RAT DER EUROPÄISCHEN UNION

Brüssel, den 7. Juni 2012 (11.06)
(OR. en)

10977/12
ADD 1

Interinstitutionelles Dossier: 2012/0146 (COD)

TELECOM 122
MI 411
DATAPROTECT 73
CODEC 1576

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	5. Juni 2012
Empfänger:	der Generalsekretär des Rates der Europäischen Union, Herr Uwe CORSEPIUS
Nr. Komm.dok.:	SWD(2012) 136 final
Betr.:	ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG *Begleitunterlage zum* Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

Die Delegationen erhalten in der Anlage das Kommissionsdokument SWD(2012) 136 final.

Anl.: SWD(2012) 136 final

EUROPÄISCHE KOMMISSION

Brüssel, den 4.6.2012
SWD(2012) 136 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zum

Vorschlag für eine
VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

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

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zum

Vorschlag für eine
VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

1. POLITISCHER KONTEXT, VERFAHRENSFRAGEN UND KONSULTATION INTERESSIERTER KREISE

Die wirtschaftliche Entwicklung setzt Vertrauen in das Online-Umfeld voraus. Mangelndes Vertrauen führt dazu, dass Verbraucher, Unternehmen und Verwaltungen nur zögerlich elektronische Transaktionen durchführen oder neue Dienste einführen bzw. nutzen. Die vorgeschlagene Initiative zur Schaffung eines Rechtsrahmens soll sichere und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgern und Verwaltungen ermöglichen und dadurch die Effektivität öffentlicher und privater elektronischer Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels erhöhen.

Bestehende Hemmnisse für grenzüberschreitende elektronische Dienste müssen beseitigt werden. **Elektronische Identifizierung, Authentifizierung und Signaturen sowie einschlägige Vertrauensdienste** (eIAS) müssen EU-weit gegenseitig anerkannt und akzeptiert werden, damit sie produktiv wirken können und keine Hindernisse darstellen.

Bislang gibt es keinen umfassenden, grenz- und sektorenübergreifenden EU-Rahmen für eIAS-Dienste. Ein Rechtsrahmen besteht auf EU-Ebene nur für elektronische Signaturen, jedoch weder für die elektronische Identifizierung und Authentifizierung, noch für einschlägige Vertrauensdienste. Die Kommission kündigte in der *Digitalen Agenda für Europa* an, dass sie Rechtsvorschriften im Bereich der e-Signaturen sowie zur gegenseitigen Anerkennung der elektronischen Identifizierung (eID) und der elektronischen Authentifizierung vorschlagen würde, um die Fragmentierung und den Mangel an Interoperabilität zu beseitigen, die digitale Bürgerschaft zu stärken und der Cyberkriminalität vorzubeugen.

Im Hinblick auf die Durchführung der vorliegenden Folgenabschätzung holte die Kommission Stellungnahmen aus den Mitgliedstaaten, dem Europäischen Parlament und von den Akteuren im Zuge von Diskussionen, Seminaren und Konferenzen ein. Außerdem wurden zum Thema eIAS mehrere Studien in Auftrag gegeben, und die Fachliteratur wurde ausgewertet. Im Jahr 2011 fand eine öffentliche Konsultation statt, um Meinungsäußerungen dazu einzuholen, wie elektronische Identifizierung, Authentifizierung und Signaturen zum Binnenmarkt beitragen könnten. Ergänzt wurde die Konsultation durch eine gezielte Umfrage zur Erfassung der besonderen Ansichten und Bedürfnisse der KMU.

2. PROBLEMSTELLUNG

Bei der grenzüberschreitenden Nutzung von eIAS-Diensten können Benutzer auf verschiedene Schwierigkeiten stoßen. Folgende Haupthindernisse stehen sicheren und nahtlosen grenzüberschreitenden eIAS-Diensten entgegen:

1 – Marktfragmentierung: Für Dienstleister gelten unterschiedliche Vorschriften je nachdem, welchen Mitgliedstaat sie bedienen.

