(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 136 073***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **22 04976**

(51) Int Cl[8] : ***G 06 F 21/00*** *(2024.01), H 04 L 51/00*

(12) BREVET D'INVENTION B1

(54) Procédé d'envoi sécurisé d'un courrier électronique.

(22) **Date de dépôt :** 24.05.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 01.12.23 Bulletin 23/48.

(45) **Date de la mise à disposition du public du brevet d'invention :** 04.10.24 Bulletin 24/40.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

(60) **Références à d'autres documents nationaux apparentés :**

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *MAILSPEC SAS Société par actions simplifiée (SAS)* — FR.

(72) **Inventeur(s) :** DOYLE Jon.

(73) **Titulaire(s) :** MAILSPEC SAS Société par actions simplifiée (SAS).

(74) **Mandataire(s) :** ATOUT PI LAPLACE.

FR 3 136 073 - B1

Description

Titre de l'invention : Procédé d'envoi sécurisé d'un courrier électronique

DOMAINE DE L'INVENTION

[0001] Le domaine technique de la présente invention concerne l'envoi et la réception sécurisé de courriers électroniques.

Technique antérieure

[0002] L'envoi et la réception de courriers électroniques sont régis par plusieurs protocoles : SMTP permettant l'envoi d'un courrier et POP et IMAP permettant de rapatrier le courrier pour être lu par un utilisateur. Un client de messagerie (MUA) de l'expéditeur envoie par SMTP le courrier électronique à un serveur. Le serveur route le message vers le serveur du destinataire. Le serveur du destinataire délivre à un MDA (Mail Delivery Agent) qui est chargé de la gestion des boîtes emails. Le destinataire, par l'intermédiaire de son MUA, demande au MDA les nouveaux messages via l'utilisation des protocoles IMAP ou POP. Le serveur envoie le message au MUA du destinataire.

[0003] Cependant, les protocoles utilisés pour l'envoi et la réception des courriers électroniques ont été inventés avant l'utilisation de l'Internet à haut débit. De plus, il existe de nombreux types de courriers électroniques provenant de différents services de messageries électroniques. Pour cette raison il est difficile de sécuriser l'envoi et la réception de courriers électroniques.

[0004] De plus, les services de messageries électroniques nécessitent l'authentification par un nom d'utilisateur et un mot de passe. Cependant, si le nom d'utilisateur et le mot de passe sont obtenus par une personne autre que l'utilisateur, par exemple, lors de l'emploi de mots de passe simples à deviner, d'autres utilisateurs peuvent envoyer des courriers électroniques malveillants ou accéder à des données confidentielles.

Résumé de l'invention

[0005] L'invention vient améliorer la situation en proposant un procédé d'envoi sécurisé de courriers électroniques. En effet, la présente invention propose une double authentification permettant de s'assurer que l'utilisateur associé à un service de messagerie est également l'utilisateur envoyant un courrier électronique depuis ce même service de messagerie.

[0006] De plus, il est noté que les protocoles utilisés pour l'envoi et la réception des courriers électroniques, dû à l'ancienneté de cette technologie, inclus un délai entre le moment où un utilisateur souhaite envoyer un courrier électronique (par exemple, en cliquant sur « envoyer ») et le moment où celui-ci est envoyé. Ainsi, le procédé décrit

dans la présente demande tire avantage de ce délai car une authentification peut être réalisée pendant ce délai.

[0007] De façon similaire, un procédé de réception sécurisé de courriers électroniques est également décrit, utilisant également une double authentification permettant de s'assurer que l'utilisateur associé à un service de messagerie est également l'utilisateur recevant un courrier électronique depuis ce même service de messagerie.

[0008] Ainsi, l'invention vient améliorer la situation en proposant un procédé d'envoi sécurisé d'un courrier électronique, le procédé comprenant : recevoir au niveau d'un serveur de messagerie électronique une requête provenant d'un utilisateur pour envoyer le courrier électronique, l'utilisateur ayant un compte de messagerie électronique sur le serveur de messagerie électronique, l'utilisateur s'étant préalablement identifié au compte de messagerie électronique ; en réponse à la réception de la requête, envoyer par le serveur un test de sécurité à compléter par l'utilisateur à un appareil de confiance associé à l'utilisateur via un canal sécurisé ; recevoir le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé ; vérifier le test de sécurité complété par l'utilisateur par le serveur ; et envoyer le courrier électronique par le serveur si le test est validé par l'utilisateur.

