



EUROPEISKA KOMMISSIONEN

Bryssel den 4.6.2012
SWD(2012) 136 final

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

Följedokument till

**Förslag till
EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING**

**om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den
inre marknaden**

{COM(2012) 238 final}
{SWD(2012) 135 final}

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

Följedokument till

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

1. POLITISK BAKGRUND, FÖRFARANDE OCH SAMRÅD MED BERÖRDA PARTER

Att bygga upp förtroendet för nätmiljön är avgörande för den ekonomiska utvecklingen. Bristande förtroende gör att konsumenter, företag och myndigheter tvekar att utföra transaktioner på elektronisk väg och att använda nya tjänster. Det föreslagna initiativet till ett regelverk syftar till att möjliggöra säkra och sömlösa elektroniska transaktioner mellan företag, medborgare och förvaltningar, för att därigenom göra offentliga och privata elektroniska tjänster, e-affärer och e-handel mer effektiva.

Det finns hinder för gränsöverskridande e-tjänster och dessa måste undanröjas. För att utgöra produktiva förutsättningar snarare än hinder måste följaktligen **e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster** ömsesidigt erkännas och godtas i hela EU.

Det finns inget heltäckande, gräns- och sektorsövergripande regelverk i EU för e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster. På EU-nivå finns endast ett regelverk för e-signaturer, men inget för e-identifiering och e-autentisering eller närliggande stödjande betrodda tjänster. I *En digital agenda för Europa* meddelade kommissionen att den skulle föreslå lagstiftningsåtgärder för att gå vidare i arbetet med e-signaturer samt för att säkerställa ömsesidigt erkännande av e-identifiering och e-autentisering i syfte att undanröja fragmentering och brist på interoperabilitet, främja det digitala medborgarskapet och förebygga it-brottslighet.

För att utföra denna konsekvensbedömning inhämtade kommissionen återkoppling från medlemsstaterna, Europaparlamentet och andra berörda parter under diskussioner, workshoppar och konferenser. Kommissionen inledde ett antal undersökningar med avseende på e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster samt gjorde en genomgång av litteraturen på området. Ett offentligt samråd genomfördes 2011 för att inhämta synpunkter på hur e-identifiering, e-autentisering och e-signaturer kan bidra till den inre marknaden. Samrådet kompletterades av en riktad undersökning för att ta del av små och medelstora företags särskilda synpunkter och behov.

2. PROBLEMFORMULERING

Användare kan stöta på svårigheter när det gäller den gränsöverskridande användningen av e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster. De

främsta hindren för säkra och sömlösa gränsöverskridande tjänster i form av e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster är följande:

1 — Fragmentering av marknaden: Olika regler gäller för tjänstetillhandahållare beroende på i vilken medlemsstat de tillhandahåller sina tjänster.

När det gäller e-signaturer är den harmonisering som genomförts genom direktiv 1999/93/EG om e-signaturer ofullständig. Följande fyra problem har identifierats: Ett olikartat genomförande på nationell nivå som beror på medlemsstaternas skiljaktiga tolkningar av direktivet. Ett faktiskt åberopande av ett undantag för tillämpningar inom den offentliga sektorn. Förlegade standarder och otydliga tillsynsskyldigheter som leder till problem med den gränsöverskridande interoperabiliteten. Ett splittrat EU-landskap och snedvridningar på den inre marknaden.

När det gäller e-identifiering leder olika tekniska lösningar för personlig identifiering i enskilda medlemsstater, bristen på rättssäkerhet vid gränsöverskridande användning av e-identifieringar samt bristen på ett tydligt ansvar för identitetsuppgifternas riktighet sammantaget till interoperabilitetsproblem.

När det gäller stödjande betrodda tjänster leder bristen på ett EU-täckande regelverk till att nationell lagstiftning antas för en del av dessa tjänster i en del medlemsstater samt till höga kostnader för tillhandahållare som vill erbjuda sina tjänster i flera medlemsstater. Tillsammans leder detta till att det uppstår hinder och fragmentering på den inre marknaden.

