Remissvar en säker och tillgänglig statlig e-legitimation

Remissvar 2024-01-29

Finansdepartementet Fi2023/02704

Delbetänkande En säker och tillgänglig statlig e-legitimation (SOU 2023:61)[1]

Inledning

Föreningen mot Nätbedrägerier är en ny ideell intresseförening av och för brottsoffer som blivit utsatta för nätbedrägerier och som vill påverka banker, företag och myndigheter att ta sitt ansvar mot nätbedrägerier, för mer information se föreningens hemsida.[2]

Förening har tidigare lämnat in ett remissvar till Fi2023/01259, SOU 2023:16 Staten och betalningarna.[3] För föreningens övergripande synpunkter när det gäller dagens stora samhällsproblem med bedrägerier och om hur viktigt digital inkludering är, så hänvisar vi till den.

Därför ska detta nya remissvar ses som en komplettering till den tidigare.

Sammanfattning

Föreningen mot Nätbedrägerier stödjer förslaget om en statlig e-legitimation.

Viktigt att nämna är att e-legitimation med högsta tillitsnivå inte säkert löser dagens problem med telefonbedrägerier om man inte ser på helheten inklusive de digitala tjänster som använder e-legitimationen.

Det är inte säkerheten för själva BankID som är dagens problem, utan hur digital tjänsterna som använder BankID utformas, till exempel banktransaktioner mellan bankkonton och betalningar med Swish.

Det är därför mycket viktigt att inte bara titta på de tekniska lösningarna för e-legitimation utan också på helheten hur digitala tjänsterna som använder e-legitimation utformas.

Det saknas ett tydligt förslag på ansvarsfördelning vid till exempel bedrägerier genom social manipulation. Stor risk att det hamnar mellan stolarna om det är olika lagar och myndigheter som ansvarar för e-legitimation och digitala betrodda tjänster.

Det hjälper inte att ha en säkerhetsdörr på husets framsida om till exempel altandörren på baksidan inte går att stänga. En liknelse som BankID hade på Svenska Bankföreningens seminarium 26/1 om Samverkan för att motverka bedrägerier.[4]

[1] Remiss av SOU 2023:61 En säker och tillgänglig statlig e-legitimation - Regeringen.se
[2] Om föreningen (motnatbedragerier.org)
[3] Remiss av SOU 2023:16 Staten och betalningarna - Regeringen.se
[4] Samverkan för att motverka bedrägerier | Swedishbankers

Föreningen mot Nätbedrägerier

Detaljerande synpunkter

Sammanfattning

Problem- och behovsbild

Vi delar utredningens beskrivning men ställer oss frågande till uttrycket ”som komplement” till dagens eftersom det inte finns någon e-legitimation som uppfyller högsta tillitsnivå 4, bara nivå 3.[5]

Föreningen mot nätbedrägerier stödjer förslaget om en statlig allmänt tillgänglig e-legitimation som har högsta säkerhetsnivå enligt EU-regelverket eIDAS, vilket dagens BankID eller konkurrenten Freja e-ID inte har.

En statlig e-legitimation för så många som möjligt

Vi håller med utredningen.

En statlig e-legitimation behöver införas då legitimering inte ska ha någon som helst koppling till bankkonton, så som det är idag.

För att få stopp på nätbedrägerier genom otillåten transaktion är det mycket viktigt att man skiljer på BankID för bankkontotransaktioner och e-legitimation för identifiering av alla övriga digitala tjänster.

Delat myndighetsansvar

Vi delar utredningens uppfattning att Polismyndigheten och Skatteverket är lämpliga.

Men vi ser brister i förslaget över tillsynen av e-legitimation och tillhandahålla en kvalificerad betrodd tjänst, som idag hanteras av PTS, se punkt 6.

Utformningen av den statliga e-legitimationen

Vi har inga synpunkter på den teknisk utformning, bara man tar i beaktande det vi nämner i sammanfattningen och att det ska vara lätt för alla att använda oavsett ålder eller funktionsnedsättning.

Krav på offentlig sektor att godta vissa e-legitimationer för identifiering i digitala tjänster

Vi delar utredningens uppfattning.

För att statlig e-legitimation ska få någon effekt när det gäller inkludering är det även viktigt med en lag som gör att alla övriga digitala tjänster som kräver e-legitimation måste acceptera alla de av staten godkända e-legitimationer.

Författningsreglering

Här blir man lite fundersam när man snabbt läser igenom vad som finns. Finns det ingen lagstiftning idag? Bara Tillitsramverk och en Vägledning för utfärdare?

1 Författningsförslag

Det saknas ett tydligt förslag på ansvarsfördelning vid till exempel bedrägerier genom social manipulation, se punkt 7.

2 Utredningens uppdrag och arbete

Vi har inga synpunkter på utredningens uppdrag.

