COMMISSION EUROPÉENNE

Bruxelles, le 4.6.2012
SWD(2012) 136 final

**DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION**

**RÉSUMÉ DE L'ANALYSE D'IMPACT**

***accompagnant la***

**proposition de**
**RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.**

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

**DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION**

**RÉSUMÉ DE L'ANALYSE D'IMPACT**

***accompagnant la***

**proposition de**
**RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.**

## 1. CONTEXTE POLITIQUE, QUESTIONS DE PROCEDURE ET CONSULTATION DES PARTIES INTERESSEES

Instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique. En effet, si les consommateurs, les entreprises et les administrations n'ont pas confiance, ils hésiteront à effectuer des transactions par voie électronique et à adopter de nouveaux services. Le cadre réglementaire proposé vise à permettre des interactions électroniques sûres et sans discontinuité entre les entreprises, les particuliers et les pouvoirs publics et à accroître ainsi l'efficacité des services électroniques publics et privés ainsi que de l'activité économique et du commerce électroniques.

Les services électroniques transnationaux sont entravés par des obstacles qu'il faut éliminer. Pour constituer des stimulants et non des obstacles**, l'identification, l'authentification et les signatures électroniques ainsi que les services de confiance associés (services eIAS)** doivent donc faire l'objet d'une reconnaissance et d'une acceptation mutuelles dans toute l'UE.

L'UE ne dispose encore d'aucun cadre transnational et intersectoriel complet pour les services eIAS. Au niveau de l'UE, il existe uniquement un cadre juridique pour les signatures électroniques, mais pas pour l'identification et l'authentification électroniques ni pour les services de confiance associés. Dans la *stratégie numérique pour l'Europe*, la Commission a annoncé qu'elle proposerait des mesures législatives relatives aux signatures électroniques et à la reconnaissance mutuelle de l'identification et de l'authentification électroniques, afin de remédier à la fragmentation et au manque d'interopérabilité, de développer la citoyenneté numérique et de prévenir la cybercriminalité.

Pour effectuer la présente analyse d'impact, la Commission a recueilli des informations auprès des États membres, du Parlement européen et des parties intéressées dans le cadre de débats, d'ateliers et de conférences. Un certain nombre d'études relatives aux eIAS ont été entreprises et la littérature a été étudiée. Une consultation publique visant à fournir des éléments d'information sur la façon dont l'identification, l'authentification et les signatures électroniques peuvent contribuer au marché unique a été lancée en 2011. La consultation a été complétée par une enquête ciblée destinée à rendre compte des avis et des besoins spécifiques des PME.

## 2. DEFINITION DU PROBLEME

L'utilisation transnationale des services eIAS peut poser des problèmes aux utilisateurs. Les principaux obstacles qui entravent le fonctionnement sûr et sans discontinuité des eIAS sont les suivants:

1.- **la fragmentation du marché**: les prestataires de services sont soumis à des règles différentes en fonction des États membres qu'ils desservent.

En ce qui concerne les signatures électroniques, le niveau d'harmonisation apporté par la directive 1999/93/CE est insuffisant. Quatre types de problèmes ont été recensés: des divergences dans la mise en œuvre au niveau national dues à des différences d'interprétation de la directive par les États membres, le recours de fait à une dérogation pour les applications du secteur public, des normes dépassées et des obligations mal définies en matière de contrôle donnant lieu à des problèmes d'interopérabilité transnationale, à une situation fragmentée dans l'UE et à des distorsions dans le marché intérieur.

Dans le domaine de l'identification électronique, l'existence de solutions technologiques différentes selon les États membres pour l'identification personnelle, le manque de sécurité juridique en ce qui concerne l'utilisation transnationale des identifications électroniques et l'absence de responsabilité clairement définie pour ce qui est de l'exactitude des données d'identité sont tous à l'origine de problèmes d'interopérabilité.