2 — Bristande förtroende: Bristen på förtroende för elektroniska system, för de verktyg som tillhandahålls och för regelverket kan skapa ett intryck av att det finns färre rättsliga garantier vid elektroniskt än vid fysiskt samspel.

För e-signaturer skiljer sig de nationella tillsynskraven kvalitativt mellan medlemsstaterna, vilket gör det komplicerat för parter som är beroende av en e-signatur att bedöma hur en tjänstetillhandahållare övervakas.

För e-identifiering och stödjande betrodda tjänster gör den heterogena nationella lagstiftningen det svårt för användarna att känna sig säkra i samband med samspel på nätet i gränsöverskridande sammanhang.

De fyra främsta orsakerna till dessa problem är följande:

A: Otillräcklig räckvidd för det nuvarande regelverket

E-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster är förutsättningar för en rad olika typer av elektroniskt samspel som t.ex. tjänster för e-bankverksamhet, e-förvaltning och e-hälsa. På EU-nivå finns det ett begränsat och ofullständigt regelverk som är huvudsakligen inriktat på e-signaturer. Det finns inget särskilt regelverk för ömsesidigt erkännande och godtagande av e-identifieringar eller för stödjande betrodda tjänster som t.ex. tidsmärkning och e-sigill.

B: Bristande samordning mellan utvecklingen av e-signaturer och e-identifieringar

Nationella infrastrukturer för e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster har utvecklats isolerat och utan samordning på EU-nivå. Resultatet är att det inte finns någon gränsöverskridande interoperabilitet för tekniska lösningar, vilket skapar hinder för e-transaktioner. Bristen på ömsesidigt erkännande och godtagande är ett av skälen till varför både användare och tillhandahållare av e-tjänster är skeptiska till att använda sig av e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster.

C: Bristande insyn i säkerhetsgarantier

En stark och harmoniserad säkerhet är nödvändig för att tillförlitliga lösningar ska kunna skapas. Detta är särskilt relevant för tillgången till tjänster där känsliga personuppgifter är inbegripna, som t.ex. e-hälsa. I direktiv 1999/93/EG erkänns att rättssäkerhet endast kan ges till e-signaturer som garanterar säkerheten och som alltså är tillräckligt skyddade mot förfalskning eller bedrägeri (avancerade och kvalificerade e-signaturer).

Användarna upplever bristen på säkra system för e-identifiering som ett stort hinder. Bristen på ett harmoniserat regelverk för e-identifieringar innebär att säkerheten och tillförlitligheten hos officiella e-identifieringar inte kan fastställas objektivt över gränserna. Detta skapar gränsöverskridande hinder, med konsekvenser i form av bristande förtroende och en fragmenterad marknad.

Ytterligare ett problem utgörs av identitetsstöld. Säkra e-identifieringar kan bidra till att minska denna risk. Dåligt säkerställda e-identifieringar kan omvänt göra det lättare för brottslingar att skaffa sig falska eller oriktiga e-identifieringar.

D: Bristande kunskap / förtroende hos användare

Komplexiteten hos de tekniker som används för e-transaktioner och den centrala roll som betrodda tredje parter spelar skapar en miljö där det är svårt att bedöma tillförlitligheten. Särskilt slutanvändare, som i allmänhet inte har tillräcklig sakkunskap, måste kunna förlita sig på regler där tydliga rättigheter och skyldigheter för alla berörda parter (tillhandahållare av betrodda tjänster, slutanvändare och förvaltningsorgan).

3. GRUNDSCEARIO

Grundscenariot för initiativet är att inga nya reglerande åtgärder vidtas. Enligt detta scenario skulle de nuvarande problemen utvecklas enligt följande:

Fragmenterings- och interoperabilitetsproblemen skulle inte lösas. Medlemsstaterna skulle sannolikt fortsätta att tillämpa och genomföra direktiv 1999/93/EG.

