Remissyttrande
2018-04-19 Dnr: Fi2018/00106/DF

Finansdepartementet
Jakobsgatan 24
103 33 STOCKHOLM

Remissyttrande över betänkandet SOU 2017:114 – Reboot – omstart för den digitala förvaltningen

Sammanfattning
Verisec AB har sedan 2002 varit verksamt inom området digitala identiteter. Bolaget lanserade 2017 e-legitimationen Freja eID+ som i januari 2018 som första mobila e-legitimation i Sverige fick E-legitimationsnämndens godkännande för kvalitetsmärket Svensk e-legitimation. I vårt yttrande kommer vi fokusera på de delar som handlar om identifiering och e-legitimering.

Vår uppfattning är att betänkandet lyfter frågor som är helt avgörande för Sveriges framtida utveckling och att utredaren i huvudsak landar i slutsatser vi delar och lösningar vi kan ställa oss bakom. Dock finns några viktiga punkter där vi tror det är viktigt att lagstiftaren gör vissa justeringar för att vi skall landa i ett regelverk som bidrar till att göra Sveriges till en ledande IT-nation. Utredningens titel berättar ju om att huvudsyftet är att göra en omstart för den digitala förvaltningen. Men stora delar i utredningen, framförallt de som handlar om e-legitimering, eller elektronisk identifiering som utredaren kallar det, är avgörande inte bara för det offentliga Sveriges framgångsrika digitalisering. Elektroniska identiteter och e-legitimation är nyckeln till en framgångsrik digitalisering för alla delar av samhället. Om vi kan skapa ett världsledande system, för såväl myndigheter som företag och andra organisationer, kring elektronisk identifiering är det vår mening att Sverige kommer att ta täten i den digitala utvecklingen.

Allmänt om vår begreppsanvändning och utredningens förslag till nya begrepp
Inledningsvis vill vi hänvisa till de avsnitt som handlar om definitioner, för att klargöra hur vi använder begreppen i vårt remissvar och vår syn på utredarens förslag till förändringar.

Utredningen menar i punkt 10.2 att ”e-legitimation” är ett missvisande begrepp då det enligt Svenska akademiens ordlista och ett språkfilosofiskt resonemang från utredarens sida innehåller en underliggande betydelse av *”behörighetsstrukturer”*. Vår mening är att det är ytterst osannolikt att detta är en vida spridd uppfattning bland allmänheten. ”Legitimation” och ”Identitetshandling” är för de allra flesta svenskar synonyma begrepp och används i dagligt språkbruk helt utan risk för vare sig förvirring eller tolkningsdiskussioner.

Under de senaste åren har användandet av e-legitimation i Sverige genomgått en explosiv utveckling och de allra flesta svenskar är numera bekanta med begreppet och vad det innebär. Att därför med hjälp av lagstiftning ändra ett så nyligen etablerat begrepp till ”elektronisk identitetshandling” vore mycket olyckligt och kontraproduktivt.

Under de senaste åren har E-legitimationsnämnden arbetat framgångsrikt med att etablera begreppet Svensk e-legitimation hos myndigheter och företag. I och med att nästan åtta miljoner medborgare idag har en e-legitimation med regelbunden användning torde begreppet ”e-legitimation” kunna anses som etablerad. I tillägg till detta har E-legitimationsnämnden under våren 2018 fått ett regeringsuppdrag just för att ytterligare sprida medvetande om ”e-legitimation” till

allmänheten. Även utfärdare av e-legitimationer, som Verisec, lägger mycket stora resurser på att marknadsföra sina tjänster under begreppet ”e-legitimation”.

Mot bakgrund av ovanstående förordar vi med emfas att lagstiftaren bortser från förslaget att ersätta begreppet ”e-legitimation” med ”elektronisk identitetshandling” och att inte heller ersätta det inarbetade begreppet ”Svensk e-legitimation” med det betydligt krångligare ”Svensk elektronisk identitetshandling”.

Utredningen diskuterar också möjligheten i avsnitt 12.2 att förbehålla rätten till begreppet ”elektronisk identitetshandling” (eller e-legitimation om befintligt begrepp behålls) för elektroniska identiteter utfärdade på tillitsnivå tre och fyra. Vi menar att detta, mot samma bakgrund som beskrivs ovan, riskerar i att resultera i en begreppsförvirring hos allmänheten. Ett bättre alternativ är att vara tydlig med hur de olika tillitsnivåerna får användas i relation till olika tjänster.