E-Signaturen: Die durch die e-Signatur-Richtlinie 1999/93/EG erreichte Harmonisierung ist unzulänglich. Vier Probleme wurden festgestellt: abweichende Umsetzung auf nationaler Ebene aufgrund unterschiedlicher Auslegung der Richtlinie durch die Mitgliedstaaten, De-facto-Inanspruchnahme von Ausnahmeregelungen für Anwendungen des öffentlichen Sektors, veraltete Normen und unklare Aufsichtsverpflichtungen, die zu Problemen bei der grenzübergreifenden Interoperabilität führen, sowie eine segmentierte EU-Landschaft und Verzerrungen im Binnenmarkt.

Elektronische Identifizierung: Unterschiedliche technische Lösungen für die persönliche Identifizierung in einzelnen Mitgliedstaaten, mangelnde Rechtssicherheit bei der grenzüberschreitenden elektronischen Identifizierung und die unklare Haftung für die Richtigkeit von Identitätsdaten führen allesamt zu Interoperabilitätsproblemen.

Einschlägige Vertrauensdienste: Das Fehlen eines EU-Rechtsrahmens führt dazu, dass in einigen Mitgliedstaaten für einige dieser Dienste nationale Vorschriften erlassen werden und dass Dienstleistern, die ihre Dienste in mehreren Mitgliedstaaten erbringen möchten, hohe Kosten entstehen. Beides führt zu Hindernissen im Binnenmarkt und zur Fragmentierung.

2 – Mangelndes Vertrauen: Durch mangelndes Vertrauen in elektronische Systeme, in die zur Verfügung stehenden Werkzeuge und in den rechtlichen Rahmen kann der Eindruck entstehen, dass auf diesem Gebiet weniger Schutzvorkehrungen bestehen als bei einer physischen Interaktion.

E-Signaturen: nationale Aufsichtsanforderungen unterscheiden sich qualitativ von einem Mitgliedstaat zum anderen, was es für Beteiligte, die sich auf eine e-Signatur verlassen müssen, schwierig macht, die Beaufsichtigung eines Dienstleisters einzuschätzen.

Elektronische Identifizierung und einschlägige Vertrauensdienste: uneinheitliche nationale Rechtsvorschriften erschweren es den Benutzern, sich bei grenzüberschreitenden Online-Vorgängen sicher zu fühlen.

Die vier Hauptgründe für diese Probleme sind:

A: Unzureichender Anwendungsbereich des derzeitigen Rechtsrahmens

eIAS-Dienste bilden die Voraussetzung für ein breites Spektrum interaktiver elektronischer Vorgänge wie z. B. elektronische Bankgeschäfte (*e*Banking), elektronische Behördendienste (*e*Government) oder elektronische Gesundheitsdienste (*e*Health). Auf EU-Ebene besteht allerdings nur ein begrenzter und unzulänglicher Rechtsrahmen, in dessen Mittelpunkt vor allem elektronische Signaturen stehen. Dagegen gibt es keinen besonderen Rahmen für die gegenseitige Anerkennung und Akzeptierung der eID oder einschlägiger Vertrauensdienste wie Zeitstempel oder elektronischer Siegel.

B: Mangelnde Koordinierung zwischen e-Signatur- und eID-Entwicklung

Nationale eIAS-Infrastrukturen wurden unabhängig voneinander und ohne jede Koordinierung auf EU-Ebene entwickelt. Das sich daraus ergebende Fehlen jeglicher grenzübergreifenden Interoperabilität der technischen Lösungen ist ein Hindernis für elektronische Transaktionen. Die fehlende gegenseitige Anerkennung und Akzeptierung ist einer der Gründe, warum sowohl Benutzer als auch Anbieter elektronischer Dienste die eIAS-Einführung eher skeptisch betrachten.

C: Mangelnde Transparenz bei den Sicherheitsgarantien

Starke und harmonisierte Sicherheitsvorkehrungen sind die Voraussetzung für das Entstehen vertrauenswürdiger Lösungen. Dies gilt insbesondere für den Zugang zu Diensten, die sensible personenbezogene Daten verarbeiten, z. B. zu elektronischen Gesundheitsdiensten. Nach Maßgabe der Richtlinie 1999/93/EG besteht Rechtssicherheit nur bei Verwendung elektronischer Signaturen, die bestimmte Sicherheitsgarantien bieten und ausreichend gegen Betrug und Fälschung geschützt sind (fortgeschrittene und qualifizierte elektronische Signaturen).

