlare av e-legitimering, har därmed ett långtgående ansvar att säkerställa att samtliga utfärdare från tid till annan upprätthåller rätt skydd för att sådana förtroendekriser inte skall uppkomma. Myndigheten måste också kunna utveckla och anpassa skyddsnivån efter omvärldens krav och förändrade hotbilder, samt förmåga att vidta kraftfulla och omedelbara åtgärder vid händelse av allvarliga brister.

Det verktyg som står myndigheten till buds är kontroll av efterlevnad genom de anslutningsavtal som tecknas med leverantören för att delta i valfrihetssystemet. Innan sådant anslutningsavtal tecknas med en leverantör genomgår denne en ingående granskning gentemot tillitsramverkets krav. Efter avslutad och godkänd granskning kan myndigheten fatta tilldelningsbeslut för deltagande i valfrihetssystemet. Genom avtalets tecknande förbinder sig leverantören att förhålla sig följsam gentemot kraven i tillitsramverket under avtalstiden, och även att regelbundet rapportera eventuella inträffade säkerhetsincidenter. Avtalet ger även myndigheten rätt till insyn i verksamheten och under vissa förutsättningar att vidta vidare granskningsåtgärder.

Det ska alltså noteras att rätten att granskas har en civilrättslig grund genom anslutningsavtalet. Något lagstadgat tillsynsansvar över utfärdarnas verksamheter finns inte. Hade så varit fallet hade tillsynsmyndigheten kunnat meddela de förelägganden som behövs för efterlevnaden av denna lag eller de föreskrifter som har meddelats med stöd av lagen, och att beslut om föreläggande kan förenas med vite i den mån det anses nödvändigt för att nå rättelse.

Inom ramarna för svensk e-legitimation har någon lagstadgad tillsynsroll emellertid inte bedömts nödvändig, med hänsyn till de starka civilrättsliga avtalsrelationer som skapas mellan samtliga deltagande parter. Ändrade förutsättningar på området, exempelvis genom allvarlig förtroendekris eller tvingande Europeisk lagstiftning, kan dock leda till ett behov av att framöver se över möjligheterna att även ställa utfärdarnas verksamhet under offentlig tillsyn med stöd av lag.

4 Europeisk samverkan kring e-legitimationer

Den 1 juli 2016 trädde förordning (EU) 910/2014 om e-legitimationer och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS) i kraft, och blev därmed gällande i bland annat Sverige.

Genom regeringens proposition 2015/16:72 har också nationella regler införts som behövs för att komplettera förordningen, vilka också trädde i kraft 1 juli 2016.

Syftet med EU-förordningen är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan privatpersoner, företag och offentliga organ och därigenom öka effektiviteten hos offentliga och privata e-tjänster samt i elektronisk affärsverksamhet och e-handel inom EU.

Inom området elektronisk identifiering finns det utöver EU-förordningen fyra beslutade genomförandeakter (med beslutsnummer och förordningens artikel inom parentes):

1. samverkan rörande elektronisk identifiering (2015/296, art. 12.7),
2. tillitsramverk (tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering, 2015/1502, art. 8.3),
3. interoperabilitetsramverk (2015/1501, art. 12.8), samt
4. förutsättningar, format och förfaranden för anmälan (2015/1984, art. 9.5).

Regeringen har med hjälp av bl.a. E-legitimationsnämnden och andra svenska myndigheter varit aktiv i EU:s arbete med att specificera tillitsnivåer och interoperabilitet på EU-nivå, och de svenska tillitsnivåerna 2, 3 och 4 avses motsvara eIDAS tillitsnivåer låg, väsentlig och hög.

eIDAS innebär ett obligatorium för offentliga organ att i sina e-tjänster erkänna andra medlemsstaters e-legitimationer (system och medel för elektronisk identifiering) som anmälts och införlivats i eIDAS-infrastrukturen, på motsvarande tillitsnivå eller högre, under förutsättning att e-tjänsten använder elektronisk identifiering på åtminstone tillitsnivå väsentlig enligt eIDAS. Motsvarande gäller frivilligt för privat sektor, samt frivilligt för offentliga organ och privat sektor i de e-tjänster som accepterar elektronisk identifiering på tillitsnivå låg. Det är kostnadsfritt för svenska myndigheter i förhållande till utlandet att nyttja erkända e-legitimationer över landsgränserna.

5 Vad är en e-legitimation?

Det saknas en legaldefinition av vad en e-legitimation är, men vanligen avses de tekniska lösningar som upphandlats av det offentliga. Dessa är för närvarande:

- BankID (Finansiell ID-teknik AB)
- Telia e-legitimation (Telia Sverige AB)
- Skatteverkets ID-kort (AB Svenska Pass)
- Freja eID+ (Verisec Freja eID AB)

De e-legitimationer som myndigheter godtar har emellertid alltid urkundskvalitet enligt brottsbalken (BrB). Med urkund menas enligt legaldefinitionen i 14 kap. 1 § BrB en elektronisk handling som upprättats till bevis eller annars är av betydelse som bevis och som har utställarangivelse som kan kontrolleras på ett tillförlitligt sätt. Bestämmelsen fick denna utformning genom regeringens proposition 2012/13:74 Förfalsknings- och sanningsbrotten.

De tekniska hjälpmedel som tillhandahålls varierar. Medan Skatteverkets ID-kort och Telia e-legitimation tillhandahålls på aktiva kort, så är e-legitimationer från Freja eID+ och övervägande delen av alla BankID lösningar med App i innehavarens smarttelefon.

Vad som normalt inte benämns som e-legitimation är bankernas olika egna identifieringslösningar med stöd av t.ex. koddosor. Dessa kan dock i stor utsträckning tillmätas samma egenskaper, med den skillnaden att de endast kan brukas mot den bank som givit ut det tekniska hjälpmedlet och den hantering som omgärdar hjälpmedlet är inte föremål för någon gemensam kravställning.

5.1 Elektroniska underskrifter

En elektronisk underskrift är ett kryptografiskt framställd informationsmängd som kan fogas till en handling som gör det möjligt att i efterhand med mycket hög tillförlitlighet kontrollera vem som skrivit under handlingen, när underskriften skedde och att handlingen inte ändrats (att den är äkta) sedan underskriften gjordes.