Vi delar däremot utredarens syn på att definitioner och tydlighet behövs, men det kan göras utan att byta etablerade namn och förbehålla vissa tillitsnivåer rätten till namn. Ett exempel på en annan del av lagstiftningsprocessen där bristen på tydlighet skapar problem är den spellicensutredning som presenterades 2017. Där föreslår utredaren att alla spelare skall registreras med e-legitimation för att en spellicens skal erhållas. Men man gör ingen vidare definition av begreppet vilket riskerar att göra denna del av lagen uddlös, vilket vi påpekade i vårt remissvar. Här borde lagstiftaren vara tydlig med att vad som krävs är dels en e-legitimation godkänd för kvalitetsmärket Svensk e-legitimation samt på vilket tillitsnivån e-legitimationen skall vara utfärdad på. Svårare än så behöver det inte vara.

Det finns dock två områden där ändring av begrepp borde övervägas. Det ena är att vi harmonierar våra svenska definitioner kring tillitsnivå 2, 3 och 4 med EU:s definitioner låg, väsentlig och hög. Vi utvecklar detta senare i remissvaret.

Det andra begreppet som bör ändras är ”kvalitetsmärke”. Utredningen föreslår att lagstiftningen skall använda begreppet ”kvalitetsmärke” för att beskriva den officiellt prövade och godkända märkningen ”Svensk e-legitimation”. Vi menar att ”kvalitetsmärke” är ett vagt begrepp utan stöd i allmänt språkbruk. Vi menar att det vore tydligare för alla parter vad som avses att använda ett begrepp som ”Certifiering” eller ”Godkänd”. Ett kvalitetsmärke menar vi är något som är öppet för tolkningar enligt en skala medan en certifiering eller ett godkännande har en absolut innebörd.

I vårt remissvar använder vi begreppen e-legitimation och elektronisk identitetshandling växelvis och med samma innebörd.

Avsnitt 1.1 Förslag till lag om statlig elektronisk identitetshandling

<u>Klargör att utfärdande av elektroniska identitetshandlingar inte är ett statligt monopol.</u>
Att staten utfärdar en elektronisk identitetshandling som kan ”växlas över” till olika e-legitimationer, i drift av offentliga och privata aktörer, är i grunden en god tanke. Det måste dock i lagstiftningen tydligt klargöras att detta kompletterar utfärdande av e-legitimationer av andra aktörer som är godkända för kvalitetsmärket Svensk e-legitimation. I dagsläget har redan nära 100% av alla medborgare en e-legitimation utfärdade av BankID, AB Svenska Pass, Telia e-legitimation, Huddinge Kommun och Freja eID. Förutsatt att dessa e-legitimationer – och även tillkommande privata och offentliga initiativ – har kvalitetsmärket Svensk e-legitimation måste de utgivningsprocesser som ligger till grund för kvalitetsmärkningen enligt tillitsramverket även efter 2020 få leva kvar parallellt med utgivningen av en statlig elektronisk identitetshandling. Staten skall garantera att en

medborgare kan få en e-legitimation utfärdad men skall inte stänga möjligheten för andra utfärdare så länge deras utgivningsprocess är godkänd enligt tillitsramverket och uppfyller kraven för Svensk e-legitimation.

Staten har under nästan 20 år genom olika initiativ försökt identifiera en lämplig infrastruktur för att utfärda e-legitimationer. Förslag har inkluderat bibliotek, apotek, polisstationer och skattekontor. Det initiativ som har kommit närmast är den nu kvalitetsmärkta e-legitimationen från AB Svenska Pass som ges ut via 28 skattekontor. Om staten inte under de drygt 20 månader som återstår till 1 januari 2020 lanserar en infrastruktur som kan svara upp mot utfärdandet av e-legitimationer till miljoner medborgare måste de existerande alternativen finnas kvar. Som en jämförelse till de 28 utlämningsställen för en e-legitimation som Skatteverket har i dagsläget erbjuder BankID, via bankkontor cirka 1500 utlämningsställen och Freja eID, via förbutiker i detaljhandeln och fristående ombud drygt 2000 utlämningsställen. Att eliminera denna värdefulla infrastruktur – som ligger till grund för de miljoner e-legitimationer som gör att det digitala Sverige överhuvudtaget fungerar idag, skulle få mycket negativa konsekvenser.

