Nils Fjelkegård
010-574 91 56

PM

Datum
2012-10-18

Dnr 131 713026-12/113

E-legitimationsnämndens övergripande synpunkter på kluster 3 i förslaget till EU-förordning om elektronisk identifiering och betrodda tjänster

Med hänsyn till kommande rådsarbetsgruppsmöten där förhandling i frågan avseende kommissionens förslag till förordning om elektronisk identifiering och betrodda tjänster pågår inkommer E-legitimationsnämnden med följande övergripande synpunkter på kluster 3 (motsvarande kapitel 2). Då det fortfarande rör sig om ett tidigt skede på förhandlingarna och förslaget troligtvis kommer att förändras i sina huvuddrag avvaktar E-legitimationsnämnden med att lämna synpunkter på alltför detaljerad nivå, utan nöjer sig med att tills vidare lämna synpunkter av mer övergripande karaktär.

1 Generella synpunkter

Först bör givetvis framhållas att det är positivt att kommissionen genom förordningsförslaget slår an en ambitiös ton i förhållande till gränsöverskridande elektronisk identifiering och betrodda tjänster, vilket visar på en genuin vilja att lösa ut en av de kanske viktigaste knutfrågorna i den Europeiska e-förvaltningen. Av naturliga skäl fokuserar dock nedanstående genomgång i större utsträckning på synpunkter av mer negativ eller ifrågasättande karaktär.

Den enskilt största invändningen som kan riktas mot förslaget i dess nuvarande lydelse är den stora mängd frågetecken som uppkommer i samband med genomläsning. Utan någon sorts vägledning till enskilda artiklars egentliga innebörd och med bristande definitioner av centrala begrepp lämnas ett väldigt stort utrymme för tolkning, vilket gör det svårt att såväl lämna kommentarer som att överblicka vilka konsekvenser förordningen får för nationella aktörer, system och tjänster. Genomgående krävs således ett arbete från kommissionens sida med att mer ingående förklara enskilda artiklars innebörd, tänkbara praktiska implementering samt förväntade konsekvenser. Därefter bör förordningen förtydligas i centrala delar för att säkerställa att tolkningsutrymmet minskar och att artiklarnas lydelse motsvarar ursprunglig intention. De förklarande dokument som kommissionen distribuerat efter förslaget presenterats är dessvärre långt ifrån så pass detaljerade och ingående som krävs för en reell förståelse för förordningen och dess konsekvenser.
En stor del av otydligheten i förordningen härstammar även från de många referenser till delegerade akter och genomförandeakter som kommissionen ges mandat att ta fram vid senare tidpunkt. Att centrala delar i kravställning på aktörer, system och tjänster lämnas till senare gör förslagets konsekvenser i stora delar oöverblickbara och med den förenklade samrådsprocessen vid de delegerade

Nils Fjelkegård
010-574 91 56

PM

Datum
2012-10-18

Dnr 131 713026-12/113

akterna lämnas i mångt och mycket ett tämligen generöst ”carte blanche” från medlemsstaterna till kommissionen avseende stora delar av förordningens mer detaljerade materia. En sådan ordning ger naturligtvis större möjligheter att anpassa förordningens krav efter rådande teknikutveckling men nuvarande delegationsmöjligheter får nog anses vara för långtgående för att säkerställa tillräcklig transparens och överblickbarhet för anslutande leverantörer av betrodda tjänster. Det finns även stora frågetecken kring hur interoperabilitet rent faktiskt ska uppnås mellan de olika betrodda tjänsterna, såväl tekniskt som semantiskt och juridiskt, där flertalet centrala frågor lämnas att lösas vid senare implementering.

Vad gäller övriga mer generella synpunkter kopplat till elektronisk identifiering så tas sådana upp nedan under respektive artikel i kapitel 2.