Enfin, dans le cas des services de confiance associés, en raison de l'absence de cadre juridique dans l'UE, certains États membres ont adopté des législations nationales pour certains de ces services et les prestataires souhaitant proposer leurs services dans plusieurs États membres doivent faire face à des coûts élevés. Il en résulte, dans un cas comme dans l'autre, des entraves au marché intérieur et une certaine fragmentation.

**2 – le manque de confiance**: le manque de confiance dans les systèmes électroniques, dans les outils fournis et dans le cadre juridique peut donner l'impression que les garanties juridiques sont moindres que dans le cas d'une interaction physique.

Pour les signatures électroniques, les exigences nationales en matière de contrôle sont, sur le plan de la qualité, différentes d'un État membre à l'autre. De ce fait, il est difficile, pour les parties qui se fient aux signatures électroniques, d'évaluer la manière dont un prestataire de service est contrôlé.

Pour l'identification électronique et les services de confiance associés, la disparité des législations nationales empêche les utilisateurs d'agir en toute confiance lorsqu'ils effectuent des transactions transnationales en ligne.

**Les quatre principales causes de ces problèmes sont les suivantes:**

*A: Un cadre juridique actuel insuffisamment développé*

L'existence de services eIAS est une condition indispensable à la mise en place d'une grande variété de services d'interaction électroniques tels que les services bancaires en ligne, l'administration en ligne ou la santé en ligne. Au niveau de l'UE, le cadre réglementaire existant, qui porte essentiellement sur les signatures électroniques, est limité et incomplet. Il n'existe pas de cadre spécifique applicable à la reconnaissance et à l'acceptation mutuelles des identifications électroniques ou aux services de confiance associés, tels que l'horodatage ou les cachets électroniques.

*B: Un manque de coordination dans le développement des signatures et de l'identification électroniques*

Les infrastructures nationales d'eIAS ont été mises au point sans coordination au niveau de l'UE. L'absence d'interopérabilité transnationale des solutions techniques qui en résulte crée des entraves aux transactions électroniques. L'absence de reconnaissance et d'acceptation mutuelles est l'une des raisons du scepticisme des utilisateurs comme des prestataires de services électroniques à l'égard du déploiement des eIAS.

*C: Le manque de transparence des garanties de sécurité*

L'adoption de mesures de sécurité harmonisées d'un niveau élevé est essentielle à la création de solutions dignes de confiance. Cet aspect est particulièrement pertinent pour ce qui est de l'accès aux services qui font appel à des données personnelles sensibles, tels que les services de santé en ligne. La directive 99/93/CE reconnaît que seules peuvent être considérées comme juridiquement sûres les signatures électroniques dont la sécurité est garantie, c'est-à-dire celles qui sont suffisamment protégées contre toute falsification ou fraude (signatures électroniques avancées et qualifiées).

Les utilisateurs considèrent que le manque de systèmes d'identification électroniques sécurisés constitue un obstacle considérable. L'absence de cadre juridique harmonisé dans le domaine de l'identification électronique signifie qu'il est impossible de déterminer objectivement le niveau de sécurité et de fiabilité d'identifications électroniques officielles dans le cas d'une interaction transnationale. Cette situation crée des entraves aux interactions transnationales, ce qui nuit à la confiance et entraîne une fragmentation du marché.

Le vol d'identité fait aussi partie des préoccupations. Les systèmes d'identification électronique sécurisés peuvent contribuer à limiter ce risque. À l'inverse, des systèmes d'identification électronique insuffisamment sécurisés peuvent faciliter la tâche aux criminels en leur permettant de se servir d'identifications électroniques falsifiées ou compromises.

*D: Le manque de sensibilisation/d'adhésion des utilisateurs*

La complexité des technologies utilisées pour les transactions électroniques et le rôle clé joué par les tiers de confiance créent un environnement dans lequel il est difficile d'évaluer la confiance. En particulier, les utilisateurs finaux, qui ne disposent généralement pas de l'expertise suffisante, doivent pouvoir compter sur des règles établissant clairement les droits et responsabilités de toutes les parties concernées (prestataires de service de confiance, utilisateurs finaux et organismes de gouvernance).