Vi tolkar egentligen inte utredarens förslag så som att man vill ge staten monopol på att utfärda e-legitimationer. Dock är formuleringarna i lagtexten öppna för en sådan tolkning och att det därmed måste klargöras att ett monopol inte är lagstiftarens avsikt.

Vi delar däremot fullt ut utredningens syn att staten skall ha ensamrätt på att grundidentifiera individer för utfärdande av fysiska identitetshandlingar. Den breda flora av ID-handlingar som idag finns är en starkt bidragande orsak till de cirka 200 000 ID-stölder och bedrägerier som sker varje år.

<u>Klargör hur den statliga elektroniska identiteten rent praktiskt skall kunna växlas in</u>
Utfärdaren diskuterar hur den statliga e-legitimationen skall tillhandahållas medborgaren och landar i slutsatsen att den skall läggas på en fysisk ID-handlingen. För det fall att så sker och att den elektroniska identiteten ligger lagrad på ett chip måste lagstiftaren också ta hänsyn till frågan om hur man möjliggör för medborgaren att växla över denna elektroniska identitet till en användbar e-legitimation utfärdad av någon av de existerande aktörerna. Den enda möjligheten är via en kortläsare eller NFC-läsare (Near Field Communication) och för det fall att staten skall ansvara för att medborgarna har tillgång till en sådan teknisk utrustning måste staten budgetera med en kostnad på flera miljarder kronor, baserat på vad sådan utrustning, hantering och distribution kostar i dagsläget. Om ansvaret skall ligga på medborgaren kan noteras – ifall en lösning med NFC genomförs – att de som har en Android-mobil i många fall har en NFC-läsare i mobil. iPhone har för vissa modeller också en NFC-läsare men Apple tillåter i dagsläget inte NFC-funktionen för den här typen av användning. iPhone och Android har i dagsläget, grovt uppskattat, hälften var av den svenska marknaden. Det är dock inte osannolik att Apple framöver kan tänkas ändra dessa regler.

<u>Inkludera pass som underlag för statligt utfärdad elektronisk identitet på tillitsnivå 3</u>
En möjlighet som utredaren förbiser och som faktiskt innebär att staten redan idag – delvis i alla fall - har löst problemet är att använda passet för utfärdande av en e-legitimation, åtminstone på tillitsnivå 3. På passet finns ett NFC-chip med en krypteringsnyckel samt ett högupplöst fotografi av användaren. Genom att läsa av informationen med en NFC-läsare, exempelvis via en smartphone och i kombination med detta låta användaren göra en biometrisk registrering av ansiktet kan – med hjälp av befintlig teknik för ansiktsigenkänning – en säker växling av identiteten från passet till den elektroniska identiteten genomföras. Tekniken är väl etablerad och används bland annat i Norge för utfärdande av elektroniska identiteter på hög tillitsnivå motsvarande nivå 3. Enligt de indikationer vi har fått fyller en sådan process de kriterier som i dagsläget finns i tillitsramverket för nivå 3. Om denna metod stadfästs i lagstiftning för utfärdande av e-legitimationer på nivå 3 har staten därmed

en befintlig lösning på det problem som utredningen har identifierat – i vart fall för Android-användare - och att den statligt utfärdade e-legitimationen på nivå 4 kan därmed bli ett komplement och en backup till övriga lösningar, i linje med utredarens förslag.

Utöka informationsplikten kring spärr av elektroniska identiteter

I paragraf 17 bör det förtydligas att de utfärdare som skapat en e-legitimation baserat på den statliga har skyldighet att informera den utfärdande myndigheten. Som texten nu är formulerad är det först när identiteten spärras hos myndigheten som övriga utfärdare blir informerade om det. En utfärdare kan ju identifiera misstänka bedrägerier med en e-legitimation och spärra denna ”lokalt” i sitt system. Det bör lagstiftas om att en sådan lokal spärr måste meddelas till utfärdande myndighet så att denne kan vidta lämpliga åtgärder i form av utredning eller en central spärr.