Vissa typer av e-legitimationer har stöd för att genomföra elektroniska underskrifter, andra har endast legitimeringsfunktion. För att underteckna en handling elektroniskt krävs ibland även att innehavaren installerar vissa särskilda programvaror i sin dator. Dessa faktorer har medfört att det växt fram *underskriftstjänster* för såväl kommersiellt bruk och sådana som möter myndigheternas behov. En underskriftstjänst kan liknas vid en notariatstjänst där tjänstetillhandahållaren i ett första steg säkert identifierar den som ska skriva under med stöd av dennes e-legitimation, och sedan tekniskt framställer den kryptografiska underskriften på innehavarens vägnar. Beroende på sammanhang kan förfarandet också innefatta att visa vad som ska skrivas under och utforma gränssnitt på ett sådant sätt att underskriften sedan uppfyller de legala krav som ställs.

En elektronisk underskrift skiljer sig från en med penna egenhändigt framställd underskrift på så sätt att förfalskningar av en egenhändig underskrift kan låta sig göras genom skriftanalys. Den elektroniska underskriftens äkthet kan förvisso kontrolleras med närmast

absolut säkerhet, men huruvida den anbringats handlingen av en behörig person är betydligt svårare att kontrollera. Därav har den elektroniska underskriften mer säkerhetsmässig karaktär av att vara en stämpel. Högsta domstolen har också i ett vägledande avgörande, NJA 2017 s. 1105, uttalat att bedömningen av om en elektronisk underskrift binder undertecknaren består således av två moment: först ska det prövas om den aktuella underskriften är äkta, och därefter vem som anbringat den.

Elektroniska underskrifters rättsliga status regleras i EU-förordningen 910/2014 (eIDAS). Där framgår att elektroniska underskrifter ska ges samma rättsverkan som egenhändigt framställda underskrifter, i alla situationer där det saknas formkrav i nationell författning. Sådana formkrav förekommer bl.a. i Jordbalken (1970:994) och Ärvdabalken (1958:637).

Genom eIDAS-förordningen definieras elektronisk underskrift, avancerad elektronisk underskrift och kvalificerad elektronisk underskrift. Kortfattat kan dessa olika former av elektroniska underskrifter något förenklat kategoriseras enligt följande:

- *Elektronisk underskrift* kan tillkomma på icke-definierat sätt. Till exempel genom att de undertecknade parterna endast identifieras genom utväxlande av e-postadresser.
- *Avancerad elektronisk underskrift* grundas i någon form av e-legitimation och underskriften som sådan avses ha urkundsstatus.
- *Kvalifierad elektronisk underskrift* en avancerad elektronisk underskrift som skapats genom användning av en kvalificerad betrodd tjänst som ska uppfylla vissa tämligen allmänt hållna funktions- och säkerhetskrav som framgår av förordningen och som står under myndighetstillsyn.

I Sverige förekommer inte kvalificerade underskrifter, och i de formkrav som numera återfinns i ett stort antal lagar preciseras användning av avancerade elektroniska underskrifter.

När krävs elektroniska underskrifter?

Det finns ett allmänt behov i samhället av att kunna lita på att handlingar är äkta, dvs. att de oförvanskat härrör från den som framstår som utställare. När till exempel avtalshandlingar ges in på papper brukar det därför vara en självklarhet att de ska vara undertecknade. Regeringen har i propositionen 2012/13:74 Förfalsknings- och sanningsbrotten förklarat att en underskrift normalt anses innebära att undertecknaren utfärdar en garanti för att handlingen är äkta samt att underskriften också ofta får anses betyda att utställaren tänkt sig för, förstått innebörden av handlingen och menat sig bli bunden av den (s. 60). Underskrifter fyller alltså olika

1. informationssäkerhetsrelaterade funktioner, såsom
    a. autentisering (visa vem undertecknaren är och att handlingen är äkta),
    b. bevissäkring (ett skriftligt bevis skapas), och
    c. originalkaraktär (det blir möjligt att skilja mellan ett oförvanskat original vars äkthet kan kontrolleras och lätt manipulerbara kopior),
2. rättsligt relaterade funktioner, såsom
    a. avslutningsfunktionen (att innehållet är fullständigt och förenligt med undertecknarens vilja),
    b. varningsfunktionen (att tänka sig för och förstå åtgärdens innebörd), och
    c. den straffrättsliga funktionen (den som manipulerar kan i vissa fall dömas för brott).

Beträffande de rättsligt relaterade funktioner som en underskrift fyller kan det övervägas om tydligt utformade användargränssnitt kan ge samma distinkta och tydliga avslutnings- och varningsfunktion som vid elektronisk underskrift. Det kan på motsvarande sätt övervägas om de informationssäkerhetsrelaterade funktionerna vid underskrift kan återskapas genom alternativa förfaranden, så att det i efterhand kan säkerställas att uppgifterna inte blivit ändrande, och att det med hög trovärdighet går att härleda uppgifterna till den person som lämnande dem.

Vilka krav som bör ställas är således både en juridisk fråga och en informationssäkerhetsfråga. Ett beslut om elektroniska underskrifter ska krävas i en e-tjänst bör därför grundas både på en riskanalys av systemet och en analys av tillämpliga rättsliga krav. Avstår tillhandahållaren av en viss tjänst från att nyttja elektroniska underskrifter gäller emellertid inte bestämmelserna om ansvar för förfalsknings- och sanningsbrott och de särskilda formkrav som anger att avancerade elektroniska underskrifter ska användas är inte uppfyllda.

Allmänt om underskriftstjänster

De underskriftstjänster som godkänts av Myndigheten för digital förvaltning, och tidigare E-legitimationsnämnden, uppfyller samma specifikationer. Dessa specifikationer omfattar tekniska krav, krav på gränssnitt, säkerhetsrelaterade krav och krav på servicenivåer. De olika leverantörernas tjänster anses alltså vara tekniskt, funktionellt och säkerhetsmässigt likvärdiga i samtliga relevanta avseenden.

Förutsättningen för underskriftstjänsten är också att själva handlingen som ska skrivas under inte behöver överföras till leverantören. Istället överförs ett elektroniskt fingeravtryck av handlingen (ett kryptografiskt kondensat, så kallad hash). Från detta fingeravtryck går det inte att återskapa några delar av urprungshandlingens innehåll. På så sätt röjs inga uppgifter för leverantören av underskriftstjänsten. Underskriftstjänsten tillhandahåller därför inte heller något användargränssnitt, annat än felmeddelanden vid sådana tillfällen då underskrift inte kan skapas.

Det är således tillhandahållaren av e-tjänsten som ansvarar för att på ett tydligt sätt presentera den handling som användaren ska underteckna, så att denne kan granska och göras införstådd med innebörden av undertecknandet.

Då användaren godtagit att skriva under handlingen och denne legitimerat sig gentemot underskriftstjänsten, skapas ett nyckelpar och ett underskriftscertifikat som knyts till användaren. Därefter skapas själva underskriften och den hemliga delen av användarens nyckel förstörs sedan direkt därefter.