2 Synpunkter på enskilda artiklar

2.1 Kluster 3 (kapitel 2)

2.1.1 Artikel 5

Som tidigare framhållits är det positivt att kommissionen föreslår en lösning som till stora delar bygger på ömsesidigt erkännande och godtagande, då detta är en förutsättning för en mer långsiktig och hållbar acceptans av elektroniska identifieringslösningar över gränserna. E-legitimationsnämnden menar dock att den modell för ömsesidigt erkännande som fastslås i förslaget till förordning bygger på delvis fel grunder och riskerar att leda till oönskade konsekvenser för utvecklingen av gränsöverskridande elektronisk identifiering. Det finns därtill stora frågetecken kring hur en sådan modell ska fungera i praktiken, med hänsyn till såväl tekniska som juridiska frågor.
Det vidareutvecklade svenska systemet för elektronisk identifiering som för E-legitimationsnämnden för närvarande arbetar med bygger även det på en modell för ömsesidigt erkännande och godtagande, med utgångspunkt i ett gemensamt tillitsramverk och tydliga spelregler för samtliga anslutande aktörer.
Internationellt ser vi en liknande utveckling i flertalet länder, och även det Europeiska pilotprojektet STORK vilar på en liknande modell med en gemensam syn på tillitsramverk som utgångspunkt för gränsöverskridande erkännande av andra elektroniska identifieringssystem. Gemensamt för de flesta av dessa tillitsbaserade system är att de bygger på följande principer:

a) En gemensam syn på tillitsramverk som fastslår vilka principer som ska gälla för risk- och säkerhetsbedömningar kopplat till elektronisk identifiering

Nils Fjelkegård
010-574 91 56

PM

Datum
2012-10-18

Dnr 131 713026-12/113

c) En möjlighet för förlitande parter att själva göra riskbedömningar med utgångspunkt i tillitsramverket för att definiera en e-tjänsts särskilda skyddsbehov

b) En frivillighet för samtliga aktörer, såväl identitetsutfärdare som förlitande parter, att ansluta sig till systemet

I det förslag till modell för ömsesidigt erkännande och godtagande som föreslås i artikel 5 i den föreslagna förordningen tycks ingen av dessa principer finnas med. Gränsöverskridande elektronisk identifiering inom EU erbjuder givetvis sina speciella svårigheter, och att i viss mån exempelvis behöva göra avkall på principen om frivillighet för att främja en snabbare utveckling av e-förvaltningen är förståeligt. Det är däremot tveksamt till vilken grad det finns ett behov av att göra avkall på möjligheten för förlitande parter i offentlig sektor att utifrån riskbedömningar kunna klassa den egna e-tjänstens skydds- och säkerhetsbehov med utgångspunkt i ett transparent och tydligt tillitsramverk. Det är förlitande part som har ansvaret för den erbjudna e-tjänsten som kräver elektronisk identifiering, vilket exempelvis innebär ansvar för det persondataskydd som måste erbjudas med hänsyn till karaktären på de personuppgifter som behandlas. Att den förlitande parten inte på något sätt själv kan bestämma över vilken säkerhet och skyddsnivå som krävs för åtkomst till tjänsten går emot den princip som i övrigt utgör normen på e-förvaltningsområdet, åtminstone i Sverige. Kommissionen har i förtydligande dokument klargjort att frågan om tillitsramverk och tillitsnivåer kan bli aktuell inom ramen för det samarbete för interoperabilitet som fastslås i artikel 8. Principen om förlitande parts möjlighet att utifrån riskbedömning skyddsklassa sin e-tjänst är emellertid så pass viktigt att det på något sätt bör finnas med redan i förordningstexten. Åtminstone bör det finnas med en möjlighet för medlemsstaterna att undanta särskilt skyddsvärda e-tjänster från artikel 5.

Vidare finns det en hel del frågetecken kring vad som egentligen avses med ”godtas för åtkomst” ur ett såväl tekniskt som juridiskt perspektiv. Hur pass långtgående är skyldigheten för den enskilda e-tjänsten att acceptera en utländsk e-legitimation som notifierats? Kan exempelvis e-tjänsten godta e-legitimationen men neka åtkomst på basis av att särskilda attribut saknas som krävs för nyttjande av tjänsten (ett exempel här kan vara svenskt personnummer)? Vilken tolkning som görs i detta avseende får långtgående konsekvenser för uppbyggnaden och anpassningen av nationella e-tjänster och med hänsyn till det stora antal frågor kring exempelvis nationella attribut och identifiering av fysiska och juridiska personer som fortfarande saknar en gränsöverskridande lösning är det svårt att se att det skulle finnas några Europeiska e-tjänster som i dagsläget kan uppfylla

Nils Fjelkegård
010-574 91 56

PM

Datum
2012-10-18

Dnr 131 713026-12/113

kraven i artikel 5. Detta särskilt med hänsyn till den otydlighet kring vilken teknisk infrastruktur som ska gälla för acceptans av utländska e-legitimationer. Pilotprojektet STORK nämns förvisso i anslutning till förordningen, men det är högst oklart om det är denna tekniska infrastruktur som avses ligga till grund för den gränsöverskridande tekniska acceptansen.

