

MUR-initiativet Stärkt grundidentitet

Försäkringskassan
Migrationsverket
Polisen
Skatteverket

Behov av en sammanhållen infrastruktur för identitet

Sammanfattning

En sammanhållen infrastruktur för identitet innebär en enhetlig hantering för kontroll och verifiering av identitet med krav på en enhetlig metod för kontroll av identitet inklusive teknik. Detta får genomslag i hela kedjan av hanteringen av identiteter från etablerandet av en identitet, utfärdande av identitetshandling till verifiering av identitet när den används och i kontrollsyfte vid missbruk. Åtgärderna syftar till en ökad tillit och trygghet i samhället för enskilda personer såväl som att motverka att identiteter kan användas som brottsverktyg i organiserad brottslighet och vid olika former av välfärdsbrottslighet. Nyckelfaktorer i åtgärderna är upptag, lagring och delning av uppgifter om och med koppling till biometriska kännetecken.

Bakgrund och beskrivning

Det finns ett starkt behov av att förstärka förutsättningarna för identitetsförvaltningen i Sverige, Identitetsförvaltningen ska bidra till såväl ökad säkerhet och informationsägarskap som förutsättningar för digital inkludering. Det krävs ett helhetsperspektiv gällande identitet för att uppnå avsedda effekter. De ska därför understrykas att det finns flera pågående initiativ som har betydelse för att en sammanhållande infrastruktur för identitet, men det finns ytterligare behov av att dessa ska kopplas ihop till en tydlig helhet. Missbruket avseende identitet sker i dess svagaste länk och de som utnyttjar identiteter anpassar sig snabbt i utvecklingen. Ett robust system med helhetssyn behöver därav utvecklas.

Skatteverket ansvarar idag för att hålla ett register som ska spegla befolkningen avseende bosättning, relationer och identitet. Det ska sedan kunna ligga till grund för beslut och åtgärder i samhället. Med det som utgångspunkt behöver hela kedjan från etablering av identitet till verifiering och användning av identitetsuppgifter oavsett om det är digitalt eller analogt hänga ihop. Vidare så ansvarar polisen för att utfärda pass och nationella ID-kort, utfärdandet av e-legitimationer sker primärt av privata aktörer under ramarna för ansvar som åligger DIGG. När det gäller identitet så saknas idag en samlad legal definition av vad en identitet är, vad en kontroll av identitet är vad förutsättningarna i form av metoder, referensdata och behandlingsregler för att genomföra detta. Det medför att det föreligger skillnader i och tillitsbrister den gemensamma hanteringen av identitetsfrågor.

Behov

Området karaktäriseras av en kraftig utvecklingsintensitet både nationellt och internationellt. Kontinuerligt ökar kunskapen och förutsättningarna för hur teknik kan användas och implementeras. Det är därav av vikt att belysa att reglering på området behöver vara hållbar över tid och ge förutsättningar att följa en hög säkerhets- och tillitsnivå i samklang med hög användarvänlighet, vilket bland annat innebär teknik- och metodneutralitet.

En infrastruktur för identitet behöver därmed bestå av en sammanhållen kedja bestående av:

- **Etablerande av identitet/användare**

Grundregistreringen av en person och dennes identitet sker normalt i samband med

födelse, flyttning till Sverige eller tilldelning av samordningsnummer. Vid svagare anknytning till Sverige kan olika former av användarregistrering även förekomma. Det förutsätter en hög grad av säkerhet, dvs. att registerhållaren av identiteten kan verifiera att personen är unik i Sverige. Det kan ske på olika sätt men ska registreringen förbli unik med "en person en identitet" krävs användande av biometri.

- **Upprättade av ID-dokument**

Upprättande, utlämnande och förvaltning av såväl fysiska som digitala identitetsdokument behöver ske på ett tillförlitligt och förutsägbart sätt. Upprättade dokument bör bestå av digital lagring av biometriska kännetecken för unikt utfärdande och verifiering. Kraven på identitetskontroll bör harmoniseras oavsett om det avser en digital eller fysisk identitetshandling.

- **Autentisering- och verifiering av identitet**

För en stark tillit till vem jag interagerar med och att en enskild person ska vara trygg med att deras uppgifter inte nyttjas av någon annan, krävs att tillförlitliga verifieringstjänster av såväl dokument som person, tillgängliggörs och nyttjas brett. Det innebär verifiering och koppling mellan den fysiska personen och identitetsdokumentet. En förutsägbart och tillgänglig modell för att verifiera en identitet för alla aktörer är viktig.