## 3. SCENARIO DE BASE

Le scénario de base est l'absence de toute nouvelle intervention réglementaire. Dans un scénario de ce type, il est prévu que la situation actuelle évoluerait comme suit:

Les problèmes de fragmentation et d'interopérabilité ne seraient pas résolus. Il est probable que les États membres continueraient à mettre en œuvre et à appliquer la directive 99/93/CE.

La sécurité juridique ne serait pas garantie: les problèmes dus à l'absence de reconnaissance mutuelle des signatures électroniques et de cadre juridique régissant la reconnaissance et l'acceptation mutuelles des systèmes d'identification électroniques et des services de confiance associés empêcheraient la reconnaissance d'une série d'interactions transnationales.

Les besoins des utilisateurs ne seraient pas entièrement satisfaits: le cadre actuel ne permet pas de profiter pleinement des possibilités offertes par les progrès de la technologie.

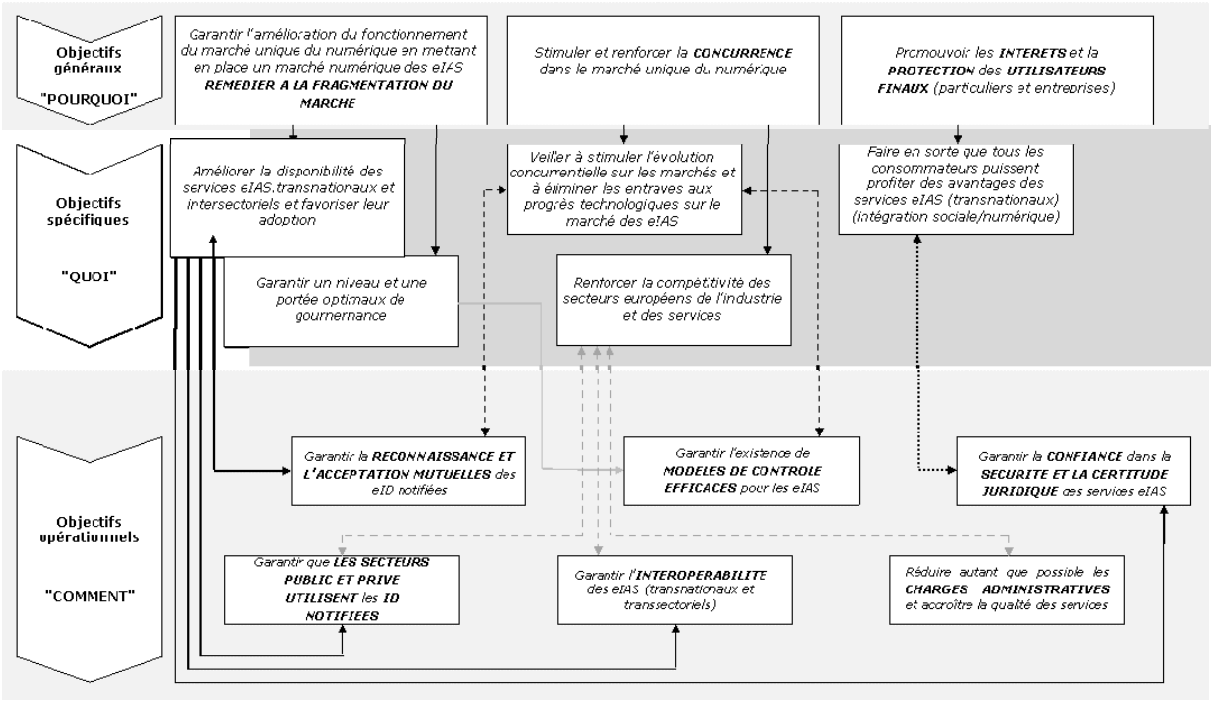
L'effet de levier des grandes initiatives européennes ne serait pas pleinement exploité: certaines politiques européennes mises en œuvre par les directives sur les services, sur les marchés publics ou sur la TVA (factures électroniques), ou les projets pilotes à grande échelle

du programme d'appui stratégique en matière de TIC[1] qui vise à éliminer les problèmes d'interopérabilité et de reconnaissance transnationale liés à certains types d'interactions électroniques ne pourraient fonctionner qu'à l'échelle expérimentale en l'absence d'un cadre législatif intersectoriel.