Rättssäkerheten skulle inte garanteras. De problem som följer av bristen på ömsesidigt erkännande av e-signaturer och avsaknaden av en rättslig ram för ömsesidigt erkännande och godtagande av e-identifieringar och stödjande betrodda tjänster skulle förhindra ett rättsligt erkännande av en rad olika typer av gränsöverskridande samspel.

Användarnas behov skulle inte tillgodoses fullt ut. Enligt det nuvarande regelverket är det inte möjligt att dra full nytta av de möjligheter som erbjuds av den tekniska utvecklingen.

Ledande EU-initiativ skulle inte utnyttjas fullt ut. EU-åtgärder som t.ex. tjänstedirektivet, direktiven om offentlig upphandling och momsdirektivet (e-fakturerings) samt de storskaliga pilotprojekten inom ramen för IKT-stödprogrammet¹ som syftar till att undanröja interoperabilitetsproblem och gränsöverskridande problem som rör erkännande av vissa typer av e-samspel skulle bara kunna genomföras på pilotnivå eftersom det inte finns något gränsöverskridande regelverk.

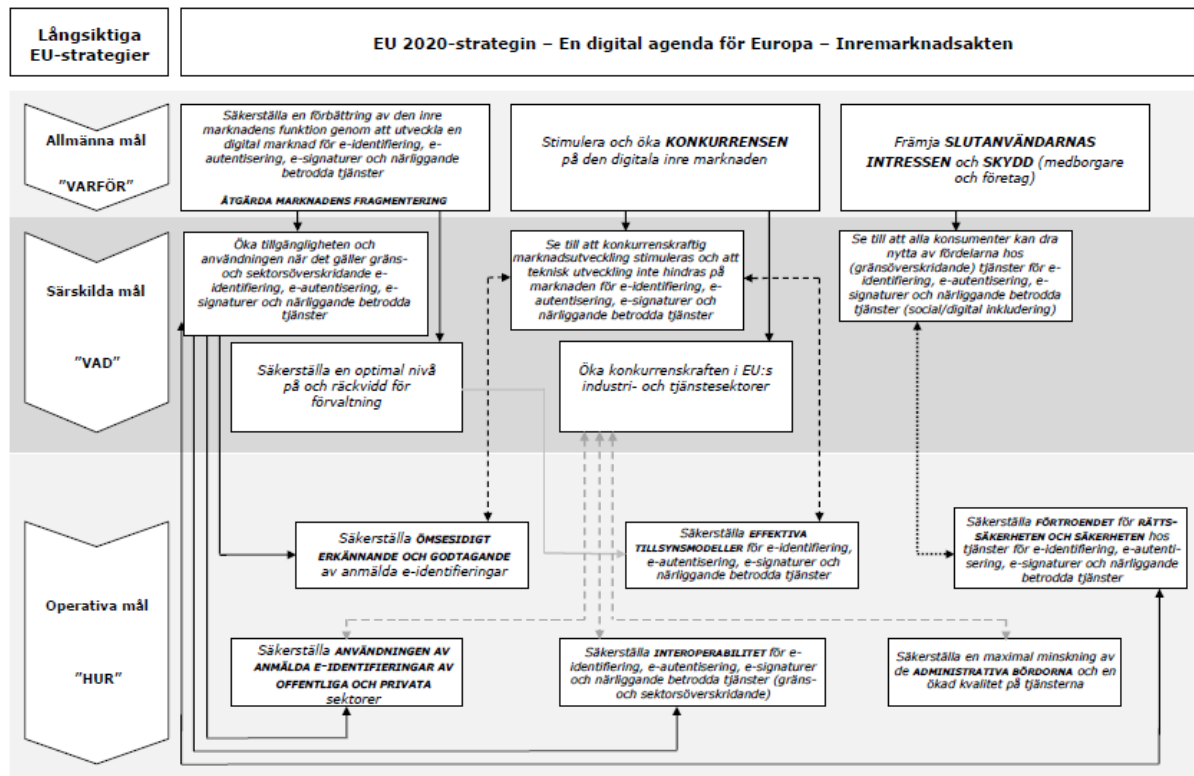
4. POLITISKA MÅL

Följande fyra **allmänna mål** har identifierats: Att säkerställa utvecklingen av en digital inre marknad. Att främja utvecklingen av centrala gränsöverskridande offentliga tjänster. Att stimulera och öka konkurrensen på den inre marknaden. Att öka användarvänligheten (medborgare och företag). Målen ligger i linje med strategiska EU-insatser som t.ex. EU

¹ http://ec.europa.eu/information_society/activities/ict_psp/about.