- **Förvaltning och registerhållning av identitet**

När missbruk, brott eller felaktiga uppgifter om identitet upptäcks krävs möjlighet att rätta, spärra och underrätta om missbruket på ett förenklat och tillgängligt sätt, brett i samhället. Det kräver ett utökat informationsutbyte och förutsättningar för att kunna behandla uppgifter i syfte att verifiera uppgifter, handlingar och biometriska kännetecken. Utöver det krävs tillräckligt med information för användare av identitetsuppgifterna för att bedöma behovet i den enskilda situationen. Vidare finns ett tydligt behov av att stödja brottsoffer som är drabbade av identitetsstöld eller bedrägerier med personuppgifter. Ett förbättrat stöd för en enskild som drabbas behöver det offentliga ta ett tydligare ansvar för.

De frågor som behöver behandlas är således upptagning och lagring av biometri i syfte att kontrollera och verifiera identitet både för privata och offentliga aktörer. Att utreda hur en behandling av biometriska kännetecken som en nationell resurs i syfte att stödja nationell infrastruktur för hur användande av unika identiteter, digitala som analoga, kan ske med korrekt information, ökat informationsägarskap, ökad trygghet samtidigt som det kan ske med en tydlig ansvarsfördelning mellan olika aktörer på området. I det föreligger behov av att utreda införande av en ny unik identitetskod som en nyckel i ett nationellt identitetsindex i syfte att på ett tillförlitligt sätt separera lagring, användning och förvaltning.

Målet är en mer sammanhållen hantering av identiteter som bygger på unika identiteter och säker verifiering av dessa. Effekten av det ger i sin tur trygghet för användarna att det enbart är jag själv som kan agera som mig såväl digitalt som analogt. En sådan nationell infrastruktur kräver en reglering och ansvarsfördelning avseende ett samordnat nationellt identitetsindex vilket syftar till att skapa förutsättning för tjänster som bygger på tillit, behörighet, trygghet och säkerhet.

När enskilda frågor på identitetsområdet utreds utan ett samlat grepp finns risk för suboptimerade lösningar. Identitet och identifiering bygger på spårbarhet och kontinuitet i uppgifter vid

etablering, utfärdande och verifiering. Idag bedöms risken för utnyttjade och kapade identiteter vara mer tongivande än renodlat falska uppgifter. Det medför att kopplingen mellan verifiering och etablering behöver stärkas. Ett införande av biometriska uppgifter som verifiering utan användning av referensdata riskerar att driva enkelhet framför säkerhet och trygghet.

Vilka lagstiftningsåtgärder behövs på området?

De lagstiftningsåtgärder som det finns behov av på området syftar framförallt till lagring, och delning av information. I det så ligger frågor om behandling, gallring, säkerhet och integritet i syfte att en sådan hantering blir tillförlitligt. Det innebär även att ett uppdrag kring eventuellt tillsynsansvar kring hanteringen av biometri eller motsvarande kan behöva belysas. En förtydligad ansvarsfördelning och ett statligt ansvar kring grundregistrering, identifiering och infrastruktur för identitet är viktigt.

- Lagring av uppgifter om biometriska kännetecken
I linje med utredningen Utökade befogenheter för Skatteverket inom brottsbekämpning och folkbokföring (dir 2023:134) finns behov av att lagra uppgifter avseende biometriska kännetecken. Syftet med att lagra uppgifterna är att motverka dubbla och multipla identiteter. Vidare syftar det till att skapa förutsättningar till att det enbart är jag som kan agera som mig själv (utöver formell ombudshantering). Lagring behöver även ske i syfte att kunna dela uppgifter mellan olika aktörer.
- Dela information om biometriska kännetecken
Syftet med lagring av biometriska uppgifter är att centrala aktörer såsom Polisen, Migrationsverket och Skatteverket (Folkbokföringen) ska kunna dela och editera lagrad information om biometriska uppgifter. Unika identiteter i ett enskilt register i en situation medför endast värde i den situationen. En ny underliggande identitetskod som bygger på en numerär översättning av jämförelse av biometriska kännetecken kan sedan bidra till att andra aktörer kan verifiera identiteter utan ett utbrett utbyte av faktiska biometriska uppgifter såsom ansiktsbild, fingeravtryck eller iris. Den informationen kan då ske genom en gemensam eller decentraliserad lagring av biometriska uppgifter. Regleringen bör dock vara teknikneutral. Det som lagras och används är primärt referenspunkter och en ny identitetskod. Andra myndigheter såväl som privata aktörer kan därigenom nyttja tekniken och möjligheterna med biometriska kännetecken för förstärkta digitala och analoga identitetshandlingar utan ett omfattande utbyte av känsliga uppgifter.
- Ramlagstiftning avseende identitet
En identitet kontrolleras eller verifieras idag på ett flertal olika sätt beroende på i vilken situation detta sker. Vilket innebär att kraven på och bedömningen av identiteten kan variera mellan situationerna eller när en identitet etableras, ett pass eller id-kort utfärdas, en e-legitimation utfärdas eller när en person ska visa vem man är. Missbruk går mot den svagaste punkten vilket nuläget är när man ska visa vem man är, identifiera sig vid användning. En ramlagstiftning syftar således till att reglera för kontroll av identitet. Det innebär inte alltid att kravet är detsamma vid användningen, men vad som krävs i samband med en kontroll av identitet har en gemensam utgångspunkt och användning av samma referensdata.