Medge automatiserad kontroll av ID-handlingar

I lagstiftningen bör också regleras att e-legitimationsutfärdare kan göra automatiserade slagningar mot det centrala spärr-registret vid ID-växling från den statligt utfärdade e-legitimationen då en e-legitimation skall utfärdas av någon av de övriga aktörerna. Det kan låta självklart men i dagsläget finns exempelvis ingen möjlighet för e-legitimationsutfärdare att göra automatiserade slagningar vid utfärdande av e-legitimationer ifall användaren använder körkort, vilket är den ID-handling som används i cirka 85% av fallen. Transportstyrelsen tillåter endast biluthyrningsfirmor och andra fordonsrelaterade verksamheter göra automatiserade slagningar. Andra aktörer som vill kontrollera giltigheten av ett körkort måste göra en manuell kontroll genom att ringa Transportstyrelsen. Vi föreslår därför också att det lagstiftas att det för alla godkända e-legitimationsutfärdare ges möjlighet att göra automatiserade slagningar mot alla de utgivare av ID-handlingar som är godkända för att ligga till grund för utfärdandet av en e-legitimation. Vi har även gjort en hemställan till regeringen i denna fråga.

Avsnitt 1.2 Förslag till lag om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk e-Identitet

Utredningen föreslår att för att få ett kvalitetsmärke skall e-legitimationen prövas mot både ett tillitsramverk och en teknisk specifikation. I dagsläget sker prövningen endast mot ett tillitsramverk. Vi anser det är rimligt att lägga till en prövning mot en teknisk specifikation men att det tydliggörs att det för aktörer har det befintliga kvalitetsmärket utfärdat får en övergångsperiod för att hinna med att anpassa sig till de tekniska specifikationerna.

Vad gäller utformningen av de tekniska specifikationerna instämmer vi i utredarens slutsats att dessa inte skall definieras av lagstiftningen. Att en myndighet gör dessa specifikationer är rimligt men vi föreslår att det i lagstiftningen förtydligas att de tekniska specifikationerna tas fram i samråd med etablerade aktörer inom e-legitimering och med etablerade teknikleverantörer.

Avsnitt 11.2 Grundidentifiering – ett statligt ansvar

I avsnitt 11.1 vill utredaren klargöra vad begreppet ”Grundidentifiering” innebär. Dessvärre kvarstår en stor otydlighet vilket vi föreslår undanröjs genom att använda begreppen ”Fysisk grundidentifiering” och ”Elektronisk grundidentifiering”. Mellan raderna utläser vi att detta också är utredarens mening, men det finns utrymme för tolkning, vilket i sig går emot utredarens syfte i avsnittet.

Det som i avsnitt 11.1 och 11.2 definieras som grundidentifiering menar vi skall klargöras som fysisk grundidentifiering där användaren får en fysisk identitetshandling. Denna fysiska identitetshandling kan därefter användas vid en elektronisk grundidentifiering av en utfärdare av e-legitimationer.

Förslaget om en statlig e-legitimation som läggs på en fysisk id-handling skulle därmed motsvara att *både* en fysisk och en elektronisk grundidentifiering görs vid samma tillfälle.

Ett exempel för att klargöra skillnaden. En person som i dagsläget saknar en e-legitimation kan vända sig till exempelvis sin bank för att få BankID eller till Verisec för att få Freja eID. Personen uppvisar då, bland annat, en ID-handling som någon annan har utfärdat genom en *fysisk* grundidentifiering. När BankID eller Freja eID med denna ID-handling som grund utfärdar en e-legitimation görs en *elektronisk* grundidentifiering.

Vi delar utredningens syn att det skall vara statens ansvar att genomföra grundidentifiering så länge det avser den fysiska grundidentifieringen, enligt definitionen ovan. Staten skall ansvara för att det också finns en elektronisk grundidentifiering – som föreslagits på tillitsnivå 4 - men andra aktörer, godkända enligt tillitsramverket, bör även fortsättningsvis få göra detta på den tillitsnivå de är godkända för.