Den är omfattande och det går inte att läsa igenom allt. Men det finns mycket som är bra och välgrundat och kommer förhoppningsvis att långsiktigt leda till många förbättringar för säkrare e-legitimation och digitala tjänster.

[5] Säker och tillgänglig digital identifiering (bankid.com)

3 Definitioner av vissa centrala begrepp och termer

Inga synpunkter.

4 E-legitimationsområdet i Sverige

Förordningens tre tillitsnivåer

Det är här resonemanget brister lite och man ser inte helheten eller konsekvensen. Vi tror inte att det är äktheten i själva e-legitimationen som är problemet, till exempel med biometriska uppgifter. Utan hur detta bevis på äkthet som sedan används för samtliga övriga skyddsnivåer är kopplad till personen som använder e-legitimationen.

Vi vänder oss därför mot att både DIGG och BankID jämför dagens BankID med fysisk legitimation.[6]

”För Svensk e-legitimation på tillitsnivå 3 är avsikten att den ska ge motsvarande skyddsnivå som den traditionella fysiska legitimationshandlingen”

Till exempel som förr när man gick till sitt bankkontor, med en fysisk legitimation för att flytta eller ta ut pengar, för det finns några mycket viktiga skillnader.

1. Jag som kund vet att jag är på mitt bankkontor.
2. Personalen i kassan ser mig som håller i legitimationen i handen och att det överensstämmer.
3. Personalen i kassan ser om jag är utsatt för hot eller för social manipulation.

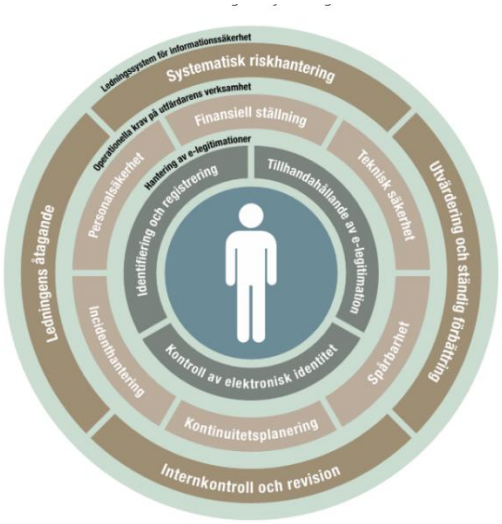

Bild från DIGG: Vägledning för utfärdare

Tillitsramverket för Svensk e-legitimation

Se punkt 7.

Här behöver man tänka till och se över helheten, som vi nämnde i vårt tidigare remissvar till Fi2023/01259 så är tillit beroende på hur e-legitimationen används av till exempel betaltjänstleverantören.

”Eftersom delegering är frivillig och inte nödvändigtvis ett tillvägagångssätt som betaltjänstleverantören prioriterar blir det i praktiken *betaltjänstleverantören som bestämmer villkor samt ansvarsfördelning* (t.ex. vem som ska ansvara för bedrägliga transaktioner). I förhållande till kortbetalningar har de internationella kortnätverken utformat särskilda bestämmelser i respektive kortregelverk (eng. Card schemes)”

[6] Vägledning för utfärdare | Digg

5. Internationell utblick

Vi håller med och tycker att det är anmärkningsvärt att Sverige ligger bland de sist i EU med att införa detta.

6 Varför behövs en statlig e-legitimation?

Vi håller med utredningen men vill särskilt peka på två viktiga områden.

Ökad tillgänglighet

Vi hänvisar till dessa punkter i vårt tidigare remissvar till Fi2023/01259.

5.4.1 Generella insatser för digital inkludering

5.5.1 Ställföreträdarutredningen

Bedrägerier och annan identitetsrelaterad brottslighet

Vi hänvisar till dessa punkter i vårt tidigare remissvar till Fi2023/01259.

5.4.1 Generella insatser för digital inkludering

7.2.3 Nya former av bedrägerier

7.3 Konsumentskyddet på den digitala betalningsmarknaden

7.3.1 Organisation av konsumentskyddsarbetet

Men vi vill även komplettera med detta.

Som vi nämnde i tidigare remissvar anser vi inte att PTS som tillsynsmyndighet uppfyller sitt uppdrag med tanke på hur utvecklingen ser ut när det gäller telefonbedrägerier där SMS och BankID har en central roll för att den organiserade brottsligheten ska komma åt pengar.[7]

Som vi tidigare nämnt så är det inte själva BankID som är problemet utan vad det kan användas till. Ett typiskt exempel på hur det kan se ut visades av SEB på Svenska Bankföreningens seminarium 26/1 Samverkan för att motverka bedrägerier. Där bedragaren via olika söktjänster och spoofing kan skicka ett SMS som man tror kommer från sin riktiga bank med uppmaning att ringa ett vanligt 08 nummer till kundtjänst om något inte stämmer.