Det har dock visat sig, som framgår i det sista avsnittet i denna PM, att vissa kommersiellt tillgängliga underskriftstjänster inte fungerar på detta sätt, och därför knappast kan tillskrivas motsvarande rättsliga och tekniska säkerhetsegenskaper.

6 Missbruk av e-legitimationer

Med en bredare användning av e-legitimationer har olika former av missbruk och bedrägerier följt. Bedrägerierna syftar oftast till att snabbt komma över pengar på ett eller annat sätt, antingen genom att plundra innehavarens tillgodohavanden i bank eller hos myndighet, eller att ta upp lån i innehavarens namn.

Bedragarnas modus är vanligen ett av två följande alternativ:

- Att söka kontakt med den enskilde, oftast via telefon, och övertala vederbörande att ta fram sin e-legitimation och genomföra vissa åtgärder som bedragaren instruerar. Bedragarna utger sig ofta att vara från banken, och kontakten sker under förevändning att några obehöriga transaktioner sker på kontot, och innehavaren måste legitimera sig för att de ska kunna stoppa transaktionerna.

- Att försöka tillskansa sig en e-legitimation i någons namn på obehörig väg, till exempel genom användande av förfalskade fysiska legitimationshandlingar, för att denna väg öppna ett bankkonto och sedan i nästa steg hämta ett BankID som kan nyttjas för att ta upp lån eller överföra pengar från konton i annan bank.

Den övervägande delen av alla bedrägerier sker enligt det första av de två tillvägagångssätten. Detta sätt att luras har skett i sådan omfattning att problemen på senare tid fått stor uppmärksamhet i media. Vad som sällan framkommer är att bedragarna i första hand är inriktade på bankdosorna, även om det förekommer att BankID också används. Uppgifter i media gör gällande att så mycket som 82 procent av alla bedrägerier av den här typen har sin grund i bankdosor.

Med hjälp av svarskoder från bankdosan har bedragarna kunnat erhålla ett BankID, och kan med hjälp av detta genomföra ett stort antal överföringar till andra konton. Det är också med detta nyutfärdade BankID möjligt att hinna plundra konton som innehavaren har i andra banker innan kontohavaren förstår vad som är i görningen och hinner spärra e-legitimationen. Denna form av bedrägerier har förekommit i systematisk form i över ett decennium. Bedragarna har på senare tid dock blivit alltmer slipade och pålästa kring offret och offrets privatliv. Problemen har därvid tilltagit under 2017 och 2018.

Det andra alternativet, att genom förfalskade fysiska legitimationshandlingar skaffa en e-legitimation i annans namn, är väsentligt svårare att genomföra i större skala, och är förknippat med betydande risker att åka fast då viss fysisk interaktion vanligen krävs. Dessutom har e-legitimationsutfärdarnas rutiner och vaksamhet skärpts på senare tid, vilket ytterligare försvårat genomförandet. Tillvägagångssättet är dock effektivare då bedrägeriet inriktas på en specifik individ, då de allra flesta trots allt inte faller för bluffmakeriet beskrivet ovan. Därför kvarstår detta modus som en angreppsväg som kontinuerligt måste stävjas genom olika förebyggande och reaktiva åtgärder. Att förbättra de fysiska legitimationshandlingarnas säkerhetsegenskaper förväntas vara en särskilt effektiv åtgärd. Under 2017 tillsatte regeringen en särskild utredare som ska utreda och lämna förslag till åtgärder för att minska det ökande antalet bedrägerier som begås med hjälp av förfalskade fysiska id-handlingar. Enligt kommittédirektivet ska uppdraget redovisas senast 29 mars 2019.

6.1 Åtgärder mot missbruk

Som tidigare nämnts är brister i säkerheten i de fysiska legitimationshandlingarna av betydelse även för e-legitimationer. Teknik avsedd för hemmabruk kan idag användas för att tillverka förfalskade legitimationshandlingar som i vart fall inte uppenbart kan skiljas från äkta. Spärr- och giltighetskontroll av fysiska legitimationshandlingar sker fortfarande via telefon mot den som utfärdat legitimationahandlingen, en process som inte sällan kan ta uppåt 10 minuter att genomföra. Det säger sig själv att detta inte kan göras varje gång vid den hantering som krävs vid till exempel ett postutlämningsställe för rekommenderade brev eller vid ett kundmöte i en bank. Legitimationshandlingar som istället på ett tillförlitligt sätt kunde läsas av elektroniskt, och i denna process även äkthets- och spärrkontrolleras automatiskt, kan förväntas öka säkerheten vid sådana personliga möten högst väsentligt. Detta naturligtvis under förutsättning att dessa fysiska legitimationshandlingar ges ut på ett säkert sätt.

6.2 Användningen av personnummer

Personnummer tilldelas alla personer folkbokförda i Sverige, och används av bl.a. myndigheter för att unikt identifiera en person. Användningen av personnummer utmålas ofta som förknippat med risk för identitetsstölder. I det följande görs en allmän genomgång av personnummeranvändningen i Sverige, den reglering som detta omgärdas av, och följder av personnummeranvändningen.

Allmänt om personnummer

Tilldelningen av personnummer och registreringen i folkbokföringsregistret sker genom Skatteverkets försorg och regleras i folkbokföringslagen (1991:481). Folkbokföringen innebär fastställande av en persons bosättning samt registrering av uppgifter om identitet, familj och andra förhållanden, som enligt lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet, får förekomma i folkbokföringsdatabasen.

Tillgång till uppgifter i folkbokföringshandlingar regleras i offentlighets- och sekretesslagen. Sekretess för personuppgifter gäller om det av särskild anledning kan antas att den enskilde eller någon honom närstående lider men om uppgiften röjs (22 kap. 1 § offentlighets- och sekretesslagen 2009:300). Ett s.k. rakt skaderekvisit uppställs, dvs. offentlighet uppställs som huvudregel, sekretess gäller endast om det kan antas att skada uppkommer om uppgiften röjs. Det måste således föreligga någon särskild anledning för att sådana uppgifter ska få hemlighållas.

För uppgifter om namn, adress, personnummer och civilstånd gäller alltså normalt inte någon sekretess.

Statens Personadressregister (SPAR)

Direktåtkomst till uppgifterna i folkbokföringsdatabasen är noga reglerad, och bestäms i förordning (2001:589) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet. För ändamål som inte faller inom ramen för det som anges i denna lag tillgodoser Skatteverket samhällets informationsförsörjningsbehov av befolkningsinformation via det statliga personadressregistret (SPAR).

