Bilaga 3 - Angående Polismyndighetens synpunkter på föreslagen teknisk lösning

Digg bedömer att Polismyndighetens synpunkter på föreslagen teknisk lösning rör tre områden:

1. förslaget omfattar personer med samordningsnummer
2. e-legitimationen ligger inte på det nationella id-kortet
3. lösningen innefattar inte biometriska funktioner

Digg ger i det följande sin syn på frågorna.

1. Personer med samordningsnummer omfattas

Ett samordningsnummer är en identitetsbeteckning för personer som inte är eller har varit folkbokförda i Sverige, men som ändå har behov av att ha kontakt med svenska myndigheter eller andra delar av samhället. Samordningsnummer tilldelas den som har anknytning till Sverige och har behov av ett samordningsnummer men inte uppfyller kraven för att bli folkbokförd. E-legitimationer ges idag inte ut till personer med samordningsnummer i någon relevant omfattning, till stor del på grund av att dessa personer vanligtvis saknar svensk fullgod id-handling.

Digg arbetar redan idag målinriktat med att minimera riskerna med samordningsnummer i de elektroniska miljöerna genom att separera hanteringen av samordningsnummer från personnummer, så att sammanblandning inte ska kunna ske av misstag av förlitande aktör. Samordningsnummer förmedlas endast till förlitande aktör som begär det, som oavsett har ett ansvar att göra de kontroller och utredningar som krävs i varje enskilt ärende. Det faktum att en person tilldelats en e-legitimation fråntar inte förlitande part detta ansvar.

Brister i systemet med samordningsnummer har varit kända länge och frågan har utretts i flera omgångar. Nya bestämmelser om tilldelning av samordningsnummer träder i kraft senare i år och innebär att tre nivåer inrättas beroende på vilken identitetskontroll som föregått tilldelningen. Den högsta nivån, kallad *styrkt identitet*, tilldelas den som har styrkt sin identitet vid personlig inställelse genom att lämna fram ett giltigt pass, id-kort eller motsvarande annan id-handling. Den identitetskontrollerande myndigheten ges också möjlighet att kontrollera biometriska uppgifter som finns lagrade i de id-handlingar som överlämnats vid kontrollen. Diggs förslag innebär att den statliga e-legitimationen på högsta tillitsnivå endast kan ges ut till dem som har styrkt sin identitet på detta sätt.

Det finns förväntningar att Sverige adresserar det växande digitala utanförskapet som leder till att det blir allt svårare att få tillgång till grundläggande samhällstjänster för personer som vistas i Sverige men saknar personnummer. Digg anser inte att det är rimligt att utestänga såväl andra unionsmedborgare som medborgare från tredje länder från det svenska samhället genom att förhindra dem att skaffa en e-legitimation. De begränsningar i tillvaron som avsaknad av ett personnummer innebär för dem som vistas i Sverige har också granskats av EU-kommissionen i ett antal så kallade pilotärenden.[1] Framställarna i dessa ärenden har i avsaknad av ett personnummer upplevt hinder att få tillgång till relevanta tjänster i vardagslivet. EU-kommissionen har konstaterat att problemen förblir olösta och avser att återkomma om vidare hantering av frågan.

2. E-legitimationen ligger inte på det nationella id-kortet

Lösningen som Digg föreslagit i slutrapporten utgör en instegslösning med kort införandetid och en möjliggörare för fortsatt utveckling. Diggs bedömning, med de förutsättningar som lämnats i aktuellt regeringsuppdrag, är att varken Skatteverkets id-kort eller det nationella id-kortet är gångbara alternativ som enda bärare av den statliga e-legitimationen. Det finns dock inget som hindrar att en traditionell id-handling även innehåller den av Digg föreslagna statliga e-legitimationen, bland annat då Diggs förslag bygger på öppna standarder. Digg lämnar som förslag i rapportens sista kapitel att regeringen ger Digg ett nytt uppdrag att påbörja utvecklingsarbetet. Digg anser att det i ett sådant uppdrag även bör ingå att ytterligare undersöka hur den statliga e-legitimationen kan tillhandahållas även på de nationella id-korten.

Digg har utifrån erfarenheterna på e-legitimationsområdet svårt att se att kortets prägling, om detta sker med namn och ansiktsbild eller inte, har någon relevant inverkan på säkerheten och tilliten i utgivningen eller användningen av en e-legitimation. Den föreslagna statliga e-legitimationen på ett kontaktlöst kort kan förvisso makuleras mekaniskt på samma sätt som en traditionell id-handling, men detta är inte nödvändigt. Om behov uppstår kan en e-legitimation omedelbart spärras i systemet och blir då samtidigt oanvändbar i samtliga förlitande aktörers digitala tjänster. Förfarandet ska ställas i kontrast till svagheter vid användning av traditionella id-handlingar, där de endast i undantagsfall spärrkontrolleras.