Avsnitt 12.5 Utformning av elektroniska identitetshandlingar på olika tillitsnivåer

Systemet med tillitsnivåer är enligt vår mening en nödvändigt men det har från tid till annan funnits osäkerhet om vad som krävs för att uppnå de olika nivåerna. Ett exempel varit har osäkerheten huruvida nivå två kräver tvåfaktorsautentisering eller inte, något som nu verkar förtydligas i och med det uppdaterade tillitsramverk som gäller från augusti i år. Ett annat problem har varit att EU har ett annat system för att kategorisera tillitsnivåer ”Låg”, ”Väsentlig” och ”Hög”. Vår mening är att man borde harmoniera nivåerna och även överge idén på att ha olika namn för de Svenska tillitsnivåerna och de i EU.

I Sverige har vi fyra tillitsnivåer men nivå ett är inte reglerad och ingår inte i tillitsramverket vilket enligt vår mening gör att den inte bör ingå i de offentliga standarderna. Således har vi i Sverige tre tillitsnivåer och EU har tre tillitsnivåer. Enligt E-legitimationsnämnden harmonierar de fullt ut, förutom kravet på fysisk närvaro vid nivå ”hög”, vilket krävs för nivå 4. Vi menar att det kommer försvåra integrationen med eIDAS om inte standarderna harmonierar. Att ha olika begrepp för vad som i grunden är samma sak är också en källa till förvirring. Om nivåerna inte harmonierar vid något tillfälle i framtiden kommer detta också skapa störningar i eIDAS-samarbetet. Ifall länder som kräver, exempelvis ”Väsentlig” plötsligt stoppar en e-legitimation från Sverige för att vi justerat vår Nivå 3 i enlighet med nya rekommendationer från NIST kan det få allvarliga konsekvenser. Det skall tilläggas att det exempelvis i Norge om att införa ytterligare en tillitsnivå, nivå 5, vilket ytterligare skulle späda på förvirringen för begreppet ”tillitsnivå”. Denna vida flora av begrepp kommer med största sannolikhet skapa stora bekymmer för såväl utfärdare, förlitande parter och användare. Sverige kan bidra till att minska begreppsförvirringen genom att anta EU:s standard för definitioner.

Vi menar att den myndighet som utses att hantera frågan om tillitsnivåer, Digitaliseringsmyndigheten, bör utreda möjligheten att helt harmoniera nivåerna och dessutom överge de befintliga definitionerna Nivå 1, 2, 3 och 4 till förmån för EU:s definitioner. Problemet är naturligtvis nivå 4 eftersom den inte helt harmonierar med Hög. Men då får man lyfta ut Nivå 4 ur eIDAS-samarbetet och ha en egen kategori för den som bara gäller i Sverige, precis som Norge som

eventuellt kommer ha en Nivå 5 som bara gäller där. En användare med nivå Hög från ett annat EU-land bör ju ändå inte kunna nå en svensk tjänst med krav på nivå 4.

Avsnitt 12. 7 En statlig elektronisk identitetshandling

Vi instämmer i utredarens förslag att en statlig e-legitimation skall finnas, som ett komplement till befintliga e-legitimationer och som en möjlighet för andra e-legitimationer att identitetsväxla från, så länge detta inte påverkar godkända utfärdares möjlighet att utfärda e-legitimationer enligt tillitsramverket oberoende av den statliga e-legitimationen.

Utredaren bygger många av sina slutsatser i detta avsnitt mot bakgrund av att BankID är en dominerade aktör och att detta har skapat behov av ett statligt alternativ. Vår uppfattning är att medborgares, myndigheters och företags efterfrågan på alternativ kommer att driva fram fler aktörer i takt med att digitaliseringen fortskrider och att det över tid kommer att skapas en välfungerande marknad för e-legitimationer. Statens roll bör vara att tillse att mekanismer för en välfungerande marknad finns på plats. Utredaren menar vidare att en statlig e-legitimation skall vara en garant för att Sverige kan anmäla en e-legitimation till eIDAS – ett problem som var uppenbart vid tidpunkten då utredningen skrevs. Sedan dess har den e-legitimation vi representerar fått godkännande för kvalitetsmärket Svensk e-legitimation och vi har också hemställt till regeringen att vi önskar att denna e-legitimation anmäls till eIDAS.