Das Fehlen eines sicheren eID-Systems wird von den Benutzern als großes Hindernis betrachtet. Mangels eines harmonisierten Rechtsrahmens für die elektronische Identifizierung ist es objektiv unmöglich, die Sicherheit und Verlässlichkeit amtlicher eIDs grenzüberschreitend festzustellen. Daraus erwachsen grenzbedingte Hindernisse, die einen Mangel an Vertrauen und eine Marktfragmentierung nach sich ziehen.

Ein weiteres Problemfeld ist der Identitätsdiebstahl. Sichere eIDs können dazu beitragen, dieses Risiko zu verringern. Im Gegenzug erleichtern schlecht gesicherte eIDs es Kriminellen, sich falsche oder beeinträchtigte eIDs zu beschaffen.

D: Mangelnde Bekanntheit und Akzeptanz seitens der Benutzer

Wegen der Komplexität der bei elektronischen Transaktionen eingesetzten Technik und der wichtigen Rolle, die vertrauenswürdige Dritte dabei spielen, entsteht ein Umfeld, in dem es schwierig ist, die Vertrauenswürdigkeit zu beurteilen. Vor allem Endnutzer, die im Allgemeinen keine ausreichenden Kenntnisse besitzen, müssen sich auf Regeln verlassen können, die eindeutige Rechte und Pflichten für alle Beteiligten festlegen (Vertrauensdiensteanbieter, Endnutzer und Behörden).

3. BASISSZENARIO

Das Basisszenario der Initiative ist der Verzicht auf jegliche neue Regulierung. Dabei wird davon ausgegangen, dass sich die bestehenden Probleme folgendermaßen weiterentwickeln:

Keine Lösung der Fragmentierungs- und Interoperabilitätsprobleme: Die Mitgliedstaaten würden die Richtlinie 1999/93/EG weiterhin anwenden und durchsetzen.

Keine Rechtssicherheit: Die Probleme, die aus der fehlenden gegenseitigen Anerkennung elektronischer Signaturen und dem Fehlen eines Rechtsrahmens für die gegenseitige Anerkennung und Akzeptierung der elektronischen Identifizierung und einschlägiger Vertrauensdienste erwachsen, würden die rechtliche Anerkennung zahlreicher interaktiver grenzüberschreitender Vorgänge verhindern.