2.1.2 Artikel 6

1(a)

Tidigare frågetecken kring vad som avses med att ett medel för elektronisk identifiering är utfärdat på den anmälande medlemsstatens ansvar får anses vara delvis utredda med hänsyn till kommissionens förtydliganden i det avseendet. Det står nu klart att kommissionen med artikeln inte avser exkludera nationella lösningar som bygger på privata aktörer som utfärdare av e-legitimation, utan även sådana nationella system kan notifieras förutsatt att medlemsstaten ikläder sig det skadeståndsansvar som stipuleras i 1(e). Detta innebär att det inte bör innebära några principiella problem att notifiera vare sig existerande eller kommande svenskt system för elektronisk identifiering. Med detta dock inte sagt att det inte finns andra problem relaterade till ett medlemsstatligt skadeståndsansvar. Dessa problem diskuteras nedan under 1(e).

1(c)

Det finns fortfarande stora frågetecken kring vad som avses med såväl ”personidentifieringsuppgifter” som ”otvetydigt hänför sig till”, vilket gör det svårt att bedöma vilket faktiskt ansvar medlemsstaten ikläder sig. Vare sig personidentifieringsuppgifter eller otvetydigt definieras i förordningens artikel 2, och ytterst lite ledning ges i de efterföljande förklaringarna från kommissionens sida. I förordningen görs konsekvent en åtskillnad mellan medel för elektronisk identifiering och personidentifieringsuppgifter, och det tycks enligt formuleringarna inte vara så att medlemsstaten ska garantera att själva medlet för elektronisk identifiering otvetydigt hänför sig till personen, utan enbart personidentifieringsuppgifterna. Av efterföljande förklaringar från kommissionen kan man emellertid uttyda att den otvetydiga kopplingen mellan personidentifieringsuppgifter och person görs i samband med registreringsprocessen, vilket pekar på att medlemsstatens ansvar sträcker sig längre än att exempelvis enbart garantera kopplingen mellan ett unikt personnummer och en person. Den ansvarsmodell som Svensk e-legitimation

Nils Fjelkegård
010-574 91 56

PM

Datum
2012-10-18

Dnr 131 713026-12/113

bygger på förutsätter att en utfärdare av svensk e-legitimation tar ett helhetsansvar för själva utfärdandeprocessen, och garanterar att de rutiner och krav för respektive tillitsnivå i tillitsramverket uppfylls i samband med utfärdandet. Att säkerställa att rätt person ansöker om en e-legitimation, att e-legitimationen enbart hänför sig till en unik person och att e-legitimationen i senare led distribueras till rätt person är alla centrala delar i detta ansvarstagande. Att enbart ta ansvar för en del av utfärdandeprocessen leder till att centrala delar i ansvarskedjan faller bort, och även om vi kan säkerställa att e-legitimationen hänför sig till en unik person finns det i sådant fall inget ansvar förknippat med att exempelvis i ett senare led dela ut den till någon helt annan. Exakt hur långt ansvaret som regleras i 1(c) sträcker sig måste bli fråga för fortsatt utredning i dialog med kommissionen, men oavsett svaret på den frågan finns det en stor risk att det vid ett begränsat ansvar blir alltför uddlöst, och vid ett fullständigt ansvar blir alltför betungande. Att under ett mer fullständigt ansvar garantera en otvetydig koppling mellan en person och en e-legitimation torde kräva en utfärdandeprocess som åtminstone motsvarar nivå 4 enligt det föreslagna svenska tillitsramverket. Då nuvarande svenska e-legitimationer bedöms motsvara ungefär nivå 3 enligt tillitsramverket kan detta innebära svårigheter för svensk del att överhuvudtaget notifiera några svenska e-legitimationer för gränsöverskridande användning.

1(d)

