



Malmö stad

**Datum**

2026-09-09

**Adress**

205 80 Malmö

**Diarienummer**

FSN-2026-5153

**Yttrande**

**Till**

Stadskontoret

**Förvaltningsremiss - Ett statligt identitetskort,  
Ju2026/01595  
STK-2026-1043**

Funktionsstödsförvaltningen lämna följande yttrande:

**Sammanfattning**

Funktionsstödsförvaltningen bedömer att en sammanhållen statlig identitetsinfrastruktur kan bidra till ökad rättssäkerhet och säkerhet samt stärka arbetet mot identitetsmissbruk, felaktiga utbetalningar och välfärdsbrott. Särskilt betydelsefull är den starkare kopplingen mellan den fysiska personen, den statliga identitetshandlingen och den elektroniska identiteten.

Samtidigt innebär den föreslagna behandlingen av biometriska uppgifter och den ökade koncentrationen av identitetsinformation betydande krav på informationssäkerhet och skydd för den personliga integriteten. Förvaltningen vill särskilt framhålla riskerna för ändamålsglidning, obehörig åtkomst och felaktig biometrisk identifiering.

**Yttrande**

Funktionsstödsförvaltningen bedömer att en sammanhållen statlig identitetsinfrastruktur kan bidra till ökad rättssäkerhet och säkerhet samt stärka arbetet mot identitetsmissbruk, felaktiga utbetalningar och välfärdsbrott. Särskilt betydelsefull är den starkare kopplingen mellan den fysiska personen, den statliga identitetshandlingen och den elektroniska identiteten.

Samtidigt innebär den föreslagna behandlingen av biometriska uppgifter och den ökade koncentrationen av identitetsinformation betydande krav på informationssäkerhet och skydd för den personliga integriteten. Förvaltningen vill särskilt framhålla riskerna för ändamålsglidning, obehörig åtkomst och felaktig biometrisk identifiering.



Förvaltningen vill särskilt framhålla följande:

- Kommunala myndigheter bör ges ändamålsenliga möjligheter att elektroniskt verifiera statliga identitetshandlingars giltighet utan att få generell tillgång till biometriska uppgifter eller det bakomliggande registret.
- Den statliga e-legitimationen bör utformas så att den kan användas på ett enkelt och säkert sätt i kommunala digitala tjänster.
- Tillgänglighet för personer med funktionsnedsättning behöver säkerställas såväl vid ansökan och utlämnande som vid användningen av den statliga e-legitimationen.
- Biometriska kontroller behöver utformas och följas upp så att risken för felaktig identifiering och diskriminerande effekter minimeras.
- Alternativa sätt att identifiera sig och ta del av offentlig service behöver finnas för personer som inte kan använda den elektroniska lösningen.

### **Ett sammanhållet system för statlig identifiering**

Förvaltningen ser positivt på ambitionen att skapa ett säkrare och mer enhetligt system för statliga identitetshandlingar.

Förslaget innebär att staten framöver ska utfärda ett statligt identitetskort som ersätter de identitetskort som staten utfärdar i dag. Kortet ska kunna utfärdas med eller utan funktion som resehandling.

För svenska medborgare ska kortet kunna utfärdas med resefunktion och därmed användas i stället för pass i de situationer där detta medges. Det innebär att det nya statliga identitetskortet övertar den funktion som dagens nationella identitetskort har som resehandling.

Passet kommer samtidigt att finnas kvar som resehandling. Även andra identitetshandlingar och handlingar med särskilda funktioner kommer att kunna finnas kvar. Reformen innebär således inte att samtliga andra identitetshandlingar försvinner, utan framför allt att statens nuvarande identitetskortsutfärdande samlas och standardiseras.

Förvaltningen bedömer att en sådan ordning kan underlätta även för kommunala verksamheter. Färre typer av statliga identitetshandlingar, en gemensam säkerhetsnivå och tydligare möjligheter att kontrollera en handlings giltighet kan minska osäkerheten vid identitetskontroller.



### **Statlig e-legitimation**

En central del av förslaget är att det statliga identitetskortet ska innehålla en statlig e-legitimation.

Förvaltningen ser positivt på att den fysiska och elektroniska identiteten därmed kan knytas samman i en gemensam statligt säkerställd identitetskedja. Detta kan ge en hög grad av säkerhet kring vem som faktiskt genomför en elektronisk identifiering.

För kommunerna är detta betydelsefullt eftersom en allt större del av kontakterna med invånare i framtiden kommer ske genom digitala tjänster. En statlig e-legitimation med hög tillitsnivå kan ge kommunerna bättre förutsättningar att med hög säkerhet fastställa vem som använder en digital tjänst.

Förvaltningen anser därför att den statliga e-legitimationen från början bör utformas för att på ett enkelt och standardiserat sätt kunna användas i kommunala digitala tjänster.

Samtidigt behöver det finnas alternativa sätt att identifiera sig och ta del av kommunal service. Tillgång till kommunala insatser och myndighetsutövning får inte i praktiken bli beroende av att en enskild person kan använda en viss digital identifikationslösning.