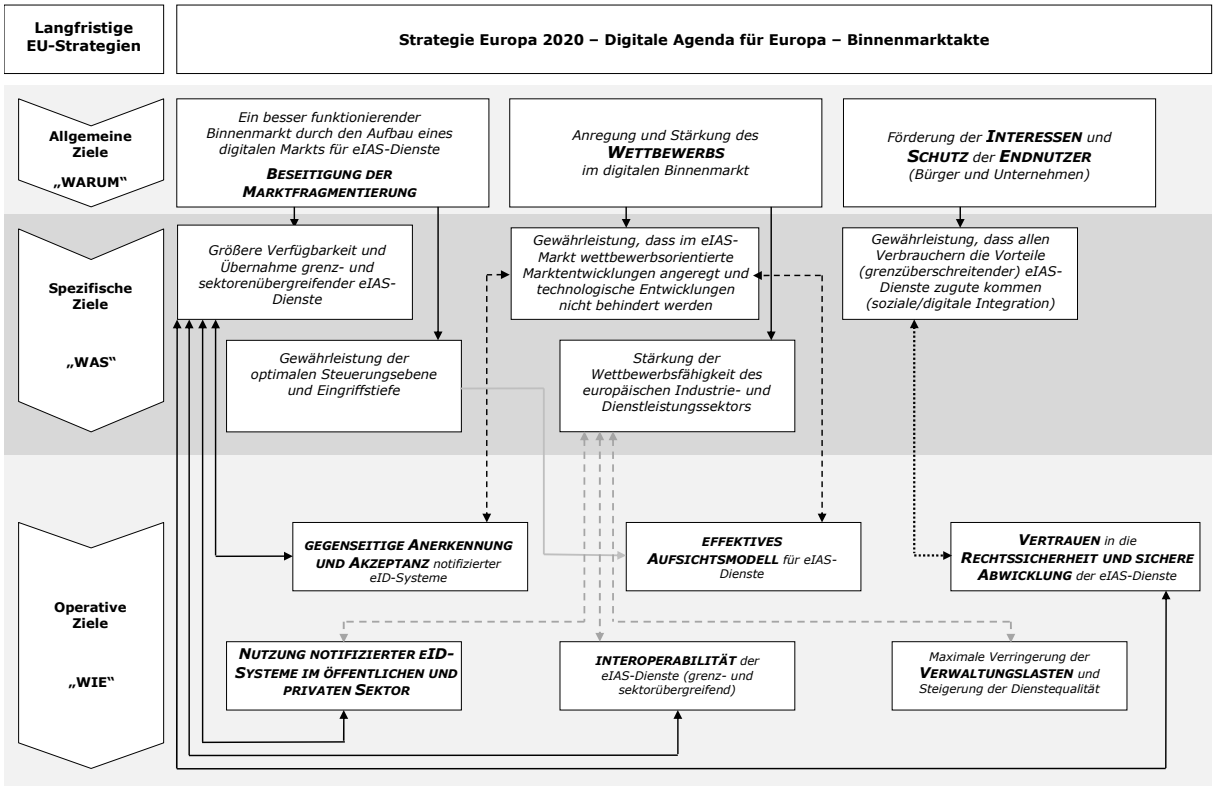
Keine Erfüllung der Benutzeranforderungen: Innerhalb des derzeitigen Rahmens ist es nicht möglich, die sich durch die technische Entwicklung eröffnenden Chancen voll zu nutzen.

Keine vollständige Nutzung der Vorteile wichtiger europäischer Initiativen: EU-Maßnahmen wie die Richtlinien über Dienstleistungen, öffentliche Aufträge oder die Mehrwertsteuer (elektronische Rechnungen), aber auch die Großpilotprojekte im Zuge des IKT-Förderprogramms (ICT-PSP)[1], mit denen die Probleme der Interoperabilität und der grenzübergreifenden Anerkennung in Bezug auf bestimmte elektronische Interaktionsarten beseitigt werden sollen, könnten nur auf Pilotprojektebene funktionieren, weil ein sektorenübergreifender rechtlicher Rahmen fehlt.

4. POLITISCHE ZIELE

Es wurden vier **allgemeine Ziele** festgelegt: Gewährleistung der Entwicklung eines digitalen Binnenmarkts; Förderung der Entwicklung wichtiger grenzüberschreitender öffentlicher Dienste; Anregung und Verstärkung des Wettbewerbs im Binnenmarkt; Verbesserung der Benutzerfreundlichkeit (Bürger und Unternehmen). Diese Ziele stehen im Einklang mit strategischen Grundsatzdokumenten der EU wie der *Strategie Europa 2020*, der *Digitalen Agenda für Europa*, der *Binnenmarktakte* und dem *Fahrplan für Stabilität und Wachstum*.

Die **spezifischen Ziele** enthalten die angestrebten Ergebnisse in Bezug auf den eIAS-Markt („*was*"), die mit der Verwirklichung der *operativen Ziele* („*wie*") erreicht werden sollen. Zu jedem spezifischen Ziel wurden mehrere **operative Ziele** festgelegt.



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

5. POLITIKOPTIONEN

Im Hinblick auf die Lösung der Probleme und die Verwirklichung der oben genannten Ziele wurden drei Aspekte untersucht: (1) Anwendungsbereich des vorgesehenen Rahmens, (2) Rechtsinstrument und (3) Aufsichtsebene:

- Zum ersten Aspekt „*Anwendungsbereich des Rahmens*“ wurden vier Optionen geprüft:

  Option 0: Aufhebung der Richtlinie 1999/93/EG und Verzicht auf jegliche Maßnahmen auf dem Gebiet der elektronischen Identifizierung oder einschlägiger Vertrauensdienste

  Diese Option umfasst die Beendigung aller EU-Tätigkeiten auf dem Gebiet der e-Signaturen. Die Richtlinie 1999/93/EG würde aufgehoben, und es würden keine Vorschriften für die gegenseitige Anerkennung der elektronischen Identifizierung vorgeschlagen.