SPAR bildades 1978, på Datainspektionens initiativ, för att begränsa möjligheterna för myndigheter och enskilda att med hjälp av dåtidens nya teknik, s.k. automatisk databehandling (ADB), föra omfattande personregister. Ett statligt befolkningsregister med monopollik-

nande ställning och under betryggande kontroll ansågs bättre från integritetssynpunkt än ett flertal offentliga och privata personregister.

SPAR är ett offentligt register som omfattar alla personer som är folkbokförda i Sverige, och uppdateras varje dygn med en delmängd av uppgifterna som finns lagrade i folkbokföringsregistret.

När personuppgifter behandlas i SPAR gäller den Europeiska dataskyddsförordningen (EU 2016/679) och lagen (1998:527) om det statliga personadressregistret. Syftet med SPAR framgår av de ändamål som anges i 3 §, där personuppgifter får behandlas för att:

- aktualisera, komplettera och kontrollera personuppgifter,
- ta ut uppgifter om namn och adress genom urvalsdragning för direktreklam, opinionsbildning eller samhällsinformation, eller annan därmed jämförlig verksamhet.

Att behandla uppgifter är i detta avseende det samma som att lämna ut uppgifterna elektroniskt. Uppgifter i SPAR lämnas ut elektroniskt efter beslut av Skatteverket.

Enligt 4 § får SPAR innehålla uppgifter om personer som är folkbokförda i landet och personer som har tilldelats personnummer enligt 18 b § folkbokföringslagen (1991:481). SPAR får även innehålla uppgifter om personer som har tilldelats samordningsnummer, om det inte råder osäkerhet om personernas identitet.

Offentlighetsprincipen och personnummer

Den tekniska utvecklingen har inneburit att offentlighetsprincipen nu får andra följder än tidigare, eftersom uppgifter i allmänna handlingar blivit mer lättåtkomliga och massuttag av personuppgifter har blivit möjliga.

Kreditupplysningsregistren används till exempel inte längre enbart för kreditupplysningsverksamhet. Flera kreditupplysningsföretag har skaffat sig utgivningsbevis med stöd av YGL (yttrandefrihetsgrundlagen, 1991:1469), och distribuerar därigenom uppgifter från sina kreditupplysningsregister. Eftersom YGL gäller framför vanlig lag blir effekten att kreditupplysningsföretagen varken behöver följa kreditupplysningslagen eller persondataskyddsförordningen. De kan därmed tillhandahålla personuppgifter för andra ändamål än kreditupplysning.

Denna spridning av offentliga personuppgifter har medfört att det är nära på trivialt slå upp en invånares namn, adress, person-/samordningsnummer, inkomst och civilstånd.

Sverige har på detta sätt ett av världens mest öppna förhållningssätt till spridning och insyn i invånarnas personuppgifter. I andra länder tillämpas ofta andra seder och bruk som följd av en helt annorlunda syn på hanteringen av personuppgifter och identiteten i stort. I flertalet av jämförliga länder finns visserligen någon variant av nationellt identitetsnummer, ofta baserat på skattenummer eller socialförsäkringsnummer, men där dessa är sekretessbelagda och förväntas vara en uppgift som endast myndigheten och innehavaren känner till.

Detta har medfört att kännedom om identitetsnumret ofta används som metod för att bestyrka en identitet, ibland i kombination med att personen i fråga kan visa upp en handling med anknytning till bostadsadressen, som t.ex. el- eller gasräkning.

Omvänt finns i andra länder ofta en större öppenhet i bankväsendet, där uppgifter om en invånares förehavanden med banken kan exploateras i olika syften. Bankuppgifter (via kreditupplysningsregister) används därför också frekvent för att verifiera en persons identitet, t.ex. genom att kontrollera att ett angivet bankkonto tillhör en viss person, eller genom att kontrollera saldo eller förekomst av en viss transaktion.

Dessa seder och bruk har lett till omfattande problem med identitetsstölder. Personuppgifter kan röjas genom att identitetstjuvar letar igenom sopor eller genom att försöka lura av

offret personuppgifter via s.k. nätfiske. Uppgifterna kan sedan användas för att t.ex. ta lån, ansöka om kreditkort eller teckna mobiltelefonabonnemang.

Risker med personnummer

Den spridning av personuppgifter som den tekniska utvecklingen medfört kan förvisso ses som problematisk från ett integritetsperspektiv. Men som erfarenheter från andra länder visat, lindras inte risker för identitetsstölder genom att omgärda sådan hantering av personuppgifter med sekretess.

Personuppgifterna används i många olika sammanhang, är ofta oförändrade under lång tid, och den enskilde saknar effektiva verktyg att skydda dem. Därigenom ökar snarare problemen med identitetsstöld i den mån tillhandahållare av olika tjänster förlitar sig på att det endast är den som uppgifterna rör som också känner till dem. Den öppenhet som existerar i Sverige kring de grundläggande personuppgifterna förhindrar snarare missbruket av personuppgifter än tvärt om.

7 Skyddet för enskilda vid användning av e-legitimationer

Som tidigare beskrivits finns ingen legaldefinition av vad en e-legitimation är, och i det följande avses inte endast sådana elektroniska ID-handlingar som används för legitimering mot myndigheter, utan även de bankdosor som de flesta banker idag nyttjar för åtkomst till respektive internetbank.

Det har vid genomgången visat sig att det övervägande antalet av polisanmälda bedrägerier rör just bankdosor. Bedragarna kontaktar den enskilde på något sätt och lurar vederbörande att släppa in bedragarna i deras internetbank. Varför bankdosorna missbrukas i så stor omfattning är inte klarlagt. Möjligen kan det förklaras av att de är mera spridda än BankID, särskilt i de grupper som bedragarna inriktar sig på.

Är då bankdosorna ett osäkert medel för identifiering? Från teknisk synvinkel är bankdosan mycket säker. Den är skyddad mot kopiering och har en personlig kod för att låsas upp. Om fel kod anges ett visst antal gånger gör det dosan obrukbar. De kryptografiska metoder som används för att framställa engångskoderna är starka. Ytterligare säkerhet påförs på så sätt att det mellan bankdosan och webbläsaren finns en luftspalt som måste överbryggas av en människa. En angripare kan därmed inte på distans ta sig in i användarens dosa och kopiera eller använda dess innehåll. Det krävs inte heller installation och underhåll av särskilda programvaror för att den ska fungera, vilket borgar för god användbarhet. Nackdelen med bankdosan är att den ofta lämnas utan uppsikt under lång tid, då den bara brukas när innehavaren ska göra bankärenden. Någon i innehavarens närhet som snappat upp den personliga koden kan sedan obehörigen nyttja dosan utan innehavarens vetskap.

