Finansiell ID-Teknik BID AB
Kungsgatan 33
111 56 Stockholm

Datum
2021-09-14

Ärende
SOU 2021_42

Till:

Finansdepartementet
Finansmarknadsavdelningen
Bankenheten
103 33 Stockholm
fi.remissvar@regeringskansliet.se
fi.fma.b@regeringskansliet.se

Remissvar på betänkande Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42) (Regeringskansliets diarienummer Fi2021/02222)

Finansiell ID-Teknik BID AB (BID) har tagit del av betänkandet av utredningen om stärkta åtgärder mot penningtvätt och finansiering av terrorism och har förslag på vissa förändringar som vi nu lämnar i detta remissvar.

Bekämpning av penningtvätt och finansiering av terrorism är ett angeläget samhällsintresse. Det ligger även ett starkt intresse att de olika tjänster som tillhandahålls av leverantörer till verksamhetsutövarna inte missbrukas och används för penningtvätt och finansiering av terrorism. Detta kan påverka menligt på varumärket BankID, likväl på kvalitetsmärket Svensk e-legitimation samt försämra tillit och förtroende för tjänsterna och i förlängningen påverka konsumenters vilja att nyttja digitala tjänster. BID anser det därför angeläget att lagstiftaren säkerställer att samhällets alla olika aktörer som på olika sätt är involverade i den infrastruktur som ibland missbrukas för penningtvätt och finansiering av terrorism, får tillräckliga verktyg från lagstiftaren att effektivt kunna motverka, förhindra, upptäcka och anmäla misstanke om penningtvätt och finansiering av terrorism. BID ställer sig positiva till stora delar av utredningens förslag och att finansutskottet tagit initiativ till berörd utredning. Men vi befarar att betänkandets förslag i vissa delar inte riktigt kommer kunna få den effekt som eftersträvats från uppdragsgivaren. Ny lagstiftning på området bör bättre kunna hantera både ny teknik, nya tjänster och helt nya modus hur tjänster, system och infrastruktur missbrukas för penningtvätt och finansiering av terrorism. BID vill i detta remissvar framföra synpunkter och förslag på vissa förändringar. De områden vi lämnar synpunkter inom och de förslag på förändringar BID förespråkar, grundar sig i vår erfarenhet och lärdom BID har som leverantör av infrastrukturen BankID. I detta sammanhang utgör BID leverantör till de tio banker/verksamhetsutövare som deltar i BankID-samarbetet. Ett samarbete där involverade parter idag upplever juridiska begränsningar att, på ett effektivt och praktiskt sätt, kunna arbeta mot penningtvätt och finansiering av terrorism.

Nedan följer därför ett antal synpunkter och förslag på ytterligare förbättringar. En del av våra synpunkter tar utgångspunkt i att förslag på förändringar skall fungera för de specifika förutsättningar som just BankID har. Vi tror inte att utredningen varit fullt ut införstådda i alla detaljer kring BankID och hur BankID-samarbetet ser ut idag. Vi börjar därför med att lämna en kortfattad beskrivning kring några faktiska faktorer kring BankID-infrastrukturen som har påverkan i varför vi lämnar några av våra förslag på förändringar.

Kortfattad beskrivning av vissa relevanta delar i BankID-samarbetet och BankID-infrastrukturen som inte fullt ut beaktats i utredningen.

BID äger, förvaltar och utvecklar BankID och BankID-infrastrukturen. Tjänsten tillhandahålls på uppdrag av ett antal banker, som i sin tur utfärdar BankID:n och tillhandahåller BankID till de privatpersoner som nyttjar BankID för e-identifieringar och elektroniska underskrifter. Tillhandahållandet av BankID till en användare regleras i avtal mellan respektive utfärdande bank och privatperson, på villkor som den utfärdande banken ställer upp. Respektive utfärdande bank ansvarar fullt ut för sina utfärdade BankIDn och är själva personuppgiftsansvarig för alla personuppgifter kopplade till sina utfärdade BankIDn i BankID-infrastrukturen. BID är således personuppgiftsbiträde till respektive utgivande bank. BID har i egenskap av personuppgiftsbiträde fått detaljerade instruktioner från respektive bank för hur bankens personuppgifter skall hanteras och helt korrekt gäller även banksekretessen på all den datan. BID har således ingen egen data i BankID-infrastrukturen. Tekniskt sett finns det ingen kompletterande data hos BID som inte en utgivande bank (verksamhetsutövaren) redan har tillgång till och den datan använder banken redan idag vid besvarandet av olika myndighetsförfrågningar.