### **Betydelse för arbetet mot välfärdsbrott**

Förvaltningen bedömer att förslaget kan få stor betydelse för arbetet med att förebygga och motverka välfärdsbrott. Förvaltningen vill dock påtala att det höjda säkerhetsförfarandet vid ansökan och utlämnande av ID-kort inte kommer få större effekt om inte myndigheterna säkerställer att de har rutiner på plats för identifiering.

Välfärdssystemen är beroende av att myndigheter med tillräcklig säkerhet kan fastställa att den person som ansöker om en insats, ersättning eller annan förmån också är den person som denne uppger sig vara. Likaså att intygsskrivaren är den som skrivit intyget på den brukaren/patienten som uppges ha undersökts. Särskilt betydelsefullt är därför möjligheten att genom biometriska kontroller stärka kopplingen mellan identiteten och den fysiska personen.

Den statliga e-legitimationen kan på motsvarande sätt bidra till att stärka säkerheten i digitala processer. Detta är särskilt relevant i takt med att ansökningar, uppgiftslämnande, beslut och andra moment inom välfärdssystemen digitaliseras.

Som Förvaltningen framfört ovan, löser säker identifiering en del av problematiken kring välfärdsbrott men inte allt. En korrekt verifierad identitet innebär inte att de sakuppgifter som personen lämnar är korrekta. En förstärkt identitetskontroll behöver därför kombineras med fortsatt utveckling av riskbaserade kontroller, informationsutbyte och andra åtgärder för att förebygga och upptäcka välfärdsbrott.



Det är särskilt viktigt att en hög tillitsnivå vid elektronisk identifiering inte skapar en felaktig föreställning om att även de uppgifter som lämnas av den identifierade personen därmed är tillförlitliga.

### **Kommunernas möjligheter att verifiera identitetshandlingar**

Kommunala myndigheter har i många verksamheter ett legitimt behov av att kunna kontrollera en persons identitet och en identitetshandlings giltighet.

Förvaltningen ser därför positivt på möjligheten att elektroniskt kunna kontrollera om ett statligt identitetskort är giltigt.

Vid den fortsatta utvecklingen bör kommunala myndigheter ges möjlighet att på ett enkelt och säkert sätt verifiera statliga identitetshandlingar.

Utgångspunkten bör vara att kommunen endast får tillgång till den information som är nödvändig för den aktuella kontrollen.

En sådan verifieringstjänst skulle exempelvis kunna lämna besked om att en identitetshandling är giltig, ogiltig eller spärrad utan att kommunen ges generell åtkomst till det bakomliggande registret eller till biometriska uppgifter.

Det skulle enligt Förvaltningens bedömning kunna ge betydande nytta i arbetet mot identitetsmissbruk och välfärdsbrott samtidigt som principerna om dataminimering och skydd för den personliga integriteten upprätthålls.

### **Tillgänglighet och delaktighet**

Förvaltningen anser att tillgänglighetsperspektivet behöver ges stor betydelse vid genomförandet av reformen. Krav på personlig inställelse, biometrisk registrering och användning av elektroniska identifieringslösningar kan innebära särskilda svårigheter för personer med vissa funktionsnedsättningar.

Förvaltningen ser därför positivt på att promemorian innehåller möjlighet att i särskilda situationer göra undantag från kravet på personlig inställelse för personer som på grund av sjukdom eller funktionsnedsättning är förhindrade att inställa sig.

Det är samtidigt viktigt att tillgänglighetsperspektivet inte begränsas till själva ansökningsförfarandet. Tekniska lösningar behöver därför utformas så att de kan användas av personer med olika typer av fysiska, kognitiva och sensoriska funktionsnedsättningar.

Det behöver också finnas fungerande alternativa förfaranden när den ordinarie tekniska lösningen inte kan användas. Förvaltningen vill särskilt betona att hög säkerhet och hög tillgänglighet inte bör betraktas som motstående intressen.



Ett identitetssystem som vissa grupper i praktiken inte kan använda riskerar i stället att leda till att mindre säkra alternativa lösningar behöver användas.

Tillgänglighet bör därför vara en del av systemets säkerhets- och kvalitetskrav redan vid utformningen.

### **Risk för diskriminering**

Användningen av biometriska uppgifter innebär särskilda risker som behöver beaktas.

Promemorian uppmärksammar själv vikten av att personuppgifter behandlas på ett sådant sätt att risken för diskriminering och felaktig identifiering minimeras vid automatiserade biometriska jämförelser.

Förvaltningen delar denna bedömning. Vi vet att systemen idag kommer med inbyggd bias och riskerna är därför stora med dagens system.

Felaktig identifiering kan få betydande konsekvenser för den enskilde, särskilt om biometriska system används i samband med myndighetsutövning, brottsbekämpning eller tillgång till offentliga förmåner.

Biometriska system behöver därför kvalitetssäkras och följas upp med avseende på både den samlade träffsäkerheten och eventuella systematiska skillnader mellan olika grupper.

Även utformningen av ansöknings- och användningsprocesserna kan få indirekt diskriminerande konsekvenser.