- *Option 1: Keine Änderung (Basisszenario)*

  Die Richtlinie 1999/93/EG würde unverändert beibehalten. Es würden keine Vorschriften über die elektronische Identifizierung vorgeschlagen.

- *Option 2: Erhöhung der Rechtssicherheit, verstärkte Koordinierung der nationalen Beaufsichtigung und Gewährleistung der gegenseitigen Anerkennung und Akzeptierung der elektronischen Identifizierung*

  Der Anwendungsbereich der Richtlinie 1999/93/EG würde um Bestimmungen über die grenzübergreifende Anerkennung und Akzeptierung notifizierter eID-Systeme[2] erweitert. Die Bestimmungen der Richtlinie in Bezug auf elektronische Signaturen würden überarbeitet, um ihre derzeitigen Schwächen zu beseitigen und um die nationalen Aufsichtsmodelle besser zu harmonisieren.

- *Option 3: Erweiterung um bestimmte einschlägige Vertrauensdienste*

  Diese Option ist eine Erweiterung der Option 2, durch die einschlägige Vertrauensdienste und Anmeldedaten in den Anwendungsbereich des Vorschlags aufgenommen werden.

  Folgende wesentliche einschlägige Funktionsmerkmale wären in die Rechtsvorschriften aufzunehmen: elektronische Zeitstempel, elektronische Siegel, Langzeitbewahrung von Informationen, bescheinigte elektronische Dokumentenzustellung, Zulässigkeit elektronischer Dokumente und Website-Authentifizierung.

---

[2] „Notifizierte eID“: Ein eID-System, das der Kommission von einem Mitgliedstaat zwecks grenzübergreifender Anerkennung und Akzeptierung gemeldet wurde. Der Begriff der notifizierten eID ist nicht auf von öffentlichen Stellen ausgestellte eIDs beschränkt. Die Mitgliedstaaten können auch vom Privatsektor ausgestellte eIDs notifizieren, die sie für die Verwendung im eigenen öffentlichen Dienst anerkennen. Dies ist notwendig, weil nicht in allen Mitgliedstaaten solche eIDs von Behörden ausgestellt werden. Aufgrund des sektorübergreifenden Konzepts der Vorschriften könnte der Privatsektor bei Notwendigkeit einer sicheren elektronischen Identifizierung die Verwendung notifizierter eIDs in elektronische Dienste integrieren.

- Zum zweiten Aspekt „Rechtsinstrument“, wurden vier Optionen geprüft:

  Entweder eine umfassende Rechtsvorschrift (Option A) oder zwei getrennte Vorschriften (Option B)

  Die Rechtssetzungsmaßnahme könnte entweder aus einer einzigen umfassenden Rechtsvorschrift für elektronische Identifizierung, Authentifizierung und Signaturen bestehen oder aber aus zwei Rechtsakten, nämlich einem Beschluss der Kommission über die eID und einer Neufassung der e-Signatur-Richtlinie.

  Richtlinie (Option C) oder Verordnung (Option D):

  Die Vorschriften können als Richtlinie oder als Verordnung erlassen werden.

- Zum dritten Aspekt „Beaufsichtigung“ wurden zwei Optionen geprüft:

  Option i): Beibehaltung der nationalen Aufsichtssysteme

  Die bestehenden einzelstaatlichen Aufsichtssysteme würden beibehalten, allerdings mit einer verstärkten Harmonisierung anhand gemeinsamer Grundanforderungen.