## 4. OBJECTIFS POLITIQUES

Les **objectifs généraux** définis sont au nombre de quatre: il s'agit de garantir la mise en place d'un marché unique du numérique, de promouvoir le développement de services publics transnationaux essentiels, de stimuler et de renforcer la concurrence dans le marché unique et d'accroître la convivialité (particuliers et entreprises). Ces objectifs sont conformes aux politiques stratégiques de l'UE telles que la *stratégie Europe 2020*, la *stratégie numérique pour l'Europe*, l'*acte pour le marché unique* et la *feuille de route pour la stabilité et la croissance.*

Des **objectifs spécifiques** ont été définis pour exprimer les résultats escomptés de la mise en place des objectifs opérationnels («comment») en ce qui concerne le marché des eIAS («quoi»). Un certain nombre **d'objectifs opérationnels** ont été recensés pour chaque objectif spécifique.




## 5. OPTIONS ENVISAGEABLES

Trois catégories d'options ont été évaluées pour résoudre ces problèmes et atteindre les objectifs précités: (1) portée du cadre envisagé, (2) instrument juridique et (3) niveau de contrôle.

- Dans la première catégorie «*Portée du cadre*», quatre options ont été examinées:

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

Option 0 Abrogation de la directive 99/93/CE et absence d'intervention réglementaire en ce qui concerne l'identification électronique ou les services de confiance associés.

Cette option prévoit l'arrêt de toutes les activités de l'UE dans le domaine des signatures électroniques. La directive 99/93/CE serait abrogée et aucune mesure législative ne serait proposée en ce qui concerne la reconnaissance mutuelle de l'identification électronique.

- Option 1 Pas de changements stratégiques (scénario de base)

  La directive 99/93/CE ne serait pas modifiée. Aucune mesure législative concernant l'identification électronique ne serait proposée.

- *Option 2 Accroître la sécurité juridique, mieux coordonner les mesures nationales de contrôle et assurer la reconnaissance et l'acceptation mutuelles de l'identification électronique*.

  La portée de la directive 99/93/CE serait étendue par l'ajout de dispositions relatives à la reconnaissance et à l'acceptation transnationales des systèmes d'identification électronique notifiés[2]. Les dispositions de la directive relatives aux signatures électroniques seraient revues pour remédier à la faiblesse actuelle de la directive en la matière et pour mieux harmoniser les modèles nationaux de contrôle.

- *Option 3 Extension à certains services de confiance associés*

  Cette option constituerait un prolongement de l'option 2 et inclurait les services de confiance associés et les informations d'identification dans le champ d'application de la proposition.

  Les services associés essentiels qui seraient couverts par la législation seraient les services d'horodatage, les cachets électroniques, la conservation à long terme des informations, la fourniture de documents électroniques certifiée, la recevabilité des documents électroniques et l'authentification des sites web.

- Dans la deuxième catégorie, qui concerne un «instrument juridique», quatre options ont été examinées:

  *Un seul instrument législatif complet (option A) ou deux instruments distincts (option B)*

  La législation pourrait prendre la forme d'une seule mesure couvrant à la fois l'identification, l'authentification et les signatures électroniques ou de deux

[2] Les systèmes d'identification électronique notifiés sont des systèmes notifiés par un État membre à la Commission afin d'être reconnus et acceptés dans tous les États membres. Le concept de systèmes d'identification électronique notifiés ne concerne pas uniquement les identifications électroniques délivrées par le secteur public: les États membres pourraient aussi notifier des identifications électroniques délivrées par le secteur privé et dont ils autorisent l'usage dans leurs propres services publics. Cette approche est nécessaire parce que toutes les autorités des États membres ne délivrent pas forcément d'identifications électroniques. L'approche intersectorielle de la législation permettrait au secteur privé d'intégrer l'utilisation des identifications électroniques notifiées dans les services électroniques où une identification électronique sécurisée est nécessaire.

instruments, à savoir une décision de la Commission sur l'identification électronique et une révision de la directive sur les signatures électroniques.

