ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) BREVET D'INVENTION

(11) N° de publication :
MA 39652 A1

(51) Cl. internationale :
H04L 9/08

(43) Date de publication :
31.08.2018

(21) N° Dépôt :
39652

(22) Date de Dépôt :
30.12.2016

(71) Demandeur(s) :
SAFEDEMAT SARL, 33 AVENUE IBN SINA APPT N 43 AGDAL RABAT (MA)

(72) Inventeur(s) :
EL HOUSSAIN BEN MESSAOUD

(74) Mandataire :
KHOUCHFI OMAIMA

(54) Titre : **SYSTEME D'ECHANGE DE CORRESPONDANCES ELECTRONIQUES SECURISE ET 0 VALEUR PROBANTE**

(57) Abrégé : La présente invention concerne un Système d'échange de correspondances électronique sécurisée et à valeur probante. Ce système est caractérisé par: Une incorporation les Fonctions de chiffrement, déchiffrement, signature, validation de signature, constitution de preuve, horodatage, authentification par certificats électroniques. Ce qui assure la confidentialité des flux, le contrôle d'accès aux données, le contrôle d'intégrité des informations échangées. Innovation par rapport au circuit physique traditionnel (Lettre recommandée postale) : Accusé de réception avec engagement sur le contenu reçu: création d'une relation entre la correspondance et l'accusé de réception qui comporte d'empreinte digitale de la correspondance (sous forme de signature électronique ou sous forme de code à barre 2 D pour l'impression)

ABREGE

La présente invention concerne un **Système d'échange de correspondances électronique sécurisée et à valeur probante.**

Ce système est caractérisé par :

- Une incorporation les Fonctions de chiffrement, déchiffrement, signature, validation de signature, constitution de preuve, horodatage, authentification par certificats électroniques. Ce qui assure la confidentialité des flux, le contrôle d'accès aux données, le contrôle d'intégrité des informations échangées.

- Innovation par rapport au circuit physique traditionnel (Lettre recommandée postale) : Accusé de réception avec engagement sur le contenu reçu : création d'une relation entre la correspondance et l'accusé de réception qui comporte d'empreinte digitale de la correspondance (sous forme de signature électronique ou sous forme de code à barre 2 D pour l'impression)

Titre: Système d'échange de correspondances électronique sécurisée et à valeur probante.

DESCRIPTION

La sécurité des systèmes information connectés est devenue une préoccupation opérationnelle généralisée. Les services de sécurité de pointe et les relations de confiance sont actuellement les caractéristiques les plus recherchées de ces systèmes.

Le besoin croissant d'échanges d'informations sécurisées au sein de l'entreprise et au-delà de ses frontières, la création de nouveaux espaces reposant sur la collaboration entre partenaires internationaux, la mutation vers une économie numérique généralisée... autant de préoccupations qui ont transformé la sécurité de l'information en un enjeu stratégique.

Seulement et de manière parallèle, les dangers entourant cette transformation se développent à rythme soutenu notamment sur le volet sécurité.

La prise de conscience en matière de sécurité amène toute entreprise, à décrire les axes à suivre dans un document de contrôle appelé politique de sécurité, recueillant la nature des objectifs de sécurité à garantir ou à atteindre. La mise en œuvre de la politique de sécurité doit permettre de répondre aux besoins d'intégrité, de disponibilité, de confidentialité, et de traçabilité, qui forment en plus des concepts de gestion des identités et des accès, un moyen de protéger les systèmes d'information des organisations en garantissant les objectifs de sécurité. Notre invention concerne le domaine de la **sécurité informatique des échanges dématérialisés.**

ETAT DE LA TECHNIQUE ANTERIEURE

La messagerie électronique est le moyen de communication principal pour de nombreuses entreprises, son utilisation dans le cadre de l'échange de documents sensibles ou confidentiels n'est pas sans poser de problèmes. Les protocoles normalisés qui permettent de mettre en œuvre les applications de messagerie ont en effet été conçus dans les années 1970, époque à laquelle le risque sécuritaire lié aux échanges dématérialisés n'était pas si critique qu'aujourd'hui. Lors des échanges électroniques, les interlocuteurs peuvent très bien ne pas se connaître et le courriel transmis en clair est potentiellement interceptable et lisible. Il faut donc un moyen sûr d'identifier l'auteur d'un message électronique, et faire en sorte que l'on puisse vérifier que le message n'a pas été altéré ou modifié lors de son transport sur le réseau.