Sverige är en liten marknad på området för privata aktörer och varje enskild myndighet än mindre. En viktig förutsättning för gemensamt regelverk och därmed förutsättningar för

gemensamt använd teknik och lösningar ger möjlighet för ett mer enhetligt och stärkt personligt möte och identifikationslösningar på exempelvis Statens servicecenter och i andra kundmöten

- Nationell kompetens avseende identitet och biometri
Området kring identitet och biometri är specialistområde som är oerhört kompetensriktat och utvecklingsorienterat. Det är en utmaning för offentliga aktörer att kontinuerligt säkerställa kompetens på området. Det kan därav finnas skäl att se över den nationella kompetensen på området. Såväl Norge som Danmark har varianter av nationella ID-center med uppdrag att stödja offentliga aktörer och driva frågor på området. Behov av reglering kan bestå i förutsättningar att arbeta för att nyttja gemensam kompetens, fördjupade granskningar, kravställningar och omvärldsbevakning som medför att Sverige och dess myndigheter kan ligga långt fram i såväl utveckling som bedömning av uppgifter/handlingar som att förstå modus och företeelser i samhället. Det kan ske genom ett riktat uppdrag till en enskild aktör/myndighet eller att tillsätta en ny funktion, men med förutsättningarna att vara en nationell resurs för att säkerställa kompetens och tillämpning hos samtliga myndigheter.

Övergripande beskrivning av lösningshypotesen

Lösningen är en förutsättningsskapande åtgärd för att alla aktörer ska kunna känna tillit till vem man interagerar med, det inbegriper både offentliga och privata aktörer. Lösningen bygger på en tydliggjord ansvarsfördelning där förslaget är att Skatteverket, Polisen och Migrationsverket får förutsättningar att ta upp, lagra och editera uppgifter om biometriska kännetecken. Det innebär att myndigheterna gemensamt hanterar uppgifter om biometriska kännetecken som sedan kopplas till en ny underliggande persistent identitetskod genom en numerär översättning av de referenspunkter som utläses från en fysisk person. Den numerära översättningen och identitetskoden kan sedan användas som referensdata utåtriktat i syfte att stärka kontroll, verifiering och autentisering av identiteter i olika situationer med hög tillitsgrad.



Tillit

Vi vill bygga en lösning för unika identiteter som stärker tilliten, genom transparens och personligt ägandeskap.



Koppling

Vi gör det genom att skapa en brygga mellan en fysisk person och identiteten som finns i register.



Gemensamt index

För att få till det behöver vi skapa ett index som håller ihop registrerade identiteter i Sverige, så att vi kan säkerställa unika identiteter och att 'det är bara jag som kan agera som mig'.

Alla identiteter lagras i identitetsindexet

- Varje identitet får en ny unik underliggande identitetsnyckel/-beteckning
- Varje nyckel kopplas till personers unika biometriska kännetecken (samt identitetshandlingar - digitala/analog)
- Identitetsnyckeln kan kopplas till samordningsnummer, personnummer, beslut, inloggnings mm. utanför det lagrade indexet.



Lösningshypotesen bygger således på att vara ett en mer central punkt som säkerställer unika identiteter, en hög tillitsgrad vid användandet av identiteter såväl digitalt som analogt och med det som utgångspunkt en ökad tillit i samhället och ett starkt informationsägarskap som innebär att det är bara jag själv som kan agera som mig.

Behandlingen av relevant information i lösningshypotesen föranleder ett flertal frågor kopplat till integritet, säkerhet, robusthet som medför ett behov av tydlig ansvarsfördelning, tillsyn och reglering att skydda en central infrastruktur och trygghet där det offentliga bör vara en viktig aktiv aktör.

Överblick av lösningshypotesen