*Directive (option C) ou règlement (option D):*

La mesure législative pourrait être une directive ou un règlement.

- Dans la troisième catégorie, le *contrôle*, deux options sont envisagées:

*Option i): Maintien des systèmes de contrôle nationaux*

Les systèmes de contrôle nationaux existants seraient maintenus mais leur harmonisation serait plus poussée grâce à des exigences essentielles communes.

**Option ii) Mise en place d'un système de contrôle à l'échelle de l'UE**

Un système de contrôle à l'échelle de l'UE serait mis en place pour réduire ou éliminer les disparités entre les systèmes de contrôle nationaux. Il pourrait prendre l'une des deux formes suivantes:

*Sous-option a:* remplacement des systèmes de contrôle nationaux existants par un système et un organe de contrôle uniques à l'échelle de l'UE.

*Sous-option b:* établissement d'un système et d'un organe de contrôle à l'échelle de l'UE tout en maintenant des systèmes nationaux de contrôle en parallèle (chaque État membre pourrait alors opter soit pour son propre système, soit pour le système européen).

## 6. COMPARAISON DES OPTIONS ET DE LEURS IMPACTS

Les options stratégiques ont été évaluées et comparées au scénario de base (option 1) au regard des critères d'efficacité, d'efficience et de cohérence.

### 6.1. Portée du cadre

L'**option 0** ne permettrait pas d'atteindre les objectifs décrits dans le rapport sur l'analyse d'impact. Elle ne permettrait pas d'améliorer la disponibilité des services eIAS transnationaux et intersectoriels et de favoriser leur adoption, de garantir un niveau et une portée optimaux de gouvernance, de stimuler l'évolution des marchés, de renforcer la compétitivité des secteurs européens de l'industrie et des services ou de faire en sorte que tous les consommateurs puissent profiter des avantages des services eIAS. Au contraire, elle entraverait la réalisation de progrès technologiques sur le marché des eIAS, interromprait le processus actuel d'évolution vers la mise en place de services électroniques transnationaux et contribuerait à perpétuer un marché de l'UE fragmenté et une situation contrastée pour ce qui est du climat de confiance.

L'**option 1** ne permettrait pas d'atteindre les objectifs. Elle perpétuerait les ambiguïtés existantes et les niveaux de confiance en ce qui concerne le contrôle resteraient inégaux. Sur le plan réglementaire, l'incertitude persisterait et la fragmentation se poursuivrait dans l'UE, ce qui fausserait la concurrence sur le marché intérieur et augmenterait la probabilité d'approches divergentes au niveau national.

L'**option 2** accroîtrait la sécurité juridique, améliorerait le contrôle et assurerait la reconnaissance et l'acceptation mutuelles de l'identification électronique. Elle contribuerait notablement à la réalisation de chacun des objectifs recensés dans le rapport sur l'analyse d'impact en donnant des résultats positifs sur les plans économique, social et environnemental.

Les services eIAS paraîtraient plus attrayants, ce qui accroîtrait le retour sur les investissements réalisés dans les infrastructures et services eIAS. Les eIAS deviendraient également disponibles pour tous les secteurs et tous les types d'entreprises et les entraves aux frontières seraient éliminées. De nouveaux marchés et de nouveaux investissements seraient alors ouverts, ce qui stimulerait l'innovation.

La fragmentation actuelle du marché diminuerait du fait de l'amélioration de l'interopérabilité transnationale par le recours à des références aux normes techniques.