Jusqu'à présent les services de la messagerie électronique actuels offrent uniquement :

- **Administration décentralisée, potentiellement lourde et coûteuse.**
- **Suivi et traçabilité limités.**
- **Confidentialité non garantie, souvent douteuse.**
- **Moyens d'authentification et de cloisonnement perfectibles**
- **Un accusé de réception ne répondant à aucun cadre juridique.**

- **Identité de l'émetteur et destinataire non garantie.**
- **N'offrent pas une traçabilité précise et de la valeur probante**

DESCRIPTION DU PROCEDE

La présente invention introduit une solution spécialement conçue pour sécuriser les échanges dématérialisés des entreprises qui placent la confidentialité et la traçabilité au cœur de leurs problématiques d'échanges. En effet, Cette solution est assimilable à un service d'échange électronique à vocation de preuve, permettant la transmission, la traçabilité et la conservation de courriers électroniques recommandés, certifiés et confidentiels. La plateforme propose la QoS suivante : **authentification forte des parties, signature électronique et chiffrement des messages par l'émetteur, traçabilité précise de l'échange avec horodatage des traces et enfin la notion d'accusé de lecture et de réception probant**. Nous proposons également les fonctions de coffre fort électronique permettant d'offrir une solution d'infrastructure de conservation de manière sécurisée des documents nécessitant des mesures de contrôle d'accès et de traçabilité renforcées et/ou de conserver des documents en leur conférant valeur probante.

Or, Le système joue le rôle de tiers de confiance entre les parties prenantes d'un échange. A ce titre, il conserve les preuves électroniques associées aux échanges, que ce soit les signatures électroniques établies par les émetteurs des messages, ou les jetons d'horodatage associés aux événements importants qui se produisent durant un échange

En réponse aux limitations indiquées dans la section « Etat de la technique antérieure». La présente invention permet de fournir un degré plus élevé de protection et de traçabilité, grâce à :

- Un mécanisme d'authentification interne (LDAP, AD) ou par SSO ou par tokens cryptographique matériels
- Un module de signature électronique avancée au format XAdES
- Un système de sécurisation des échanges et des données par chiffrement (symétrique AES et asymétrique RSA)
- Des accusés de dépôt, de réception et de lecture des courriels signés et horodatés numériques probants

En effet, le courrier doit être acheminé par un tiers selon un procédé permettant d'identifier ce dernier, les identités de l'expéditeur et du destinataire doivent être garanties par le moyen des certificats et de l'authentification forte, et La remise (ou la non remise) de la lettre au destinataire doit également être établie.

La valeur ajoutée de l'invention, concerne la notion de l'enveloppe inviolable qui réside en la détection de l'ouverture précoce de fichier par rapport à l'ouverture par le destinataire, et l'innovation par rapport au circuit physique traditionnel ou lettre recommandée postale via la création d'une relation entre la correspondance et l'accusé de réception qui comporte l'empreinte digitale de la correspondance sous forme de signature électronique et sous forme de code à barre 2D pour l'impression. De plus, un historique complet des actions effectuées est conservé et permet d'assurer une traçabilité complète pour chaque échange de document pour des raisons d'audit à postériori.

DESCRIPTION TECHNIQUE

COMPOSANTES DE LA SOLUTION

Notre solution se compose des modules applicatifs suivants :

Connexion (Portail d'accès sécurisé)

L'utilisateur se connecte sur la plateforme par authentification forte à base de certificat matériel. Il accède à un tableau de bord permettant de classer, trier les courriers par date, par expéditeur, par destinataire, par mode d'envoi et par type de courrier.