Problemet bankerna har idag är när sökningen på en myndighetsförfrågan rör mer än en bank. Här ställer nuvarande lagstiftning begränsning i vad som utgör tillåtet informationsutbyte mellan bankerna i kombination med reglerna hur personuppgifter skall behandlas enligt GDPR. Logiskt så kan man kan tänka att all data i BankID-infrastrukturen är uppdelad i olika silos, en silo för varje personuppgiftsansvarig bank där det finns strikta regler på hur sökningar får utföras i systemet. Ingen sökning av data, delning av information eller behandling av personuppgifter får ske utan laglig grund. Detta är en mycket viktig fråga för aktörerna inom BankID-samarbetet och det finns välutvecklade rutiner, processer och kontroller som säkerställer att all behandling sker inom ramen för gällande lagar och regler.

Sen finns det många andra finansiella aktörer som inte ingår i BankID samarbetet, men som via avtal med en säljande BankID-bank har avtal om BankID-tjänsten. Dessa andra verksamhetsutövare har inte BID som leverantör av e-legitimationstjänst, utan har faktiskt en annan BankID-bank som leverantör av e-legitimationstjänst. Det är således en annan verksamhetsutövare (en säljande BankID-bank) som tillhandahåller en e-legitimatinstjänst till en annan verksamhetsutövare utanför BankID-samarbetet. BID är bara leverantör av BankID-tjänsten till de tio banker som ingår i BankID-samarbetet, resterande och numerärt räknat en majoritet av berörda verksamhetsutövare har således en annan verksamhetsutövare som leverantör av BankID.

Det stämmer det utredningen beskriver, en bit in i kap 17.4.2, att det data som finns i BankID-infrastrukturen är på en generell teknisk nivå. Enbart information om att en identifiering eller underskrift har utförts, och mot vilken förlitandepart, sparas tillsammans med viss teknisk information. Syfte med en identifiering eller vad som undertecknades finns det ingen information om. Men det utredningen inte visste är att visst data, namnet på förlitandeparten, inte kan uteslutas utgöra känsliga personuppgifter (artikel 9, GDPR) enligt Integritetsskyddsmyndigheten (dåvarande Datainspektionen, samrådsärende DI-2018-7689). Detta faktum att det finns känsliga personuppgifter lagrade i BankID-infrastrukturen smittar av sig på all behandling av personuppgifter som utförs.

Det finns även flera andra regelverk som BankID också har att förhålla sig till. BankID uppfyller tillitsramverket Svensk e-legitimation och har dithörande kvalitetsmärke. BankID utgör även en stark kundautentisering och metod för dynamisk länkning enligt andra betaltjänstdirektivets RTS. Sen är Sverige för närvarande ett ”pre-notified country” för att anmäla eID-system enligt eIDAS-förordningen där BankID ingår. eIDAS förordningen är dessutom just nu under översyn.

Ovanstående mycket kortfattade beskrivning, som till stor del är specifika för BankID, föranleder några av de synpunkter BID framför, i syfte att säkerställa att ny reglering faktiskt fungerar på tänkt sätt rörande BankID.

Lämnade synpunkter och förlag på förändringar redovisas inte i någon prioriteringsordning, utan vi försöker följa utredningens disposition.

Utöka antalet aktörer som har en möjlighet att delta i särskilt beslutad samverkan. (kap 15.1.2)

BID är positiv till förslaget om särskild samverkan och tror att denna möjlighet kan göra stor skillnad i fråga att mer effektivt och på kortare tid vidta åtgärder mot penningtvätt och finansiering av terrorism i särskilda fall. Men BID anser att föreslagen begränsning i vilka aktörer som kan delta i samverkan i praktiken riskerar att särskild samverkan inte kommer fungera för vissa typer av modus/särskilda fall.