<u>Angående Krav på den statliga elektroniska identitetshandlingen</u>

Läser man kraven framstår det som att en individ inte behöver något annat än den statliga e-legitimationen för att kunna identifiera sig elektroniskt. För de som skall stifta lagen låter detta självklart välkommet då det framstår som att staten nu kan vara oberoende i förhållande till andra aktörer. Detta är dock missvisande och i de krav som radas upp finns en inbyggd motsättning. Å ena sidan säger man att den statliga e-legitimationen inte skall kräva att användaren har vare sig mobil, dator eller kortläsare. Å andra sidan säger man att den skall vara utfärdad på en fysisk bärare. Om man med fysisk bärare menar ID-kort med chip – vilket är det mest sannolika – är denna e-legitimation värdelös utan kortläsare eller NFC-läsare. På sidan 203 motsäger utredningen sig själv genom att hävda:

”Det innebär att individer som vill använda sin statliga elektroniska identitetshandling måste ha en kortläsare eller liknande för att kunna använda den”

Den enda rimliga lösningen för att få ihop resonemanget är att staten erbjuder en omfattande infrastruktur av uppkopplade datorer med kortläsare på offentliga platser dit medborgare kan komma med sitt kort för att göra sina elektroniska ärenden. Det är i sig en bra lösning för de individer som befinner sig i ett digitalt utanförskap, men lagstiftaren kan i så fall inte bortse från att tilldela de resurser som krävs för att erbjuda en sådan infrastruktur.

Avsnitt 15.8 Skilj på tjänsteutövning och privata ärenden

Vi delar utredningens syn på att det finns anledning att i vissa sammanhang hålla isär tjänsteutövning och privata ärenden. Dock är det fel väg att gå att i lagstiftningen säga att en person inte ska använda sin privata e-legitimation i tjänsten. Bakgrunden tror vi är att man inte vill tvinga användarna att i tjänstesammanhang använda sitt personnummer vid identifieringen, något som har varit en de-facto standard tills nu. Dock finns nu en lösning som adresserar detta problem. Freja eID möjliggör för en anställd, exempelvis i en kommun, att identifiera sig med sitt anställningsnummer. I bakgrunden görs

en matchning av att det är rätt person, men individen behöver inte skylta med sitt personnummer – något som av många upplevs som integritetskränkande.

Utöver det faktum att det alltså redan finns en lösning på det problem som utredningen pekar på finns ett logiskt felslut i diskussionen kring tjänstelegitimation och privata legitimationer. En tjänstelegitimation identifierar privatpersonen och gör den inte det saknar tjänstelegitimationen helt värde. Så att förbjuda användning av privata legitimationer i tjänstesammanhang löser egentligen inte den grundläggande frågan som snarare handlar om vilken information man som tjänsteutövare vill släppa ifrån sig då man identifierar sig med sin tjänstelegitimation. Så länge det bara fanns e-legitimationer som fungerade med personnummer var detta ett problem. Med e-legitimationer som tillåter och hanterar fler attribut är problemet alltså redan löst.

Avsnitt 15.8.1 Den statliga elektroniska identitetshandlingen är bara för privat bruk

Utredningen landar i en slutsats kring att fysiska kort är framtiden för identifiering i tjänstesammanhang. Som leverantör med kontakt med många myndigheter, kommuner, företag och andra som behöver elektronisk identifiering av sina anställda är vår bild den motsatta. Allt fler vill komma ifrån beroendet av olika fysiska enheter och drivkraften är stark att använda mobilen som plattform, inte bara för e-legitimering utan för en lång rad andra verktyg anställda behöver i tjänsten. Det skulle rimma illa med regeringens mål ”Digitalt först” att i ett lagförslag som syftar till att öka digitaliseringstakten lägga förslag som går i motsatt riktning. Den utveckling som mobilen har haft de senaste åren har gjort att de flesta individer är vana att hantera såväl privata ärenden som tjänsteärenden på samma mobil. Det vore därför orimligt att det i lagstiftningen reglerades vad en individs mobiltelefon får och inte får användas till.