Envoi de courrier (routage)

L'utilisateur choisit le mode d'envoi de son courrier. Il renseigne un ou plusieurs destinataires, saisit le titre du courrier, insère un texte et/ou des pièces jointes et définit les options de signature et d'archivage.

Avant de valider l'envoi d'un courrier, l'utilisateur consulte le solde disponible sur son compte et confirme sa demande en cliquant sur le bouton « envoyer », l'acceptation, par l'utilisateur, du décompte des courriers correspondants étant dès lors ferme et définitive.

Archivage du courrier (Archivage)

L'archivage d'un courrier peut être demandé par l'expéditeur avant ou après l'envoi et par les destinataires après l'ouverture du courrier. Avant de valider la demande d'archivage, l'utilisateur consulte l'espace d'archivage (en Mo) nécessaire au dépôt et si le solde disponible sur son compte est suffisant, l'utilisateur confirme sa demande en cliquant sur le bouton « archiver » (ou « envoyer » si l'archivage est demandé en même temps que l'envoi), l'acceptation, par l'utilisateur, du décompte de l'espace d'archivage correspondant étant dès lors ferme et définitive.

Réception et ouverture d'une lettre recommandée électronique (Notifications)

Pour avertir un utilisateur qu'une lettre recommandée lui est adressée, la plateforme déclenche l'envoi d'un email de notification à l'adresse donnée par l'expéditeur. Une fois connecté à l'application, l'utilisateur peut accepter et ouvrir, accéder au contenu et à l'historique des événements ou bien refuser la lettre recommandée électronique. L'accusé de lecture n'est pas générer dans le dernier cas.

Signature électronique (Preuves électroniques) :

La plateforme fournit une solution pour signer électroniquement les documents joints aux courriers en utilisant un certificat de signature de type X509 délivré par une autorité de certification du marché configuré en backoffice.

Traçabilité des échanges (Preuves électroniques):

L'historique des événements intégré au courrier contient la liste des événements enregistrés pendant la « période d'activité », période pendant laquelle les utilisateurs mentionnés peuvent effectuer des opérations sur le courrier : acceptation, première ouverture, archivage. La période d'activité est égale à la durée de maintien en ligne. A l'issue de la période d'activité, s'il a déjà ouvert son courrier, l'utilisateur pourra le rouvrir et ce tant que le courrier sera disponible en ligne. Inversement, s'il n'a pas ouvert son courrier dans les délais, l'utilisateur ne pourra plus jamais accéder à son contenu (texte et/ou pièces jointes). Les

événements sont journalisés, signés et archivés par la plateforme pour une durée, appelée « durée de séquestre », pendant laquelle, en cas de contestation par un utilisateur, la plateforme sera en mesure d'attester et de témoigner de la réalité des événements.

DESCRIPTION FONCTIONNELLE

Le système proposé correspond à un **système d'échanges de correspondances électronique** permettant à ses utilisateurs, via un espace front office, la gestion des courriers en incorporant des modules d'authentification, d'envoi et de réception du courrier, de gestion des options (signature et archivage) et de suivi et classement du courrier. Les utilisateurs peuvent également gérer leurs comptes (identité, certificat, email...) et abonnement via un module de commande en ligne et de consultation du solde disponible de courriers et d'espace d'archivage. L'espace back office permet à l'administrateur de la plateforme d'initier les clés de chiffrement de la plateforme, d'installer les certificats de signature et authentification, de paramétrer les serveurs d 'horodatage et serveurs mail, d'accéder aux statistiques et d'exporter les journaux et de consulter les avis d'opérations (accusé de dépôt, accusé de réception, accusé de lecture).