La reconnaissance et l'acceptation mutuelles de l'identification électronique contribueraient à faire disparaître les entraves actuelles au marché unique. Enfin, il est probable que les exigences essentielles communes favoriseraient un contrôle plus homogène, qui améliorerait le climat de confiance, faciliterait la détection des fraudes et permettrait de prévenir le vol d'identité.

**L'option 3** rendrait les services eIAS encore plus attrayants et amplifierait leur impact positif car elle élargirait le champ d'application du cadre à certains services de confiance associés essentiels.

*L'**option 3** est jugée plus susceptible d'avoir une incidence notable sur les transactions électroniques sécurisées et simples d'utilisation que l'option 0, 1 ou 2.*

### 6.2. Instrument juridique

Le recours à **un seul instrument** pour établir un cadre complet garantirait la cohérence des mesures législatives concernant les différents aspects des eIAS. L'existence de **deux instruments distincts** pourrait être à l'origine de disparités dans les dispositions juridiques adoptées pour les signatures et l'identification électroniques et, surtout dans l'approche des initiatives.

L'adoption d'une **directive** ne permettrait pas de résoudre les problèmes actuels d'interopérabilité dans le domaine des signatures électroniques, dus à des divergences dans la transposition de la directive 99/93/CE. En revanche, un **règlement,** qui est directement applicable sans interprétation, garantit une meilleure harmonisation et est par conséquent plus approprié pour atteindre les objectifs de la législation proposée.

*L'adoption d'un règlement unique semble être le moyen le plus approprié de réaliser les objectifs.*

### 6.3. Niveau de contrôle

**L'option i** prévoit le maintien des systèmes de contrôle nationaux existants et l'imposition aux prestataires de services d'exigences essentielles communes. L'adoption, au niveau de l'UE, d'une approche harmonisée pour les signatures électroniques comme pour les services de confiance associés accroîtrait l'efficacité du système de contrôle et renforcerait la sécurité juridique ainsi que la sécurité des transactions électroniques et la confiance qu'elles inspirent.

L'**option ii** permettrait de garantir l'existence d'un système de contrôle homogène, efficace et de qualité dans toute l'UE. La **sous-option b** offre davantage de souplesse que l'organe de

contrôle unique à l'échelle de l'UE prévu par la **sous-option a**: il pourrait se révéler avantageux, pour les États membres dans lesquels les prestataires de services de confiance sont rares ou inexistants, de transférer les tâches de contrôle à un organe de contrôle de l'UE. D'autres États membres pourraient, s'ils le souhaitent, maintenir leur système de contrôle. Toutefois, l'existence d'un modèle de contrôle centralisé au niveau de l'UE suscite des préoccupations en ce qui concerne la subsidiarité.

*Il semblerait, compte tenu du principe de subsidiarité, que l'option la plus appropriée soit* ***l'option i****.*

## 7. JUSTIFICATION DE L'ACTION DE L'UE, VALEUR AJOUTEE ET SUBSIDIARITE

Comme dans le cas de la directive 99/93/CE, la base juridique retenue pour la proposition législative est l'article 114 du TFUE sur le marché intérieur car la mesure vise à éliminer les entraves au fonctionnement du marché intérieur en encourageant la reconnaissance et l'acceptation mutuelles de l'identification, de l'authentification et des signatures électroniques ainsi que des services de confiance associés au niveau transnational lorsque les opérations électroniques le nécessitent.

En raison de la nature non territoriale des services eIAS, une action au niveau de l'UE est justifiée et proportionnée pour mettre en œuvre le marché unique du numérique. Il ne semble pas possible d'atteindre le même résultat en adoptant des mesures réglementaires au niveau des États membres. Une intervention de l'UE est donc nécessaire, appropriée et justifiée.

## 8. SUIVI ET EVALUATION

La Commission surveillera l’application de la législation par un dialogue constant avec toutes les parties concernées et par la collecte de statistiques; elle soumettra au Parlement européen et au Conseil un rapport sur l'incidence de la nouvelle législation quatre ans après l'entrée en vigueur de cette dernière.