[1] Se EUP[2016]8967, EUP[2018]9384 och EUP[2019]9455.

3. Lösningen innefattar inte biometriska funktioner

Digg har i rapporten lämnat förslag till att förutsättningar för att behandla biometriska personuppgifter i samband med utfärdande av den statliga e-legitimationen behöver utredas vidare. Utöver vad som redan anförts i rapporten vill Digg lägga till några ytterligare kommentarer.

Biometriska uppgifter i form av ansiktsbild och fingeravtryck lagras sedan lång tid tillbaka i pass och nationella id-kort. Biometrijämförande kontroller sker där en person fysiskt befinner sig, till exempel vid en gränsövergång. Biometriska sensorer läser av personens fingeravtryck på plats och jämförs med de uppgifter som finns lagrade i passet eller id-kortet. Genom en sådan maskinell jämförelse stärks identitetskontrollen. Misslyckas den maskinella jämförelsen finns det manuella rutiner att tillgå på plats. Detta tillvägagångssätt fungerar inte på distans i en elektronisk miljö. När den biometriska jämförelsen på distans misslyckas, vilket under alla omständigheter kommer att ske i en inte obetydlig andel av fallen, saknas möjlighet till kompletterande handläggning. Detta medför då att e-legitimationen inte kan användas.

Det finns även tekniska hinder för biometriverifiering på distans. De biometriska sensorer som finns i dagens smarttelefoner är inte åtkomliga för tredjepartstillämpningar, det vill säga appar. Det går varken att läsa ut de biometriska uppgifterna som användaren registrerat i telefonen eller att tillföra biometriska uppgifter från annat håll. Begränsningarna finns för att skydda telefonens innehavare från integritetsintrång, men medför att telefonernas inbyggda sensorer inte kan användas för att stärka säkerheten i elektronisk identifiering på distans. Även om sensorerna, till exempel en fingeravtrycksläsare, skulle ha varit tillgängliga för tredjepartstillämpningar på det sätt som krävs, så skulle avläsning och verifiering av biometrin äga rum i en okontrollerad miljö. Det är exempelvis enkelt att skapa avgjutningar av fingeravtryck. Genom att avläsningen av de biometriska avtrycken sker oövervakat när detta görs på distans så kan inte den här typen av manipulationer upptäckas.

En annan möjlig tillämpning är att användaren får ta en bild av sig själv i samband med genomförande av vissa känsligare transaktioner, där förlitande part anser det påkallat. Bilden skulle kunna överföras till en tjänst där en ansiktsjämförelse görs mot en tidigare lagrad ansiktsbild, vilket ställer stora krav på bildens kvalitet. Detta ställer i sin tur krav, dels på telefonens kvalitet och dels på omgivningen där bilden tas, vilket i sin tur kan medföra problem med användbarheten. Därtill fordrar en sådan lösning att tillförlitliga kontroller kan göras av att bilden som överförs verkligen härrör från telefonens bildsensor och att det som avbildas är en levande människa. Utmaningen blir även i det här fallet att finna en

fungerande kompletterande handläggning. En sådan lösning skulle också spä på det digitala utanförskapet genom att ställa krav på en smarttelefon samt fler och mer avancerade moment för användaren.

Slutligen, ett påtvingat kroppsligt ingrepp i form av upptagning av biometriska uppgifter utgör ett intrång i den enskildes grundläggande fri- och rättigheter. Även den efterföljande behandlingen av de biometriska uppgifterna är av integritetskänsligt slag. Biometriska funktioner kan därför i praktiken endast komma ifråga som komplement för dem som samtyckt till att använda funktionerna och där realistiska alternativ erbjuds.

Digg kan även konstatera att det inom eIDAS-samarbetet förekommit att medlemsländer föranmält e-legitimationslösningar som innefattat biometrisk aktivering i mobila enheter (alltså som komplement till personlig kod, på samma sätt som vid upplåsning av enheten) på nivån hög, där lösningen vid sakkunniggranskningen förkastats av andra medlemsländer på grund av att man inte anser att biometrisk aktivering är tillräckligt säker för att användas på tillitsnivå hög. Detta speglar den verklighet där biometritekniken ibland tillmäts avsevärt högre tilltro än vad tekniken idag är mogen för.

Sammantaget anser Digg därför inte att tillkommande biometriska kontroller i nuläget utgör ett realistiskt alternativ för den statliga e-legitimationen.