WORKFLOW DE FONCTIONNEMENT DU SYSTEME :

Après la création de son compte en déclarant le certificat d'authentification/signature et la partie publique du certificat de chiffrement, l'expéditeur se connecte à la plateforme à en utilisant un token cryptographique. Dès que l'expéditeur compose sa lettre recommandée numérique, le tiers de confiance acheminant la lettre enregistre l'expédition qui est par la suite enveloppée et signée par le certificat utilisateur. La plateforme chiffre la correspondance avec la clé publique du destinataire et génère l'empreinte de l'enveloppe finale de la correspondance. Le destinataire notifié par sms et par email accède à la plateforme à l'aide de son certificat matériel et visualise le contenu du courrier qui reste maintenu en ligne, pour tous les correspondants, pendant une période configurable, mentionnée sur le courrier, appelée « durée de validité». A l'issue de cette durée, le courrier est supprimé des serveurs et son contenu n'est plus accessible. Si le courrier a été archivé dans le coffre numérique, son contenu sera accessible en ligne pendant toute la durée d'archivage.
Parallèlement, pour chaque étape, un accusé signé et horodaté est généré et stocké, et le journal est mis à jour avec l'historique de la correspondance avec les dates de chaque événement.
Voir **figure 1**.

EXPOSE DU MODE DE REALISATION

Une implémentation possible de ce système, peut être faite grâce à l'utilisation des briques suivantes :

- **Infrastructure de gestion de clés :** pour la signature, l'horodatage et la gestion des CRLs.
- **Module de notification :** afin de notifier le destinataire de la réception d'un nouveau courrier par sms et email.
- **Système d'archivage électronique :** la plateforme étant un canal d'échange de correspondance, le stockage des courriels est confié à un module externe d'archivage pour la conservation des documents à valeur probante.

APPLICATIONS INDUSTRIELLES

L'invention objet de la présente, est susceptible d'applications industrielles dans les domaines suivants (parmi d'autres), cette liste n'est pas exhaustive :

- A2B : Télé-déclaration, échange inter-Administration...
- B2B : Bon de commande, devis, facture...
- B2C : Bulletins de paie, dossiers médicaux...
- Finance : Relevé bancaire, ordres de virements, contrats d'assurances...

REVENDICATIONS D'INNOVATION

Les revendications portent sur :

1. Système d'échange et de transmission applicatif des données informatiques, caractérisé en ce qu'il comprend au moins un moyen de confiner de manière sécurisée les données dans une enveloppe scellée, protégée et confidentielle, au moins un moyen d'identification de manière fiable de l'expéditeur et du destinataire à travers un mécanisme d'authentification forte, au moins un moyen d'engager le destinataire sur l'acceptation ou le refus de recevoir cette enveloppe et au moins un moyen de notifier l'expéditeur de la décision du destinataire.

2. Système conforme à la revendication 1, en ce qu'il permet de générer un Accusé de réception avec engagement sur le contenu reçu à travers la création d'une relation entre l'enveloppe et l'accusé de réception qui comporte d'empreinte digitale de l'enveloppe (sous forme de signature électronique ou sous forme de code à barre 2 D pour l'impression).

3. Système conforme à la revendication 1, à travers duquel les données transitent confinées dans une enveloppe sécurisé permettant la détection de son ouverture précoce par un acteur autre que le destinataire désigné par l'émetteur.