Det andra utbredda medlet för elektronisk identifiering är Mobilt BankID. Det är en applikation som installeras i innehavarens smarttelefon eller surfplatta, och som sedan genom vissa förfaranden (ofta genom att använda bankdosan i internetbanken) knyts till innehavaren. Mobilt BankID har blivit mycket populärt, inte minst då innehavaren i princip alltid har sin mobiltelefon nära till hands. Det krävs inte heller att användaren till banken manuellt överför de kryptografiska svarskoder som framställs, utan detta sker genom mobiltelefonens internetuppkoppling och BankID-infrastrukturen. Mobilt BankID kan också användas i många olika tjänster, inte bara i en viss internetbank.

En svaghet som Mobilt BankID dragits med är dels att personnummer används för att koppla samman den elektroniska legitimering som sker via telefonen med den faktiska inloggningen, dels att inloggningen kan ske i annan enhet än den där använt BankID finns installerat (t.ex. en mobiltelefon) tillsammans med viss programvara.

Eftersom personnummer är offentliga har bedragaren kunnat initiera en inloggningssession för att sedan förmå offret att genomföra en legitimering. Detta har – när vilseledandet lyckats – gett bedragaren den åtkomst som denne behövt för att fullborda ett bedrägeri. Att nyttja personnumret har förstås också en användbarhetsaspekt, då var och en normalt har detta memorerat. Alla former av personliga koder som skulle matas in istället för personnumret hade komplicerat legitimeringsförfarandet, och det är knappast givet att det skulle

leda till en högre säkerhet. Det hade möjligen krävts att bedragaren lotsar offret genom ytterligare ett steg, men som problemen med bankdosorna visat är det inget hinder.

Till detta kommer att inloggning kan ske genom valfri annan dator än den där använt BankID finns installerat. Finansiell ID-teknik har dock nyligen infört ett alternativt förfarande där en optisk kod läses in med mobiltelefonens kamera. Denna kod kan inte knappas in manuellt, utan måste på något sätt tillsändas offret för att bedrägeriet ska kunna fullbordas. Det är en bra förbättring som förlitande e-tjänster successivt förväntas börja nyttja. Åtgärden är sannolikt effektiv mot bedrägerier som genomförs över telefon, men hjälper inte då offret på något sätt leds till en falsk webbplats som kan spegla den optiska koden.

Mobilt BankID är ett exempel på en lösning som blivit mycket populär för att den kombinerar god användbarhet med väl avvägd säkerhet. Vid en jämförelse med andra säkerhetslösningar går det inte att dra slutsatsen att Mobilt BankID skulle vara svårare att använda säkert.

Några säkerhetstekniker som möjliggör identifiering på distans och som inte i någon del beror på viss aktsamhet från den enskildes sida är i dagsläget inte kända. Inte heller traditionella tillvägagångssätt erbjuder absolut säkerhet. Det finns dock en skillnad mellan automatiserad masshantering och personliga besök på till exempel ett bankkontor. En person som kommer in på ett bankkontor med avvikande beteende och som önskar genomföra en rad riskfyllda transaktioner kommer att nekas, eller i vart fall utsättas för särskilt ingående extra kontroller för att kompensera en ökad risk. När motsvarande riskfyllda beteende äger rum med ett BankID fungerar emellertid det automatiserade tillvägagångssättet på samma sätt som vid en transaktion som inte präglas av särskilda risker. Rimlighetsspärrar för särskilt riskfyllda transaktioner och ovanliga användningsmönster måste dock enligt min mening även finnas på plats vid den automatiserade behandlingen. Om en sådan rimlighetsspärr löser ut kan det komma att krävas att en tjänsteman gör en manuell granskning och utför eventuella tillkommande kontroller av diverse slag, innan denna tar beslut om att den ifrågavarande transaktionen ska genomföras. Införandet av sådana rimlighetskontroller ankommer således på tillhandahållaren av tjänsten (t.ex. internetbanken), då det endast är denna som har tillgång till de uppgifter som krävs för kontrollen.

Det är därför enligt min mening inte rimligt att ålägga den enskilde ett obegränsat ansvar för obehöriga transaktioner med BankID eller bankdosa.

7.1 Ansvar och bevisbörda

Vid hantering och användning av e-legitimationer deltar åtminstone tre parter som står för olika led i den tekniska och administrativa processen vid en legitimering; *utgivaren* av medlet för elektronisk identifiering, *innehavaren* av detta medel och *tillhandahållaren av den tjänst* som förlitar sig på legitimeringen.

Däremellan kan två tillkommande parter finnas som vanligtvis inte är synliga för innehavaren av en e-legitimation. De är *utställare av identitetsintyg* och leverantör av *underskriftstjänst*, som tillhandahåller stödtjänster för att infrastrukturen ska fungera på ett bra sätt. Utställare av identitetsintyg är en part som säkert identifierar en innehavare som har använt sin e-legitimation. När en sådan identifiering har lyckats ställer denne ut ett elektronisk intyg om detta i ett standardiserat format, ett s.k. identitetsintyg. Nyttan med detta steg är att identitetsintyget eliminerar behovet för varje tillhandahållare av e-tjänst göra en egen kontroll av en legitimering. Det räcker att lita på intyget. På detta sätt slipper också varje tillhandahållare av e-tjänst att göra tekniska integrationer mot (dvs. koppla ihop sina system

med) var och en av utfärdarnas e-legitimationslösningar. Underskrifttjänstens funktion har beskrivits i tidigare avsnitt.

Den enskilde har sällan någon möjlighet att påverka de säkerhetslösningar som tillhandahålls. Ansvaret för att en tjänst som erbjuds är säker att använda vilar på tillhandahållaren, innefattande samtliga bakomliggande tjänsteleverantörer (utfärdare av e-legitimation, utställare av identitetsintyg och tillhandahållare av underskriftstjänst).

De kravställningar och avtal som blir tillämpliga mellan var och en av dessa leverantörer blir således av avgörande betydelse för ansvarsfördelningen.

Utfärdare av e-legitimationer och tillhandahållare av underskriftstjänster

För utfärdare av e-legitimationer och tillhandahållare av underskriftstjänster gäller normalt ett metodansvar. De ska efterleva de säkerhetsregler och andra villkor som ställs upp i de anslutningsavtal som tecknas (dessa aktörers verksamheter regleras alltså normalt inte lag) men lovar inte ett visst resultat. Har t.ex. en enäggstvilling använt sin brors körkort för att få en e-legitimation kan detta ha skett på ett så utstuderat sätt att utfärdaren har uppfyllt alla metodkrav.