2020-strategin, En digital agenda för Europa, Inre marknadsakten och En färdplan för stabilitet och tillväxt.

I de **särskilda målen** anges de önskade resultaten när det gäller marknaden för e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster (vad) genom förverkligandet av det **operativa målet** (hur). För varje enskilt mål har ett antal **operativa mål** identifierats.



5. ALTERNATIV

För att lösa problemen och nå ovan angivna mål bedömdes följande tre uppsättningar alternativ: 1) Räckvidden för det planerade regelverket. 2) Rättsligt instrument. 3) Tillsyns nivå.

- Inom ramen för den första uppsättningen, *Regelverkets räckvidd*, har följande fyra alternativ undersökts:

Alternativ 0: Upphävande av direktiv 1999/93/EG och inga reglerande åtgärder rörande e-identifiering eller stödjande betrodda tjänster

Det här alternativet består av ett avslutande av all EU-verksamhet på området för e-signaturer. Direktiv 1999/93/EG skulle upphävas och inga lagstiftningsåtgärder för ömsesidigt erkännande av e-identifieringar skulle föreslås.

- Alternativ 1: Oförändrad politik (grundscenario)*

Direktiv 1999/93/EG skulle behållas som det är. Ingen lagstiftning om e-identifiering skulle föreslås.

- *Alternativ 2: Ökad rättssäkerhet, ökad samordning av nationell tillsyn och säkerställt ömsesidigt erkännande och godtagande av e-identificeringar*

Räckvidden för direktiv 1999/93/EG skulle utökas för att lägga till bestämmelser om gränsöverskridande erkännande och godtagande av system för "anmäld e-identificering"². De bestämmelser i direktivet som avser e-signaturer skulle behöva ändras för att åtgärda dess nuvarande svagheter och därigenom ge en bättre harmonisering av de nationella tillsynsmodellerna.

- *Alternativ 3: Utvidgning för att inbegripa vissa stödjande betrodda tjänster*

Det här alternativet är en utbyggnad av alternativ 2 som innebär att stödjande betrodda tjänster och identifieringsinformation inkluderas i förslagets räckvidd.

De väsentliga stödjande funktioner som skulle införlivas i lagstiftningen är tidsmärkning, e-sigill, långsiktigt bevarande av information, certifierad leverans av e-dokument, e-dokuments giltighet som bevis vid rättsliga förfaranden och autentisering av webbplatser.

- Inom ramen för den andra uppsättningen, som omfattar ett "rättsligt instrument", har följande fyra alternativ undersökts:

Ett heltäckande lagstiftningsinstrument (alternativ A) eller två separata lagstiftningsinstrument (alternativ B)

Lagstiftningen skulle bestå av en enda heltäckande åtgärd som omfattar e-identificering, e-autentisering, och e-signaturer, eller av två åtgärder, dvs. ett beslut från kommissionen om e-identificering och en ändring av direktivet om e-signaturer.

Ett direktiv (alternativ C) eller en förordning (alternativ D)

Lagstiftningen skulle kunna vara ett direktiv eller en förordning.

- På den tredje nivån, *övervakning*, har följande två alternativ beaktats:

Alternativ i): Upprätthållande av nationella tillsynssystem

De nuvarande nationellt baserade tillsynssystemen skulle upprätthållas, men med ökad harmonisering genom gemensamma väsentliga krav.