DESSIN

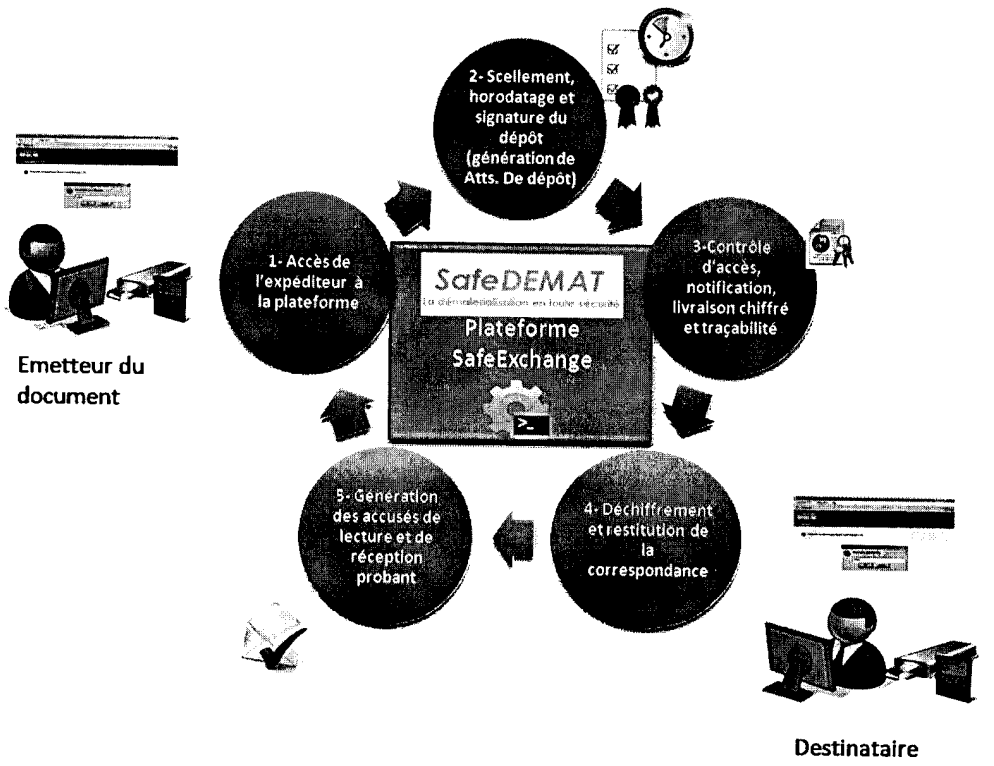

Figure 1 – Workflow du Système d'échange de correspondances électroniques sécurisé et à valeur probante

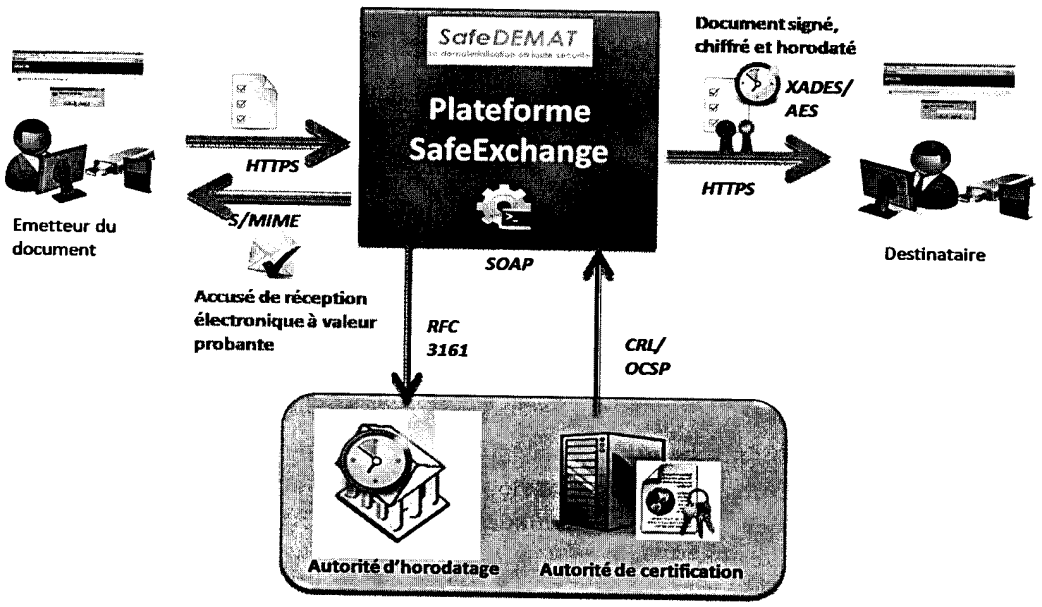

Figure 2 – Composantes du Système d'échange de correspondances électroniques sécurisé et à valeur probante