  Option ii): Schaffung eines EU-Aufsichtssystems

  Ein EU-Aufsichtssystem würde eingerichtet, um Unterschiede zwischen den nationalen Aufsichtsregelungen zu beseitigen oder zu verringern. Dafür gibt es zwei Möglichkeiten:

  Unteroption a: Ersetzung der bestehenden nationalen Aufsichtssysteme durch ein einziges EU-Aufsichtssystem mit einer einzigen EU-Aufsichtsbehörde;

  Unteroption b: Einrichtung eines EU-Aufsichtssystems mit einer Aufsichtsbehörde unter Beibehaltung paralleler nationaler Aufsichtssysteme (jeder Mitgliedstaat könnte entweder sein eigenes oder das europäische System wählen).

6. VERGLEICH DER POLITIKOPTIONEN UND DER AUSWIRKUNGEN

Die Politikoptionen wurden geprüft und im Hinblick auf Effektivität, Effizienz und Kohärenz mit dem Basisszenario (Option 1) verglichen.

6.1. Anwendungsbereich des Rahmens

Option 0 würde nicht dazu beitragen, die in der Folgenabschätzung festgelegten Ziele zu erreichen. Sie würde die Verfügbarkeit und Übernahme von grenz- und sektorübergreifenden eIAS-Diensten nicht erhöhen, keine optimale Verwaltungsebene gewährleisten, die Entwicklung der Märkte nicht fördern, die Wettbewerbsfähigkeit der europäischen Industrie- und Dienstleistungssektoren nicht stärken helfen und auch nicht gewährleisten, dass alle Endnutzer in den Genuss der Vorteile von eIAS-Diensten kommen. Ganz im Gegenteil würde diese Option die technologische Entwicklung im eIAS-Markt behindern, die laufende Schaffung der Grundlagen für grenzüberschreitende e-Dienste stören sowie die Fragmentierung des EU-Markts und ein ungleiches Vertrauensumfeld zementieren.

Option 1 würde es nicht erlauben, die Ziele zu erreichen. Sie würde die bestehenden Unklarheiten nicht beseitigen. Das Vertrauensumfeld bezüglich der Beaufsichtigung bliebe uneinheitlich. Regulatorische Unsicherheiten würden bestehen bleiben, und ein segmentiertes EU-Umfeld würde fortgeschrieben, was zu ungleichen Wettbewerbsbedingungen im Binnenmarkt führen und unterschiedliche Vorgehensweisen auf nationaler Ebene wahrscheinlicher machen dürfte.

Option 2 würde die Rechtssicherheit erhöhen, die Aufsicht verbessern und die gegenseitige Anerkennung und Akzeptierung der eIDs sicherstellen. Sie würde beträchtlich zur Verwirklichung aller in der Folgenabschätzung festgelegten Ziele beitragen und positive wirtschaftliche, soziale und umweltpolitische Ergebnisse hervorbringen.

eIAS-Dienste wären attraktiver, und Investitionen in eIAS-Infrastrukturen und -dienste würden höhere Renditen ermöglichen. Außerdem stände eIAS für alle Sektoren und alle Arten von Unternehmen zur Verfügung, während Hindernisse an den Grenzen entfielen. Es würden sich neue Märkte und neue Investitionen ergeben, wodurch die Innovation angeregt würde.

Die derzeitige Marktfragmentierung würde verringert, weil durch die mögliche Bezugnahme auf technische Normen die grenzübergreifende Interoperabilität verbessert würde.

Die gegenseitige Anerkennung und Akzeptierung von eIDs würde weiter dazu beitragen, die bestehenden Schranken im Binnenmarkt abzubauen. Schließlich würde die einheitliche Beaufsichtigung, die sich aus gemeinsamen Grundanforderungen ergibt, wahrscheinlich das Vertrauen erhöhen, die Aufdeckung von Betrugsfällen erleichtern und zur Verhinderung von Identitätsdiebstahl beitragen.

Option 3 würde eIAS-Dienste mit der Ausweitung des Rahmens auf bestimmte wesentliche einschlägige Vertrauensdienste noch attraktiver machen und dadurch ihre positiven Auswirkungen weiter steigern.