Personer med funktionsnedsättning, äldre personer, personer med begränsad digital vana eller personer som av andra skäl har svårare att använda digital teknik får inte i praktiken ges sämre tillgång till offentlig service eller utsättas för mer ingripande kontroll enbart på grund av svårigheter att använda den ordinarie tekniska lösningen.

Förvaltningen anser därför att konsekvenserna för olika grupper bör följas upp efter införandet och att det bör finnas tydliga rutiner för att identifiera och åtgärda systematiska skillnader.

### **Personlig integritet**

Förvaltningen konstaterar att förslaget innebär behandling av särskilt skyddsvärda personuppgifter.

Biometriska uppgifter skiljer sig från många andra personuppgifter genom att de är varaktigt knutna till individen. Ett lösenord eller en elektronisk behörighet kan bytas efter en säkerhetsincident, medan exempelvis ansiktsdrag och fingeravtryck inte kan ersättas på motsvarande sätt.



Det ställer mycket höga krav på hur uppgifterna samlas in, lagras, används och görs tillgängliga.

Utgångspunkten bör även fortsättningsvis vara att en myndighet endast får tillgång till den information som är nödvändig för det aktuella ändamålet.

### **Koncentration av flera funktioner till samma identitetshandling**

Det nya statliga identitetskortet kommer att kunna fylla flera funktioner. För svenska medborgare kan samma kort fungera som fysisk identitetshandling, resehandling och bärare av den statliga e-legitimationen.

Det innebär betydande praktiska fördelar men skapar samtidigt ett ökat beroende av en och samma handling. Om kortet tappas, stjäls, skadas eller behöver spärras kan flera funktioner påverkas samtidigt.

Förvaltningen anser därför att systemet behöver utformas med tydliga och lättillgängliga rutiner för spärr, återställning och utfärdande av ny handling. Det behöver också säkerställas att en enskild inte under en längre tid utestängs från nödvändiga offentliga digitala tjänster på grund av att kortet eller dess elektroniska funktion har spärrats.

### **Risk för ändamålsglidning**

Förvaltningen vill särskilt uppmärksamma risken för ändamålsglidning.

En central identitetsinfrastruktur med biometriska uppgifter kan över tid skapa önskemål om att uppgifterna ska användas för ytterligare ändamål.

Varje sådan utvidgning behöver föregås av en självständig bedömning av behov, proportionalitet, rättssäkerhet och konsekvenser för den personliga integriteten.

Det är därför viktigt att ändamålen för vilka biometriska uppgifter får behandlas är tydligt reglerade och att möjligheten att använda uppgifterna för andra syften inte successivt utvidgas utan motsvarande rättssäkerhets- och integritetsbedömningar.

### **Samlad bedömning**

Förvaltningen bedömer sammantaget att förslaget kan bidra till en säkrare och mer tillförlitlig identitetsförvaltning och därigenom stärka rättssäkerheten, den digitala förvaltningen och arbetet mot identitetsmissbruk, felaktiga utbetalningar och välfärdsbrott.

Särskilt positivt är möjligheten att skapa en starkare och mer sammanhållen koppling mellan fysisk person, statlig identitetshandling och elektronisk identitet.



Förvaltningen ser också fördelar med att statens identitetskortsutfärdande samlas i en gemensam handling och att kortet kan kombinera fysisk identifiering, elektronisk identifiering och, för svenska medborgare, funktion som resehandling.

Samtidigt innebär central behandling av identitetsuppgifter och biometri betydande integritets- och informationssäkerhetsrisker. Dessa behöver hanteras genom tydliga ändamålsbegränsningar, restriktiv och behovsstyrd åtkomst, dataminimering, hög informationssäkerhet och effektiv kontroll av hur uppgifterna används.

Förvaltningen anser därutöver att tillgänglighet och likvärdighet måste betraktas som grundläggande krav på den nya identitetsinfrastrukturen. Personer med funktionsnedsättning eller andra svårigheter att använda de ordinarie tekniska lösningarna måste erbjudas tillgängliga och rättssäkra alternativ.

Biometrisk system behöver utformas och följas upp så att risken för felaktig identifiering och diskriminerande effekter minimeras. Automatiserad identifiering bör inte ensam få leda till negativa konsekvenser för den enskilde utan möjlighet till mänsklig kontroll och rättelse.

Ur ett kommunalt perspektiv bör den fortsatta utvecklingen särskilt inriktas på att kommunala myndigheter får möjlighet att på ett enkelt och säkert sätt verifiera statliga identitetshandlingars giltighet och använda den statliga e-legitimationen utan att få tillgång till fler personuppgifter än vad som krävs för det aktuella ändamålet.

Förvaltningen anser slutligen att möjligheten till riskbaserad förstärkt identifiering vid särskilt riskfyllda moment inom välfärdssystemen bör övervägas i det fortsatta arbetet.

En sådan utformning kan enligt Förvaltningens bedömning ge betydande nytta för såväl den enskildes rättssäkerhet som arbetet mot välfärdsbrott, samtidigt som skyddet för personlig integritet, tillgänglighet och likabehandling upprätthålls.

Direktör

Charlotte Widén Odder

Ansvarig utredare

Nicolas Ferreria