Att PTS inte stoppar telekombolagens tjänst som möjliggör detta anser vi vara anmärkningsvärt och vi får medhåll från NOA, angående SMS, som också svarade på PTS förslag till vägledning gällande åtgärder för samtal med manipulerade telefonnummer.

Vi med flera delar därför Svenska Bankföreningens uppfattning på seminariet 26/1 över 8 åtgärder mot bedrägerier, framför allt punkt 2 att förbjuda spoofing.[8]

Föreningens remissvar till PTS går att ladda ner på hemsidan.[9]

[7] Delrapportering från arbetsgruppen om brottslighet i det finansiella systemet - Regeringen.se
[8] Spoofing: Regeringen ger Post- och telestyrelsen uppdrag (tv4.se)
[9] Ladda ner (motnatbedragerier.org)

7 Utredningens överväganden och förslag

Särskild reglering och rättspraxis i fråga om användning av e-legitimationer för betalningstransaktioner och ingående av kreditavtal

Bankerna och ARN har sedan 2018 låtit kunderna själva ta hela ansvaret för bristerna i dagens digitala tjänster med påstående som att det skulle vara lätt att undvika att bli lurad, helt utan några hänvisningar till någon forskning.

Att vem som helst kan bli lurad framgår av det forskarutlåtande från Göteborgs universitet om social manipulation och om hur hjärnan kan delas upp i två olika system och som bygger på teorier av Nobelpristagaren och psykologen Daniel Kahneman.[10]

På uppdrag av Konsumentverket har de sammanställt ”relevant psykologisk kunskap och forskning om människors beslutsfattande och vilka faktorer som kan påverka konsumenter att fatta riskfyllda och irrationella beslut i en bedrägerisituation”.[11]

Vi vill därför att man särskilt noga se över lagstiftningen så vi aldrig mer hamnar i tveksamheter om hur lagen ska tolkas så som det blev med betaltjänstlagen där personer, utan annat val när man använder digitala tjänsten, anses vara särskilt klandervärd.[12] Eller att det varit en beröring transaktion med samtycke.[13]

Ansvarsfördelningen mellan tillhandahållare[14] för en kvalificerad betrodd tjänst och den som använder den måste vara tydligt i ny lag om elektronisk identifiering och även ta i beaktande att bedrägerier genom social manipulation inte är något som man enkelt kan undvika bara genom information. Utan måste utgå ifrån forskning om hur hjärnan fungerar när man blir utsatt för stress och hot.

Mer information om detta finns att se i det Riksdagsseminarium som vi deltog i 21/11.[15]

Vi ser positivt på att BankID nu börjar inse allvaret och kommer med förbättringar. Något som vi anser skulle gjorts för länge sedan.

Särskilt intressant att notera är den skiljaktig mening av två ledamöter i ARN:s senaste vägledande beslut[16] angående hur lätt det egentligen är att se varningsmeddelandet från BankID.

8 Ikraftträdande- och övergångsbestämmelser

Vi har inga synpunkter eftersom vi tror att orsaken till att bedrägerier ökar beror på andra saker än avsaknad av en statlig e-legitimation. Till exempel telekombolagens tjänst som möjliggör manipulerade telefonnummer, se punkt 6.

Dessutom påstår SEB på seminariet 26/1 att andelen ”behöriga bedrägligs transaktioner” ökat kraftigt sedan 2019 och 2023 landar på 90%. Så då blir ju hela denna utredning ändå verkningslös när det gäller att stoppa bedrägerier, eller?

[10] Snabbt och långsamt tänkande enligt Daniel Kahneman - Utforska Sinnet
[11] Forskarutlåtande om psykologin bakom riskfyllda och irrationella ekonomiska beslut (windows.net)
[12] Konsument får ersättning av bank för obehöriga transaktioner som gjorts från konsumentens konto - Högsta domstolen
[13] ARN vägledande beslut 2022-13993
[14] Så här blir du kvalificerad tillhandahållare | PTS
[15] Riksdagsseminarium (motnatbedragerier.org)
[16] ARN:s vägledande beslut 2022-2236 och 2023-00686

9 Konsekvenser

Nollalternativet, dvs att BankID skulle få behålla sitt monopol tror vi skulle få allvarliga långsiktiga konsekvenser för Sverige och är inget alternativ.

10 Författningskommentar

Inga synpunkter.

Särskilt yttrande av Ulf Palmgren, Försäkringskassan

Vi nämnde problemet med just Försäkringskassan som exempel om en person inte har BankID i det tidigare remissvaret till Fi2023/01259.

Men vi håller absolut med om att frågan behöver utredas i ett bredare perspektiv men då inte bara mot missbruk och brott i välfärden utan även mot enskildas brottsoffer. Och gäller inte bara falska id-handlingar utan även äkta id-handlingar i fel händer som vi har beskrivit tidigare i detta remissvar.

Föreningen mot Nätbedrägerier

Mikael Förborgen

Styrelseledamot