MA 39652A1

ROYAUME DU MAROC
****
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
****

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 39652	Date de dépôt : 30/12/2016
Déposant : SAFEDEMAT SARL	
Intitulé de l'invention : SYSTEME D'ECHANGE DE CORRESPONDANCES ELECTRONIQUES SECURISE ET A VALEUR PROBANTE	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☐ Cadre 4 : Remarques de clarté
- ☒ Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée
- ☐ Cadre 7 : Défaut d'unité d'invention

Examinateur: BAMI MOHAMMED	**Date d'établissement du rapport** : 10/03/2017
Téléphone: **212 5 22 58 64 14/00**	

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  5 Pages
- Revendications
  1-3
- Planches de dessin
  1 Page

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L9/32

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	EP2372947 A1; Evidencecube ; 05/10/2011	1
Y	EP2372947 A1; Evidencecube ; 05/10/2011 US9444645 B2 ; Trustseed Sas ; 13/09/2016	2
Y	EP2372947 A1; Evidencecube ; 05/10/2011 US9338011 B2 ; Adobe Systems Incorporated ; 10/05/2016	3

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications 2-3 Revendications 1	Oui Non
Activité inventive (AI)	Revendications aucune Revendications 1-3	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-3 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : EP2372947 A1
D2 : US9444645 B2
D3 : US9338011 B2

1. **Nouveauté (N) :**

Le document D1 divulgue :
Un système d'échange et de transmission des données informatiques (voir description paragraphe 0001) caractérisé en ce qu'il comprend un moyen de confiner de manière sécurisée les données dans une enveloppe scellée (voir description paragraphe 0013), protégée et confidentielle (voir description paragraphe 0013 qui divulgue que l'enveloppe digitale est protégée par une clé cryptée, voir aussi paragraphe 0021 qui décrit la confidentialité de l'information contenue dans l'enveloppe).
Un moyen d'identification fiable de l'expéditeur et du destinataire (voir paragraphe 0029).
Un moyen d'engager le destinataire sur l'acceptation ou le refus de recevoir cette enveloppe et un moyen de notifier l'expéditeur de la décision du destinataire (voir paragraphe 0047, un tiers génère deux notifications sous la forme d'un accusé d'acceptation et un accusé de refus).
L'objet de la revendication 1 n'est donc pas nouveau au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.
Le document D1 ne divulgue pas que l'accusé de réception comporte un code à barre.
L'objet de la revendication 2 est donc nouveau au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.
Le document D1 ne divulgue pas la détection de l'ouverture précoce de l'enveloppe. L'objet de la revendication 3 est donc nouveau au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

2. **Activité inventive (AI) :**

Le document D1 est considéré comme l'état de la technique le plus proche de l'objet de la revendication 2.
L'objet de la revendication 2 diffère de D1 en ce que l'accusé de réception comporte un code à barre 2D.
L'objet de la revendication 2 n'implique pas une activité inventive au sens de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13. En effet D1 divulgue que l'accusé de réception (voir paragraphe 0048) est de la même structure que l'accusé d'envoi comprenant une

signature digitale. La signature digitale peut être sous plusieurs formes, y compris les codes à barre. En outre, le document D2, considéré comme un état de l'art analogue, divulgue un accusé de réception comprenant un code à barre (voir description page 28, colonne 36, lignes 36-40). L'homme du métier aurait évidemment combiné les enseignements de D1 et D2 pour aboutir à la solution proposée sans faire preuve d'esprit inventif.
Les techniques de la détection de l'ouverture d'un contenu numérique (voir D3 à titre d'exemple) sont largement connues et répandues dans les systèmes de communication électroniques. L'objet de la revendication 3 ne contient aucune caractéristique technique qui, en combinaison avec l'une quelconque des revendications à laquelle elle se réfère, implique une activité inventive au sens de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

3. Possibilité d'application industrielle (PAI) :

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.