BID anser att gruppen aktörer som kan delta i särskild beslutad samverkan behöver utökas med de aktörer som inte är verksamhetsutövare men som enligt utredningen föreslås bli underrättelse- respektive uppgiftsskyldiga i vissa avseenden.

Om en särskild beslutad samverkan exempelvis skulle röra mer tekniska samband i ett nytt modus där e-legitimationer utgör en central komponent, så vore det från BankID-samarbetets del mer ändamålsenligt och resurseffektivt om BID i egenskap av leverantör av e-legitimeringstjänst, deltar istället för 10 st BankID-banker. BID innehar en större kompetens kring helheten och skulle ha betydligt bättre möjlighet att undersöka övergripande mönster och samband som behöver utredas i det särskilda fallet. En enskild BankID-bank som deltar i särskild samverkan skulle inte ha laglig grund att söka information om andra bankers kunders BankID-transaktioner. Om lagstiftaren önskar att brottsutredandemyndigheter vid särskild samverkan skall kunna få en samlad bild av vissa mönster bestående av personuppgifter och data under banksekretessen, så är det lämpligast att leverantören deltar i särskild samverkan och ges laglig grund för den behandlingen som behövs. Vi tror heller inte att detta förhållande är unikt för BankID utan är troligen tillämpligt även för andra leverantörer.

Utredningen gör bedömningen att det vore för långt att inkludera dessa berörda tjänsteleverantörer som deltagare i särskild beslutad samverkan då dessa tjänsteleverantörer inte har någon skyldighet att på eget initiativ vidta åtgärder mot penningtvätt eller finansiering av terrorism. BID har däremot via instruktion från respektive BankID-bank en skyldighet att vidta åtgärder mot penningtvätt och finansiering av terrorism som en del i varje banks leveranskedja. Vi tror inte heller i detta fall att detta är unikt för BankID utan är troligen tillämpligt även för andra leverantörer.

Deltagandet i särskild beslutad samverkan är dessutom frivilligt och BID skulle enbart överväga att delta i särskild beslutad samverkan där BID skulle kunna ha en roll i samverkan som de enskilda bankerna enskilt eller tillsammans inte skulle kunna motsvara.

Informationsutbyte mellan verksamhetsutövare behöver breddas (kap 16.3)

Utredningen föreslår att möjligheten att utbyta uppgifter med varandra skall begränsas till att det måste finnas ett transaktionssamband (kap 16.3.1).

BID anser att denna begränsning kommer begränsa verksamhetsutövarnas faktiska möjlighet att motverka och förhindra penningtvätt och finansiering av terrorism på ett sätt som utredningen fullt ut inte förstått konsekvenserna av. Utredningen bedömer att konsekvenser för den enskilda vid ett utökat utbyte inte är proportionerligt i förhållande till ändamålen med sådant utbyte. Vi håller med om att informationsutbytet givetvis måste begränsas, men att utredningen går för långt i begränsningen att ett informationsutbyte enbart får ske när det finns ett transaktionssamband.

Det finns annan information som behöver kunna utbytas mellan verksamhetsutövare för att exempelvis kunna förhindra pågående bedrägerier. Information rörande rent tekniska samband, som om det frivilligt utbyts mellan verksamhetsutövare, faktiskt kan förhindra ekonomisk skada för enskilda (typiskt bedrägerioffer). Utredningen har tyvärr inte beaktat brottsoffrens rättigheter i bedömningen och proportionalitetsvärderingen. Utredningen har heller inte tagit med den teknikutveckling som sker, där kravet på ett transaktionssamband (en överföring av monetära medel) blir starkt begränsande. Vid praktiskt utredningsarbete idag, så är det ofta olika tekniska samband som är avgörande för att komma fram till vad som skett eller om det verkar röra sig om missbruk och i förlängningen penningtvätt.

BID anser att undantaget från tystnadsplikten i 4 kap. 9§ penningtvättslagen ändras på så vis att uppgifter rörande samma transaktion ***eller transaktioner med ett tekniskt samband*** skall omfattas i när en verksamhetsutövare får utbyta information med varandra.