Säkerhetskrav och skadeståndsskyldighet måste således tämligen detaljerat preciseras i de avtal (förlitandeavtal) som tecknas mellan tillhandahållare av e-tjänst (förlitande part) och utställare av identitetsintyg respektive tillhandahållare av underskriftstjänster. De måste också preciseras för utgivaren av medlet för elektronisk identifiering när denne är part i berörda avtal. Saknas förlitandeavtal är det mer tveksamt om förlitande e-tjänst kan begära ersättning för ren förmögenhetsskada på grund av att en tjänstetillhandahållare inte följt säkerhetskraven. Ren förmögenhetsskada, dvs. ekonomisk skada som inte har samband med en person- eller sakskada, berättigar till ersättning enbart i kontraktsförhållanden eller kontraktsliknande förhållanden eller när skadan har orsakats genom brottslig handling. Denna grundläggande princip inom skadeståndsrätten följer av 2 kap 2 § skadeståndslagen där det föreskrivs att den som vållar ren förmögenhetsskada genom brott ska ersätta skadan. Detta har dock inte ansetts hindra en utveckling i rättspraxis i riktning mot ett vidgat ansvar för ren förmögenhetsskada; se bl.a. NJA 1987 s. 692 (det s.k. Konefallet). De fall som är aktuella här rör utpräglade tillitstjänster, där det inte kan uteslutas att det vid en kommande domstolsprövning anses befogat att lita på en sådan tjänst även utan förlitandeavtal. I så fall skulle ersättning för ren förmögenhetsskada även kunna komma ifråga vid vårdslöshet från tillhandahållarens sida. Rättsläget är emellertid osäkert och en vanlig innehavare av e-legitimation kan knappast driva en sådan process och inte heller stå risken för de rättegångskostnader som drabbar denne vid en förlust.

En sådan skadeståndsskyldighet skulle knappast heller utgöra ett tillräckligt incitament för att uppnå en mer preciserad skyddsnivå. Tillitsramverket för Svensk e-legitimation är därför en avgörande del i den kravställning som bör ingå i varje förlitandeavtal som tecknas med en utgivare av medel för elektronisk identifiering. Dessutom saknas motsvarande kravställning för underskriftstjänster, vilket visat sig vara problematiskt.

Det har framkommit att vissa kommersiellt förekommande underskriftstjänster har sådana egenskaper i termer av säkerhet och tillförlitlighet att de inte borde anses resultera i avancerade elektroniska underskrifter. Högsta domstolens vägledande avgörande i NJA 2017 s. 1105 bygger på bedömningen att det varit fråga om en avancerad elektronisk signatur i det aktuella fallet. Den bevisning som åberopats bestod emellertid i en promemoria från Finansinspektionen. Bakgrunden är Finansinspektionens föreskrifter och allmänna råd

om åtgärder mot penningtvätt och finansiering av terrorism (FFFS 2009:1), där föreskrifter finns om identifiering av fysisk person på distans. Det kan ske bl.a. genom att använda e-legitimation för att skapa en avancerad elektronisk signatur enligt definition i 2 § lagen (2000:832) om kvalificerade elektroniska signaturer eller att använda någon annan motsvarande teknik för elektronisk identifiering (se 4 kap. 3 § FFFS 2009:1). Enligt samma föreskrift godtar emellertid Finansinspektionen från penningtvättsynpunkt också andra metoder, t.ex. att kunden skickar in en kopia av sin id-handling förenad med vissa andra kontroller där användning av e-legitimation framstår som en betydligt säkrare metod. Högsta domstolen har endast haft att pröva det som förs in i målet. Vad som prövats är dessutom om en viss använd teknik kan likställas vid en avancerad elektronisk underskrift.

Enligt min bedömning är det rimligt att anta att Högsta domstolen gjort en annan bedömning om dessa fakta presenterats fullt ut och rättsfrågan varit huruvida den använda metoden resulterat i en avancerad elektronisk signatur (inte fråga om den kan jämställas med en sådan eller om den kan anses uppnå en sådan lägre nivå som Finansinspektionen förefaller godta i penningtvättsammanhang).

Till detta kommer att den aktuella tjänsten nyttjat en teknik för identifiering som sätter sig mellan användaren och dennes internetbank och använder så kallad skärmskrapning (automatiserad avläsning av det som annars visas i användarens webbläsares fönster) för att bekräfta dennes identitet. Den legitimering som skett har alltså gått till så att undertecknaren – i stället för att besöka sin internetbank och logga in där – har besökt en annan webbplats där undertecknaren aktiverat sin bankdosa och via denna utbytt koderna med banken. Tillhandahållaren av den andra webbplatsen har härvid beretts åtkomst till kundens uppgifter i Internetbanken som resultat av att undertecknaren legitimerat sig med sin bankdosa.

Den tjänst som nyttjats för identifieringen inför underskriftsmomentet har alltså lurat banken att lämna ut information som tyder på att undertecknaren har en viss identitet. Om det därefter ska kontrolleras om resultatet av denna identifiering hos banken verkligen varit korrekt finns varken avtalsförhållanden eller annan rättslig grund för förlitande part att begära dessa uppgifter från banken.

Förfarandet torde strida mot 15 kap. 12 § första stycket BrB eftersom de bankdosor som används under alla omständigheter bör kunna tillskrivas urkundsstatus enligt definitionen i 14 kap. 1 § 2 stycket 2 i BrB. Genom att leverantören av identifieringstjänsten åberopar denna urkund som gällande för sig själv kan denne dömas för missbruk av urkund.

Detta har varken uppmärksammats av Finansinspektionen när inspektionen i sin promemoria godtagit beskrivet förfarande som motsvarande identifiering genom en avancerad elektronisk signatur, och inte heller av parterna när de fört sin talan i Högsta domstolen. Istället har Högsta domstolen utifrån det processmaterial som förts in i målet funnit att det varit fråga om en teknik som motsvarar avancerad elektronisk underskrift. Detta har sin grund i följande utsaga som tillhandahållaren av identifieringstjänsten själv avgivit:

”[...] ansåg sig bolaget ha en sådan betryggande teknisk lösning att ingen utomstående kan komma åt informationen innan den når företaget, som är deras kund.”

Denna således från såväl säkerhetsmässig som rättslig synvinkel högst tveksamma identifiering har sedan lagts till grund för att en signal skickats till den som beställt identifieringen. Ingen avancerad elektronisk underskrift har i varken teknisk eller juridisk mening

skapats, vilket framgår tydligt av promemorian och den övriga bevisföringen.