Alternativ ii): Upprättande av ett EU-baserat tillsynssystem

Ett EU-baserat tillsynssystem skulle upprättas för att minska eller undanröja skillnader mellan nationella tillsynsordningar. Detta skulle kunna ha en av följande två former:

²

"Anmäld e-identificering": Ett system för e-identificeringar som anmälts till kommissionen av en medlemsstat för att erkännas och godtas över gränserna. Begreppet anmäld e-identificering är inte begränsat till e-identificeringar som utfärdats av den offentliga sektorn, även medlemsstaterna skulle kunna anmäla e-identificeringar som utfärdats av den privata sektorn och som de erkänner för användning i deras egna tjänster inom den offentliga sektorn. Den här strategin är nödvändig eftersom alla medlemsstaters myndigheter inte utfärdar e-identificeringar. Den gränsöverskridande lagstiftningsstrategin skulle göra det möjligt för den privata sektorn att integrera användningen av anmälda e-identificeringar i e-tjänster för vilka säker e-identificering behövs.

Underalternativ a: De befintliga nationella tillsynssystemen ersätts av ett enda tillsynssystem och tillsynsorgan på EU-nivå.

Underalternativ b: Ett tillsynssystem och tillsynsorgan på EU-nivå upprättas samtidigt som de nationella tillsynssystemen upprätthålls (varje medlemsstat väljer sitt eget system eller EU-systemet).

6. JÄMFÖRELSE AV ALTERNATIVEN OCH KONSEKVENSERNA

Alternativen har bedömts och jämförts med grundscenariot (alternativ 1) i fråga om effektivitet, ändamålsenlighet och enhetlighet.

6.1. Räckvidd för regelverket

Alternativ 0 skulle inte bidra till att uppnå de mål som identifieras i konsekvensbedömningsrapporten. Det skulle inte öka tillgängligheten och användningen när det gäller gräns- och sektorsöverskridande e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster, säkerställa en optimal förvaltningsnivå, stimulera marknadsutvecklingen, bidra till ökad konkurrenskraft i EU:s industri- och tjänstesektorer eller säkerställa att alla slutanvändare kan dra nytta av fördelarna med e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster. Det skulle tvärtom hindra den tekniska utvecklingen på marknaden för dessa tjänster, störa den nuvarande processen för att möjliggöra gränsöverskridande e-tjänster samt bevara en fragmenterad EU-marknad och ojämna förutsättningar för förtroendet.

Alternativ 1 skulle inte uppnå målen. Det skulle upprätthålla de befintliga oklarheterna och förutsättningarna när det gäller förtroendet för tillsynen skulle förbli ojämna. Den rättsliga osäkerheten skulle kvarstå och ett splittrat EU-landskap skulle fortsätta att utvecklas och leda till snedvridna konkurrensvillkor på den inre marknaden samt öka sannolikheten för skiljaktiga strategier på nationell nivå.

Alternativ 2 skulle öka rättssäkerheten, öka tillsynen och säkerställa ömsesidigt erkännande och godtagande av e-identifieringar, samt väsentligt bidra till att uppnå vart och ett av de mål som identifieras i konsekvensbedömningsrapporten och därmed ge positiva ekonomiska, sociala och miljömässiga resultat.

E-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster skulle bli mer attraktiva och öka avkastningen av investeringar i dessa tjänster och infrastrukturer för dem. E-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster skulle dessutom bli tillgängliga för alla sektorer och alla typer av företag samtidigt som gränsöverskridande hinder skulle undanröjas. Nya marknader och nya investeringar skulle öppnas, vilket i sin tur skulle stimulera innovation.

Den nuvarande fragmenteringen av marknaden skulle minskas, eftersom den gränsöverskridande interoperabiliteten skulle förbättras genom att hänvisningar till tekniska standarder blir möjliga.

Ömsesidigt erkännande och godtagande av e-identifiering skulle bidra till att ytterligare undanröja de nuvarande hindren på den inre marknaden. Slutligen är det sannolikt att den enhetliga tillsyn som skulle följa av gemensamma väsentliga krav skulle öka förtroendet, underlätta upptäckten av bedrägerier och bidra till att förhindra identitetsstöld.