Samtliga andra aktörer som har samlad information bör ha samma rapporterings- och uppgiftsskyldighet. (kap 17.4 och 17.5)

Utredningen föreslår att reglera leverantörer av clearing- och avvecklingstjänster och leverantörer av e-legitimationstjänst och leverantör av tjänst avseende mobil överföring av pengar där överföringen sker omedelbart, på olika sätt rörande rapporterings- och uppgiftsskyldigheten.

BID anser inte att de olika aktörerna skall hanteras på olika sätt. Samtliga leverantörer som utredningen tar upp bör ha samma rapporterings- och uppgiftsskyldighet. Att inte ge leverantörer av e-legitimationstjänster eller leverantörer av tjänst avseende mobil överföring av pengar där överföringen sker omedelbart, möjligheten att rapportera misstanke om penningtvätt eller finansiering av terrorism, riskerar att information som borde komma exempelvis Polismyndigheten tillhanda, inte kommer till deras kännedom. Däremot viktigt att det enbart är en möjlighet att rapportera misstanke om penningtvätt eller finansiering av terrorism som ges berörda leverantörer och inte någon skyldighet att göra detta.

Exempel 1: Finanspolisen utnyttjar sin frågerätt mot BID och i arbetet att sammanställa svar på frågan, så upptäcker BID ett helt nytt, till synes parallellt fall, till det frågan berör. BID tolkar lagstiftningen att vi i så fall inte får lämna information om det parallella fallet till Finanspolisen utan vi besvarar strikt frågan.

Exempel 2: I annat arbete så stöter vi på ett misstänkt avvikande beteende där det finns skälig misstanke att det rör sig om ett missbruk och i förlängningen penningtvätt, men där ingen av BankID-bankerna på något sätt är del i det avvikande och misstänkta beteendet. Enbart andra förlitandeparter än BankID bankerna förekommer i det misstänkta avvikande beteendet. BID kan inte informera någon av våra BankID-banker, då ingen av dem är involverade eller den/de förlitandeparter som verkar utsatta. Resultatet blir att informationen stannar kvar hos BID utan någon vidare åtgärd, om vi inte har en laglig möjlighet att informera Polismyndigheten.

Frågerätten bör i första hand alltid ställas till verksamhetsutövaren (kap 17.5.2)

I normalfallet på en myndighetsförfrågan, så har utgivande BankID-bank (verksamhetsutövaren) tillgång till tillräcklig information för att hantera sin uppgiftsskyldighet. Våra verksamhetsutövare inom BankID-samarbetet har organisation, rutiner och processer att hantera dessa myndighetsförfrågningar och har ofta bemanning även utanför ordinarie kontorstid. BID har heller inte tillgång till någon annan data än vad verksamhetsutövarna själva har tillgång till.

Med dagens instruktioner för behandling av personuppgifter, som BID i egenskap av personuppgiftsbiträde har fått från respektive personuppgiftsansvarig bank, så är BID idag förhindrad att lämna ut bankens data till någon annan part. Dessutom gäller givetvis banksekretessen. Alla eventuella förfrågningar så hänvisar vi till banken. BID har därmed varken rutiner, processer eller personal att idag hantera och besvara myndighetsförfrågningar. Kommer vi via reglering få den skyldigheten kommer vi se till att vi kan hantera detta. Vi bedömer dock att verksamhetsutövaren även framgent kommer har bättre möjligheter att skyndsamt hantera en myndighetsförfrågan än vad BID kommer ha.

BID vill att det i kompletterande föreskrifter, eller i annan lämplig reglering eller instruktion, skall framgå att Polismyndigheten och Säkerhetspolisen i första hand skall nyttja sin frågerätt direkt mot verksamhetsutövaren och enbart nyttja frågerätten direkt mot berörda leverantörer när omständigheterna är sådana att myndigheten befarar att verksamhetsutövaren inte kan besvara förfrågan.

Behandling av känsliga personuppgifter (kap 18.5)

Utredningen tog inte specifikt upp eventuellt behov kring anpassningar i reglering för det förhållande när en berörd aktör är personuppgiftsbiträde, som det är för BID. Som redan beskrivits i inledningen så kan det inte heller uteslutas att information lagrad i BankID-infrastrukturen kan utgöra känsliga personuppgifter, och att information som överlämnas vid uppgiftsskyldighet, frågerätt eller särskilt beslutad samverkan kan utgöra känsliga personuppgifter.