Vad gäller 1(d) har kommissionen förtydligat att kravet på en kostnadsfri ”autentiseringsmöjlighet” enbart ska gälla vid gränsöverskridande användning, vilket är positivt för svenskt vidkommande då en central del i den nationella försörjningen av tjänster för elektronisk identifiering bygger på kostnadsbelagd autentisering. Det återstår emellertid en hel del frågetecken kopplat till hur autentiseringstjänsten rent tekniskt och affärsmässigt ska tillhandahållas. Den modell för autentisering som föreslås inom ramen för Svensk e-legitimation bygger på SAML 2.0, där standardiserade identitetsintyg utbyts mellan en identitetsutfärdare och en förlitande part. För en förlitande part som ingår i samma identitetsfederation som identitetsutfärdaren finns det inget behov av att ytterligare autentisera eller validera ett sådant identitetsintyg, utan den federerade modellen bygger på tillit till och mellan anslutna parter. Det finns således ingen autentiseringstjänst där man som eventuell tredje förlitande part skulle kunna stoppa ett identitetsintyg som kommer från en utfärdare av svensk e-legitimation för att få det autentiserat eller validerat. Någon sådan teknisk modell förutses inte inom ramen för Svensk e-legitimation och tillämpningen av SAML-standarden utan istället förutsätts att samtliga förlitande parter är anslutna till

Nils Fjelkegård
010-574 91 56

PM

Datum
2012-10-18

Dnr 131 713026-12/113

identitetsfederationen, antingen i egen regi eller genom en proxy-IDP som representerar en annan federation med motsvarande överenskommen tillit. På så sätt fungerar exempelvis autentisering genom PEPS-noder enligt den av STORK föreslagna Europeiska infrastrukturen för gränsöverskridande elektronisk identifiering. Om det med autentiseringsmöjlighet menas att exempelvis tillhandahålla en nationell PEPS-nod så innebär detta krav inte några tekniska svårigheter från ett svenskt perspektiv. Det innebär dock att en förlitande part måste vara tekniskt ansluten till ett motsvarande nationellt system med en motsvarande nationell PEPS-nod för att kunna autentisera ett identitetsintyg som härstammar från en svensk e-legitimation. Huruvida det är förenligt med förordningens och den specifika artikelns krav på att inte införa några särskilda tekniska krav på förlitande part är svårt att överskåda. Att samtliga eventuella förlitande parter ska kunna få tillgång till en autentiseringstjänst via Internet verkar härstamma från en syn på e-legitimationen som ett certifikatbaserat verktyg där spärrlistor publiceras kostnadsfritt, på motsvarande sätt som för kvalificerade certifikat för elektronisk signatur. Kommissionen är dock tydlig med att förordningen ska vara teknikneutral med hänsyn till valda tekniska lösningar för respektive nationellt system för elektronisk identifiering, vilket borde innebära att även icke certifikatbaserade lösningar borde kunna notifieras. Därmed återstår den stora frågan hur en sådan autentiseringstjänst rent praktiskt ska kunna introduceras och göras förenlig med de krav som ställs upp i artikel 6.
Vidare är det oklart hur de affärsmässiga aspekterna av gränsöverskridande kostnadsfri autentisering ska lösas mellan medlemsstaterna. Så länge det inte påverkar eventuella möjligheter till kostnadsbelagda autentiseringstjänster nationellt bör det dock finnas möjlighet att mellan medlemsstaterna komma överens om en modell där var medlemsstat bär de egna kostnaderna för eventuell användning av nationella e-legitimationer i utlandet.

1(e)

Kommissionen har förtydligat att medlemsstatens skadeståndsansvar ska begränsas till vårdslöshet och att det inte finns några begränsningar i hur den nationella fördelningen eller delegeringen av skadeståndsansvaret kan konstrueras. Det finns dock fortfarande ett antal mer principiella invändningar mot det förslag som presenteras.
För det första är det diskutabelt om en modell med ett medlemsstatligt skadeståndsansvar är ett bra instrument för att garantera en adekvat säkerhetsnivå i notifierade system för elektronisk identifiering. Då de potentiella skadelidande parterna till största del kommer att röra sig om olika förlitande parter i form av