Option 3 *eignet sich wahrscheinlich besser als die Optionen 0, 1 und 2 zur Herbeiführung spürbarer Auswirkungen auf die Sicherheit und Benutzerfreundlichkeit elektronischer Transaktionen.*

6.2. Rechtsinstrument

Durch die Schaffung eines umfassenden Rahmens innerhalb **eines Rechtsinstruments** würde sichergestellt, dass die Vorschriften zur Regulierung der verschiedenen eIAS-Aspekte perfekt aufeinander abgestimmt sind. Bei **zwei getrennten Instrumenten** könnte es zu Abweichungen in den rechtlichen Bestimmungen, die für elektronische Signaturen und die elektronische Identifizierung erlassen werden, sowie – was noch schwerer wiegt – in der Gesamtkonzeption der Initiativen kommen.

Der Erlass einer **Richtlinie** würde nicht helfen, die gegenwärtigen Interoperabilitätsprobleme bei elektronischen Signaturen zu lösen, die auf eine abweichende Umsetzung der Richtlinie 1999/93/EG zurückgehen. Eine **Verordnung** erlangt unmittelbare Geltung ohne weitere Auslegung und bringt daher eine größere Harmonisierung. Deshalb ist sie besser geeignet, um die Ziele der vorgeschlagenen Rechtsvorschriften zu erreichen.

Der Erlass einer einzigen Verordnung erscheint als der effektivste Weg zur Erreichung der angestrebten Ziele.

6.3. Aufsichtsebene

Bei **Option i** würden die neuen Vorschriften das bestehende nationale Aufsichtssystem beibehalten und gemeinsame Grundanforderungen an Diensteanbieter vorschreiben. Ein harmonisierter Ansatz auf EU-Ebene sowohl für elektronische Signaturen als auch für einschlägige Vertrauensdienste würde die Aufsicht effektiver machen, die Rechtssicherheit verbessern sowie das Vertrauen und die Sicherheit elektronischer Transaktionen erhöhen.

Option ii würde eine einheitliche, effiziente und hochwertige Aufsicht durch die EU garantieren. Die **Unteroption b** hat den Vorteil der größeren Flexibilität als bei einer zentralen EU-Aufsichtsbehörde, wie sie in **Unteroption a** vorgesehenen ist, denn sie böte für Mitgliedstaaten, in denen es keine oder nur wenige Vertrauensdiensteanbieter gibt, den Vorteil, dass diese ihre Aufsichtspflichten auf eine EU-Aufsichtsbehörde übertragen könnten. Andere Mitgliedstaaten könnten, wenn sie dies wünschen, ihr eigenes Aufsichtssystem beibehalten. Ein zentralisiertes EU-Aufsichtsmodell wirft jedoch Subsidiaritätsfragen auf.

*Im Hinblick auf die Wahrung des Subsidiaritätsprinzips dürfte die **Option i** am besten geeignet sein.*

7. GRÜNDE FÜR EU-MAßNAHMEN, MEHRWERT AUF EU-EBENE UND SUBSIDIARITÄT

Wie bei der Richtlinie 1999/93/EG ist die Rechtsgrundlage für den Legislativvorschlag der Binnenmarktartikel 114 AEUV, denn er dient der Beseitigung bestehender Hindernisse für das Funktionieren des Binnenmarkts, indem er die gegenseitige Anerkennung und Akzeptierung der elektronischen Identifizierung, Authentifizierung und Signaturen sowie einschlägiger Vertrauensdienste fördert, soweit diese für grenzüberschreitende elektronische Transaktionen benötigt werden.

Da eIAS-Dienste von Natur aus nicht-territorial sind, ist ein Vorgehen auf EU-Ebene zur Verwirklichung des digitalen Binnenmarkts angemessen und verhältnismäßig. Das gleiche Ergebnis kann mit auf der Ebene der Mitgliedstaaten getroffenen Regulierungsmaßnahmen voraussichtlich nicht erzielt werden. Ein Eingreifen der EU ist daher erforderlich, angemessen und gerechtfertigt.

8. ÜBERWACHUNG UND BEWERTUNG

Die Kommission würde die Anwendung der Rechtsvorschriften im ständigen Dialog mit den Beteiligten und durch Erfassung von Statistiken überwachen und dem Europäischen Parlament und dem Rat über die Folgen der neuen Vorschriften vier Jahre nach deren Inkrafttreten Bericht erstatten.