Detta blottlägger ett problemområde inom elektronisk legitimering och elektroniska underskrifter. Det vore önskvärt att PTS, som utöver tillsyn inom området elektroniska underskrifter, klargör vilka krav som ställs för att en underskriftstjänst ska anses tillhandahålla avancerade elektroniska underskrifter i rättslig bemärkelse.

Ett rimligt grundkrav är att tjänsten anmäls till tillsynsmyndigheten som betrodd tjänst, och att artikel 13 och 19 i eIDAS-förordningen därmed blir tillämpliga.

Innehavaren av en e-legitimation

Nämnda HD-avgörande belyser även ett annat problemområde i användandet av elektroniska underskrifter. I de fall då den underliggande e-legitimationen använts som ett betalningsinstrument gällde lagen (2010:738) om obehöriga transaktioner med betalningsinstrument (OTBIL) fram till den 30 april 2018. Reglerna om obehöriga transaktioner, som är tvingande till konsumentens fördel, återfinns sedan 1 maj 2018 i 5 a kap. lagen (2010:751) om betaltjänster (betaltjänstlagen). Vid ett bestridande av en transaktion åläggs tillhandahållaren av betaltjänsten genom denna lag bördan att visa att

1. kontoinnehavaren inte försummat sin skyldighet i fråga om att skydda betalningsinstrumentet och att
2. det system som använts för genomförande av transaktionen är tillförlitligt, har fungerar korrekt och inte påverkats av något tekniskt fel vid stunden för genomförandet av transaktionen.

Kan denne visa detta åligger det kontoinnehavaren att givet omständigheterna göra det *antagligt* att det inte är kontoinnehavaren själv som genomfört den aktuella transaktionen.

Att göra det antagligt är en lågt ställd bevisbörda, och det förväntas knappast att den enskilde ska lägga fram någon sorts IT-forensisk utredning som gör gällande att något tekniskt fallissemang orsakat den felaktiga underskriften. Omständigheter som istället tillmäts betydelse är bl.a. rimligheten i de belopp som överförts till och från kontoinnehavaren, hur kontoinnehavaren agerat då de obehöriga transaktionerna upptäckts, hur kontoinnehavaren förvarat och skyddat betalningsinstrumentet, et cetera. Om dessa omständigheter är sådana att de föranleder tvivel kring att det verkligen varit kontoinnehavaren som legat bakom transaktionerna undgår denne ansvaret för transaktionen.

Denna fördelning av bevisbörda är sannolikt rimlig vid den masshantering som till exempel kontokortstransaktioner utgör, men torde vara lika rimlig inom hela området för elektronisk legitimering och underskrift. Osäkerhet uppkommer dock för sådan användning av e-legitimationer där betaltjänstlagen ej är tillämplig[1]. Ett exempel på detta är när en bedragare använder en e-legitimation för att uppta lån hos en långivare, som den bedragne saknar avtalsrelation med. Då är betaltjänstlagen inte tillämplig.

Vid sådan användning saknas därmed också de ansvarsbegränsningar som framgår av 5 a kap. 2 och 3 §§ betaltjänstlagen, vilket måste anses vara en brist i skyddet av den enskilde som i praktiken inte kan styra över de tekniska säkerhetslösningar som banker och andra utfärdare tillhandahåller dem. Omvänt så gäller heller inte de aktsamhetskrav som ställs upp genom 5 kap 6 § betaltjänstlagen, som syftar till att skydda den som förlitar sig på legitimeringarna och underskrifterna.

[1] Jmf Hovrätten för Västra Sverige, dom i mål 2473-18 där rätten fann att e-legitimationen förvisso användes som ett betalningsinstrument, men där OTBIL ändå inte ansågs vara tillämplig.

Allmänna reklamationsnämnden (ARN) har under 2018, i utökad sammansättning, tagit upp fyra ärenden för vägledande beslut som samtliga rör bedrägerier med bankdosor och BankID. I samtliga av dessa fall har OTBIL varit tillämplig. I ett av fallen bedömdes innehavaren av bankdosan ha agerat särskilt klandervärt och ansetts varit likgiltig inför risken för obehöriga transaktioner, och därmed fått stå för hela det aktuella beloppet om 120 000 kr.

I de tre andra avgörandena konstaterades visserligen att bankkunden agerat grovt oaktsamt i lagens mening, men inte så klandervärt att det skulle vara stötande om banken skulle stå för en del av beloppet. ARN fann därför att ansvaret för de enskilda skulle begränsas till 12 000 kronor.

I de fall Mobilt BankID användes fann ARN att avtalsvillkoren för Mobilt BankID var strängare än de som anges i 6 § OTBIL. I villkoren angavs att innehavaren står risken om någon obehörig använt Mobilt BankID samt att innehavaren ansvarar för alla förpliktelser som uppkommer som en följd av att Mobilt BankID används. ARN konstaterade att då OTBIL är tillämplig ska dessa villkor lämnas utan avseende. Om inte OBTIL varit tillämplig är det således mer oklart vilket ansvar som skulle ålegat respektive part.

Som visat här finns ett behov av att tydligt reglera ansvar och bevisbörda för all typ av användning av e-legitimationer och elektroniska underskrifter för att skapa förutsebarhet i och tilltro till dessa viktiga funktioner.

En sådan ordning som likt betaltjänstlagen tydligt begränsar innehavarens ansvar vid särskilt riskfyllda transaktioner är också rimlig utifrån det faktum att det endast är den e-tjänst som förlitar sig på identifieringen eller underskriften som i stunden kan göra den riskbedömning som krävs för att avgöra om en transaktion ska genomföras eller ej, eller om tillkommande (möjligen manuella) kontroller måste göras. Att de aktuella betrodda tjänsterna håller en hög kvalitet fråntar inte förlitande e-tjänst ansvaret att göra ingående sådana rimlighetsbedömningar som krävs för att begränsa risken för bedrägerier och andra skador. Att med stöd av en helt nyutfärdad e-legitimation länsa sparkontot med överföringar till ett flertal nya och annars okända mottagare är helt enkelt inte ett rimligt användningsmönster. På motsvarande sätt måste myndigheter också införa rimlighetskontroller i riskfyllda verksamheter för att förhindra till exempel bolagskapningar, oriktiga utbetalningar av sociala förmåner, utbetalningar från skattekonton, med mera.