Nils Fjelkegård
010-574 91 56

PM

Datum
2012-10-18

Dnr 131 713026-12/113

offentliga e-tjänster, kommer en eventuell skadeståndstalan med största sannolikhet att väckas av en medlemsstat (i egenskap av tillhandahållare av e-tjänst) mot en annan medlemsstat (i egenskap av ansvarig för systemet för elektronisk identifiering). Är det verkligen kommissionens tanke med den här förordningen att skapa en ordning där medlemsstater förväntas stämma andra medlemsstater för bristande tillgänglighet i autentiseringstjänster eller för vårdslöshet i registreringen av personidentifieringsuppgifter? Hur realistiskt är det att sådana skadeståndsprocesser kommer att aktualiseras mellan medlemsstaterna? Vilka forum- och lagvalsregler ska gälla för sådana processer mellan medlemsstaterna? Vidare finns det i enlighet med ovan fört resonemang i samband med övriga artiklar betydande oklarheter kring omfattningen och definitionen av medlemsstatens ansvar avseende såväl den otvetydiga kopplingen och autentiseringstjänsten. Att basera hela grundmodellen för tillit mellan de notifierade systemen på ett otydligt skadeståndsansvar medlemsstaterna mellan riskerar att driva säkerhetsnivåerna uppåt till oproportionerliga nivåer utav rädsla för att notifiera annat än extremt säkra och därmed kostsamma system, samtidigt som det vid faktiska fall av allvarliga incidenter riskerar att bli ett trubbigt instrument för att garantera fortsatt säkerhet och tillit till de notifierade systemen. Vidare är skadeståndsansvarets potentiella konsekvenser svåröverblickbara då det inte finns någon egentlig begränsning av ansvar eller vem som kan anses vara skadelidande och således äger rätt att väcka talan. Även om kommissionen har klargjort att vårdslöshet ska krävas framgår inte detta av förordningen och i förordningen redogörs inte heller närmre för bevisbördans placering mellan parterna. I ett system såsom det som föreslås för Svensk e-legitimation där privata utfärdare har en central roll riskerar vi att tappa intresse från flertalet utfärdare, alternativt driva stora kostnader för offentlig sektor, om ett svåröverblickbart skadeståndsansvar enligt förordningen ska speglas i en nationell kravställning av utfärdare.

2.1.3 Artikel 7

Här finns ett par ytterligare otydligheter kopplat till ovan fört resonemang. Enligt artikel 6 förutsätts medlemsstaten ta ett ansvar för notifierade system för elektronisk identifiering. I artikel 7(b) står det att det ska finnas en eller flera myndigheter som ansvarar för det anmälda systemet. Blir det i fallet Svensk e-legitimation, med privata utfärdare, frågan om att E-legitimationsnämnden blir ansvarig myndighet, eller är det snarare frågan om en eller flera tillsynsmyndigheter som blir ansvariga? Behöver det finnas en tydligt utpekad myndighet och hur långt sträcker sig i sådant fall ansvaret för den ansvarige myndigheten?

Nils Fjelkegård
010-574 91 56

PM

Datum
2012-10-18

Dnr 131 713026-12/113

Vidare är det oklart vad som avses med punkten (c) där information ska anges om vem som registrerar de otvetydiga personidentifieringsuppgifterna. Avses här eventuella privata utfärdare av e-legitimation och processen i samband med utfärdande av e-legitimationen, eller avses något annat med den registreringsprocessen, som snarare hänför sig till registrering i folkbokföringsregister eller motsvarande? Se vidare resonemang under artikel 6(c) kring otydligheten kopplat till personidentifieringsuppgifter.

2.1.4 Artikel 8

Med hänsyn till den stora andel frågetecken som uppstår i samband med övriga artiklar, får det antas att kommissionen ser framför sig att flertalet frågor av mer specifik karaktär ska lösas ut genom efterföljande samordning och genom delegerade akter. Samordning mellan medlemsstaterna är givetvis positivt och en förutsättning för att gränsöverskridande interoperabilitet ska uppnås, men frågan är om det inte är för många och för stora frågetecken som förväntas lösas i dessa efterföljande processer. Medlemsstaternas möjlighet att uppfylla de krav som ställs upp i tidigare artiklar blir helt avhängiga resultaten i kritiska avvägningar mellan medlemsstaterna avseende juridiska, affärsmässiga och tekniska frågor. Frågan är om man inte gör bättre i att först försöka hitta en mellanstatlig lösning på de centrala frågor som återstår, för att säkerställa att det finns juridiska, tekniska och affärsmässiga förutsättningar för en reglering av den karaktären som föreslås innan förordningen beslutas och träder i kraft.

Vidare kan det ifrågasättas vilken grad av teknikneutralitet i de egna nationella system för elektronisk identifiering som tillåts enligt förordningen, med hänsyn till att kommissionen ges en tämligen långtgående möjlighet att genom delegerade akter specificera tekniska minimikrav på de system som notifieras och förväntas användas i en gränsöverskridande kontext. Om de tekniska krav som ställs upp för gränsöverskridande användning exempelvis förutsätter certifikatbaserade lösningar finns det en risk att flertalet av kommande svenska e-legitimationer inte kan notifieras. Här bör det finnas ett större mått av tydlighet från kommissionens sida vilken teknisk lösning och vilka tekniska minimikrav man ser framför sig inom ramen för sådana delegerade akter.