Avsnitt 15.9 Organisering och ansvarsfördelning

För det fall att det är utredningens mening att det på sikt skall finnas en gemensam lösning kring e-legitimation för hela den offentliga förvaltningen bör en sådan utredning inte bara baseras på en enskild aktör, EFOS. Vi delar inte uppfattningen att det är en god idé att ha en gemensam lösning för alla inom den offentliga förvaltningen. Behoven skiljer sig enormt mellan olika myndigheter, kommuner och landsting. Vissa föredrar mobila lösningar medan andra fortfarande tycker kortbaserade lösningar är bättre. Vissa har stora resurser att lägga på ID-lösningar medan andra har tuffa budgetkrav att ta hänsyn till. Utredningen handlar ju till stor del om värdet och nyttan att skapa valfrihet gentemot medborgarna – och för den offentliga förvaltningen vad gäller ID-lösningar för medborgarna. Att man i detta avsnitt öppnar för att utreda en lösning som pekar på mindre valfrihet är därför förvånande.

Valfrihet är nyckeln till digitaliseringen. Den tekniska utvecklingen går så fort att det vore orimligt att tänka sig att den bästa tekniska lösningen för e-legitimering av offentliganställda skulle tas fram av en enskild aktör – offentlig eller privat - för att täcka alla behov från hundratals olika offentliga förvaltningar. För det fall att det är lagstiftarens mening att införa en förvaltningsgemensam lösning bör i vart fall en sådan process föregås av en offentlig upphandling.

Det största problemet med förslaget i 15.9 är dock något annat än ovanstående. Det är att en sådan indikation från regeringens sida kommer få många myndigheter, kommuner och landsting att tveka att idag införa nödvändiga ID-lösningar i väntan på ett framtida direktiv. Vi är överens med utredningen om att elektronisk identifiering är en av de viktigaste nycklarna för vår fortsatta digitalisering. Vill man sätta paus för digitaliseringen av det offentliga Sverige gör man det genom den här typen av utredningsförslag som bara kommer spä på osäkerheten och göra att många tar det

säkra före det osäkra – vilket i det här fallet är att vänta. Och redan nu har väntetiden faktiskt förlängts. EFOS skulle lanseras den 3 april men lanseringen har nu skjutits upp på obestämd framtid. När det finns färdiga lösningar som ett stort antal offentliga förvaltningar redan idag vill skaffa – och några faktiskt redan har skaffat – vore det ödesdigert att sätta en hämsko på utvecklingen genom att från högsta ort ge signaler som skapar osäkerhet.

Avsnitt 18.2 och 18.3 Sverige skall anmäla elektroniska identitetshandlingar

eIDAS träder i kraft den 29 september 2018. Ett flertal länder har redan anmält e-legitimationer till eIDAS och fler är sannolikt att vänta före september. När utredningen skrevs fanns ingen Svensk e-legitimation som fyllde kraven för att anmälas till eIDAS men idag finns det en sådan och vi menar därför att Sverige utan dröjsmål bör anmäla denna till eIDAS.

Freja eID+ godkändes för kvalitetsmärket Svensk e-legitimation den 17 januari och är etablerad på den svenska marknaden med såväl användare som förlitande parter. Freja eID+ är redo för de tekniska specifikationer som krävs för anslutning till eIDAS och Verisec har också i en hemställan till regeringen uttryckt en vilja om att e-legitimationen blir ansluten.

Utredningen landar i slutsatsen att även privata aktörer skall kunna ingå i Sveriges eIDAS åtagande. Dessutom finns det en välfungerande och kompetent myndighet i E-legitimationsnämnden som i dagsläget kan ansvara för uppgiften att anmäla en e-legitimation till eIDAS. Återstående frågor kring tex. ansvar, försäkringar, ersättningar och liknande finns tid att reglera innan den 29 september. Därmed finns inga skäl att vänta och låta Sverige hamna långt bak i kön över EU-länder som ansluter sig till eIDAS. Sverige är världsledande inom digitalisering på många områden och vi menar att vårt rykte som ledande IT-nation riskerar att skadas för det fall att vi inte är i framkant när det gäller eIDAS.

Utredningen föreslår att Digitaliseringsmyndigheten skall stå för anmälan till eIDAS. Vi delar denna åsikt, men eftersom myndigheten inte börjar sitt arbete förrän 1 september är det vår mening att E-Legitimationsnämnden får denna uppgift till dess att den nya myndigheten är igång.

För Verisec AB,

Johan Henrikson, VD
Mobil: +46 733 45 89 02
Epost: johan.henrikson@verisec.com