Alternativ 3 skulle göra e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster ännu mer attraktiva och följaktligen öka deras positiva inverkan genom att utvidga regelverket till att inbegripa vissa väsentliga stödjande betrodda tjänster.

*Bedömningen är att det är mer sannolikt att **alternativ 3** kan ha en betydande inverkan på säkra och lättanvända e-transaktioner än alternativen 0, 1 eller 2.*

6.2. Rättsliga instrument

Ett heltäckande regelverk inom ramen för **ett instrument** skulle säkerställa en lagstiftning om de olika aspekterna av e-identifiering, e-autentisering, e-signaturer och närliggande stödjande betrodda tjänster. **Två separata instrument** skulle kunna leda till skillnader när det gäller de lagstiftningsåtgärder som vidtas för e-signaturer och e-identifiering — samt i initiativens strategier, vilket är ännu viktigare.

Att anta ett **direktiv** skulle inte bidra till att lösa de nuvarande problemen med interoperabiliteten för e-signaturer som har sin grund i de skiljaktiga införlivandena av direktiv 1999/93/EG. En **förordning** ger omedelbar tillämplighet utan behov av tolkning och följaktligen ökad harmonisering, vilket betyder att en förordning är mer lämplig för att uppnå målen för den föreslagna förordningen.

En enda förordning verkar vara det effektivaste sättet att uppnå målen.

6.3. Tillsynsnivå

Enligt **alternativ i** skulle man genom ny lagstiftning upprätthålla de nuvarande nationellt baserade tillsynssystemen och belägga tjänstetillhandahållare med gemensamma väsentliga krav. En harmoniserad strategi på EU-nivå för både e-signaturer och stödjande betrodda tjänster skulle göra tillsynen mer effektiv, öka rättssäkerheten samt öka förtroendet för och säkerheten hos e-transaktioner.

Alternativ ii skulle ge homogen och effektiv tillsyn av hög kvalitet i hela EU. **Underalternativ b** har fördelen att ge större flexibilitet än vad som ges med det enda EU-organ för tillsyn som förutses i **underalternativ a**. Det skulle kunna vara fördelaktigt för medlemsstater där inga eller få tillhandahållare av betrodda tjänster är etablerade att överföra tillsynsuppgifter till ett EU-organ för tillsyn. Övriga medlemsstater skulle om de ville kunna behålla sina tillsynssystem. En centraliserad modell för EU-tillsyn ger dock upphov till subsidiaritetsproblem.

*Med hänsyn till subsidiaritetsprincipen framstår **alternativ i** som det lämpligaste.*

7. MOTIVERING TILL EU-ÅTGÄRD, MERVÄRDE FÖR EU OCH SUBSIDIARITET

Den rättsliga grunden för lagstiftningsförslaget är i likhet med direktiv 1999/93/EG artikel 114 i EUF-fördraget om den inre marknaden, eftersom det syftar till att undanröja befintliga hinder för den inre marknads funktion genom att främja ömsesidigt erkännande och godtagande av e-identifiering, e-autentisering, e-signaturer och andra gränsöverskridande stödjande betrodda tjänster när sådana behövs för e-transaktioner.

Eftersom e-identifiering, e-autentisering, e-signaturer och stödjande betrodda tjänster är av en inneboende gränsöverskridande natur är en åtgärd på EU-nivå lämplig och proportionell för

att genomföra den digitala inre marknaden. Lagstiftningsåtgärder på medlemsstatsnivå kan inte förväntas ge samma resultat. En EU-åtgärd är därför nödvändig, lämplig och motiverad.

8. ÖVERVAKNING OCH UTVÄRDERING

Kommissionen kommer att övervaka lagstiftningens tillämpning genom kontinuerliga dialoger med berörda parter och insamling av statistiska uppgifter. Den kommer att rapportera till Europaparlamentet och rådet om konsekvenserna av den nya lagstiftningen senast fyra år efter dess ikraftträdande.