Hur skall en aktör förhålla sig till föreslagen reglering om man via personuppgiftsbiträdesavtal har mot regleringen motstridig instruktion för behandling av personuppgifter från personuppgiftsansvarig? Vi hade generellt önskat att utredningen tagit upp perspektivet personuppgiftsbiträde mer i betänkandet. Speciellt när det gäller behandling av känsliga personuppgifter som ett personuppgiftsbiträde skulle behöva behandla med hänsyn till föreslagen reglering och BIDs förslag på förändringar i regleringen, så behöver de delar av regleringen som tar upp personuppgiftsbehandling ses över så att rätten att behandla känsliga personuppgifter inte enbart faller på verksamhetsutövaren.

Hur skall leverantör av e-legitimationstjänst definieras?

Vi vill väcka frågan vad som är den lämpligaste definitionen av den aktör ”som till en verksamhetsutövare tillhandahåller en e-legitimationstjänst” egentligen är. Vi vill här väcka några funderingar.

- Skulle man i regleringen istället kunna referera till betaltjänstdirektivets definition av stark kundautentisering och dynamisk länkning[1]? Teoretiskt kan det vara två olika leverantörer, en för identifiering/stark kundautentisering och en annan leverantör för dynamisk länkning/elektronisk underskrift. (Det finns inget krav att en e-legitimation även skall kunna användas för elektronisk underskrift, utan vissa tekniska lösningar av e-legitimationer kräver en central underskriftstjänst)
- Det finns också en möjlighet att i reglering referera till tillitsramverket Svensk e-legitimation[2].

[1] EU 2015/2366, delegerad förordning (EU) 2018/389 (RTS)

[2] Förvaltas av DIGG, Myndigheten för digital förvalting.

- Reboot-utredningen[3] föreslog även att i egen ny lag reglera Svensk elektronisk identitetshandling, vilket också skulle kunna vara ett alternativ.
- Vi har också betaltjänstlagen där begreppet betalningsinstrument används och där lagstiftaren betraktar att BankID utgör ett betalningsinstrument[4].
- Kommande förändringar av eIDAS-förordningen[5] kan också föranleda att man i regleringen vill referera till anmälda eID-system enligt eIDAS eller europeisk digital identitetsplånbok.

Även begreppet av den verksamhetsutövare som tillhandahåller en tjänst avseende mobil överföring av pengar där överföringen sker omedelbart kan man fundera på. Borde inte formuleringen göras mer teknikneutral och framtidssäker?

Hur förhåller sig föreslagen reglering med förslag till förändring i eIDAS-förordningen?

Ny eIDAS-förordning är ännu inte fastslagen, så vi förstår att utredningen inte har beaktat detta. Men vi vill till den fortsatta beredningen på regeringskansliet lyfta frågeställningen hur föreslagen ny reglering fungerar tillsammans med den kommande uppdateringen av eIDAS-förordningen. I nya eIDAS-förordningen så föreslås en skyldighet för vissa grupper av privata aktörer, däribland banker och finansiella aktörer, att erkänna samtliga anmälda eID-system/identitetsplånböcker i EU. Om den förändringen träder i kraft, kommer alla anmälda eID-system/identitetsplånböcker enligt eIDAS att erkännas som en e-legitimationstjänst till berörda verksamhetsutövare. Vilken aktör i egenskap av tillhandahållare av e-legitimationstjänst skall då träffas av regleringen när e-legitimationerna är anmälda eID-system/identitetsplånböcker enligt eIDAS? Blir det Myndigheten för digital förvaltning (DIGG) i egenskap av tillhandahållare av den Svenska eIDAS-noden, det medlemsland som anmält, eller den faktiska utländska aktör som utfärdat eID-metoden/identitetsplånboken som träffas av regleringen?

Föredragande i ärendet
Petter Dahl

Stockholm den 14:e september 2021

Johan Eriksson
VD Finansiell ID-Teknik BID AB

[3] SOU 2017:114

[4] Prop. 2009/10:122 s. 24

[5] COM(2021) 281 final