7.2 Ytterligare tänkbara förbättringsåtgärder

En sådan riskbedömning som förlitande e-tjänst enligt det föregående har att göra inför det att riskfyllda transaktioner ska utföras, kan underlättas och förfinas om vissa indikatorer kan förmedlas till e-tjänsten från den som utfärdat e-legitimationen. Sådana indikatorer kan till exempel innefatta tiden för när e-legitimationen utfärdades. Ofta, men långt ifrån alltid, nyttjas helt nyutfärdade e-legitimationer för vad som sedan visar sig vara obehöriga transaktioner. Denna information skulle kunna förmedlas på ett standardiserat sätt från utfärdaren av e-legitimationen i det identitetsintyg som ställs ut till förlitande e-tjänst. I förlängningen skulle man även kunna tänka sig en mer sofistikerad poängsättning som grundas i en sammanvägd riskbedömning att en viss e-legitimation missbrukas. Poängsättningen kan fungera på ungefär samma sätt som när försäkringsbolag som försäkrar fordon gör en bedömning baserat på fordonstyp, förarens ålder, antal skadefria år och hemvist.

Från den enskildes sida är det idag emellertid tämligen svårt att skydda sig mot olika former av sådana bedrägerier som diskuteras här. Produkter benämnda *Id-skydd* marknadsförs av flertalet aktörer som någon form av tjänst som syftar till att förhindra vad så kallade

ID-stölder. Vid en genomgång som Konsumentverket gjorde 2016 av 14 sådana tjänster fann man i flera fall stora brister, både i marknadsföringen och i de villkor bolagen tillämpade. Man fann att bolagen tenderade att överdriva de risker som konsumenten kunde förmodas löpa genom att inte köpa tjänsten. Samtidigt gjorde bolagen ofta sken av att konsumenten, med rätt skydd, inte kan drabbas av en ID-stöld. En mer rättrogen beskrivning är att såväl de bevakningstjänster som de rena försäkringsmoment bolagen erbjuder endast är reaktiva, och fordrar att den enskilde själv agerar på händelserna. I tjänsterna ingår vanligen bevakning av tagna kreditupplysningar, bevakning av adressändring, bevakning av röjda inloggningsuppgifter och ett försäkringsskydd som innefattar stöd att reda ut tillvaron vid en konstaterad ID-stöld. I förehållande till detta kan konstateras att:

- Elektroniskt förmedlade omfrågandekopior som når den omfrågande direkt erbjuds gratis av de flesta kreditupplysningsföretag.
- Likartade bevakningstjänster för röjda inloggningsuppgifter som de som erbjuds av bolagen finns att tillgå gratis på internet[2].
- Spärr mot obehörig adressändring erbjuds av Skatteverket utan kostnad.
- De försäkringsmoment som erbjuds ingår redan i de flesta hemförsäkringar.

Mot bakgrund av detta är det befogat att ifrågasätta nyttan av dessa tjänster, särskilt då produkterna är synnerligen kostsamma med avgifter kring 1000 kronor per år.

Som alternativ till dessa så kallade ID-skyddstjänster kan den enskilde alltså själv vidta vissa minst lika effektiva åtgärder som inte heller kostar något. Som redan nämnts har Skatteverket nyligen infört möjligheten att spärra obehörig adressändring. Efter att sådan spärr gjorts krävs e-legitimation för att genomföra en adressändring. Det kan också vara en god idé att se över det försäkringsskydd som erbjuds via hemförsäkringen inom detta område. Allt detta kräver dock vaksamhet och inte minst kännedom om de olika möjligheter som finns att minska risken för att falla offer för bedrägerier.

Ett generellt problem är således att dessa tjänster inte är sammanhållna på ett sätt som gör att den enskilde får en överblick. För att till exempel förhindra att kreditupplysningar tas måste varje kreditupplysningsbolag kontaktas var och en för sig. Det går inte heller att i förebyggande syfte spärra, eller att för den delen godkänna kreditupplysningsfrågor i den stund de sker. Hade sådana mekanismer funnits hade i vart fall de enklare bedrägerierna beträffande till exempel varuinköp mot faktura, mobiltelefoniabonnemang och SMS-lån blivit svårare att genomföra. De mer förslagna bedrägerierna där bedragaren i ett första steg skaffat en e-legitimation i annans namn är fortsatt betydligt svårare att skydda sig mot, då bedragaren då också har möjlighet att stänga av sådana spärrar.

En mer sammanhållen åtgärd som förvisso också fungerar reaktivt, men som på ett påtagligt sätt ändå skulle kunna bidra till att stävja bedrägerier, är om folkbokföringsregistret kunde utökas att även omfatta en frivillig uppgift om en persons mobiltelefonnummer. Användningen av denna uppgift skulle då regleras särskilt, så att den omfattas av sekretess och endast får lov att användas för syftet att skicka notiser till den enskilde om vissa händelser av särskild betydelse för att upptäcka och reagera på bedrägerier. Sådana notiser kan innefatta att en e-legitimation utfärdats, en bankrelation inletts, anmälan om adressändring mottagits eller att en kreditupplysning tagits. Förslagsvis skulle Skatteverket svara för att givet ett personnummer förmedla textmeddelandet till det aktuella mobiltelefonnumret.

[2]https://haveibeenpwned.com

Registreringen av uppgiften skulle kunna ingå som ett led i utfärdandet av e-legitimationer. Detta registreringsförfarande måste förstås utformas på så sätt att det löper en tidsfrist innan ett mobiltelefonnummer kan avregistreras, så att det inte blir möjligt för en bedragare att ändra eller ta bort uppgiften utan innehavarens vetskap.

Vidare får konstateras att det, mot bakgrund av att bedrägerierna med bankdosor och BankID kunnat förekomma under så lång tid och att problemet snarare varit tilltagande än avtagande på senare tid, kan ifrågasättas om bankerna tillräckligt tydligt och omfattande har informerat sina kunder om dessa risker. Som jämförelse kan nämnas att bankerna i Storbritannien i stor utsträckning och under lång tid köpt TV-reklam på olika klockslag över dygnet, för att nå så många målgrupper som det är praktiskt möjligt, och där informerat om riskerna och hur kunderna ska agera om de blir kontaktade av bedragare.

Avslutningsvis, så som framgått av denna utredning, saknas reglering kring ansvar och aktsamhetskrav vid sådan användning av e-legitimering där betaltjänstlagen inte är tillämplig. Därmed saknas vid all sådan användning såväl de ansvarsbegränsningar och som de aktsamhetskrav som annars ställs upp genom denna lag. En särreglering på detta område förefaller önskvärd. Detta är dock en fråga som måste utredas betydligt mer ingående än vad som varit möjligt att göra inom ramen för detta uppdrag. Då frågan i grunden berör tilliten till denna viktiga infrastruktur kan den dock antas vara av betydelse för samhällsutvecklingen på detta område.

Kungsbacka den 23 januari 2019

Fredrik Ljunggren