[0009] De plus, l'invention vient améliorer la situation en proposant un procédé d'envoi sécurisé d'un courrier électronique, le procédé comprenant : recevoir, à un appareil de confiance associé à l'utilisateur en réponse à la réception d'une requête de transmission d'un courrier électronique par un serveur, un test de sécurité à compléter par l'utilisateur via un canal sécurisé ; compléter le test de sécurité par l'utilisateur sur l'appareil de confiance ; transmettre le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé pour validation et transmission du courrier électronique par le serveur si le test est validé par l'utilisateur.

[0010] De plus, l'invention vient améliorer la situation en proposant un procédé de détection d'une requête pour l'envoi d'un courrier électronique, le procédé comprenant : recevoir au niveau d'un serveur de messagerie électronique une requête provenant d'un utilisateur pour envoyer le courrier électronique, l'utilisateur ayant un compte de messagerie électronique sur le serveur de messagerie électronique, l'utilisateur s'étant préalablement identifié au compte de messagerie électronique; en réponse à la réception de la requête, envoyer par le serveur un test de sécurité à compléter par l'utilisateur à un appareil de confiance associé à l'utilisateur via un canal sécurisé ; recevoir le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé ; vérifier le test de sécurité complété par l'utilisateur par le serveur ; et rejeter le courrier électronique ou l'envoyer par le serveur à un autre destinataire que celui précisé dans le message si le test n'est pas validé par l'utilisateur.

[0011] Dans un mode de réalisation, le procédé comprend en outre : recevoir au niveau du

serveur de messagerie électronique une autre requête provenant de l'utilisateur pour envoyer un autre courrier électronique ; vérifier un paramètre de sécurité pré-déterminé ; envoyer le courrier électronique par le serveur si le paramètre de sécurité prédéterminé est satisfait.

[0012] Dans un mode de réalisation, le paramètre de sécurité comprenant : un temps écoulé entre l'envoie de la requête et de l'autre requête, un changement d'adresse IP utilisée par l'utilisateur et une date à laquelle la requête est envoyée par l'utilisateur.

[0013] Dans un mode de réalisation, le test de sécurité comprend une comparaison d'une entrée biométrique avec des données biométriques associées à l'utilisateur et stockées sur l'appareil de confiance associé à l'utilisateur.

[0014] Dans un mode de réalisation, l'appareil de confiance associé à l'utilisateur est un téléphone portable ou une clé USB.

[0015] Dans un mode de réalisation, l'appareil de confiance comprend une application permettant de compléter le test de sécurité.

[0016] De plus l'invention vient à améliorer la situation en proposant un produit-programme d'ordinateur comprenant des instructions qui, lorsque le programme est exécuté par un ordinateur, amènent l'ordinateur à mettre en œuvre les procédés décrits ci-dessus.

[0017] De plus, l'invention vient à améliorer la situation en proposant un serveur permettant l'envoi sécurisé d'un courrier électronique, le serveur étant configuré pour mettre en œuvre le procédé d'envoi sécurisé d'un courrier électronique.

[0018] De plus, l'invention vient à améliorer la situation en proposant un appareil de confiance permettant l'envoi sécurisé d'un courrier électronique, l'appareil de confiance étant configuré pour mettre en œuvre le procédé d'envoi sécurisé d'un courrier électronique.

[0019] De plus, l'invention vient à améliorer la situation en proposant un procédé de réception sécurisée d'un courrier électronique par un utilisateur, le procédé comprenant : recevoir au niveau d'un serveur de messagerie électronique une requête pour recevoir le courrier électronique, l'utilisateur ayant un compte de messagerie électronique sur le serveur de messagerie électronique, l'utilisateur s'étant préalablement identifié au compte de messagerie électronique ; en réponse à la réception de la requête, envoyer par le serveur un test de sécurité à compléter par l'utilisateur à un appareil de confiance associé à l'utilisateur via un canal sécurisé ; recevoir le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé ; vérifier le test de sécurité complété par l'utilisateur par le serveur ; recevoir le courrier électronique par le serveur ; et envoyer le courrier électronique par le serveur à l'utilisateur si le test est validé par l'utilisateur.

[0020] Procédé de réception sécurisée d'un courrier électronique par un utilisateur, le procédé comprenant : recevoir, à un appareil de confiance associé à l'utilisateur, en

réponse à la réception d'une requête de réception d'un courrier électronique par un serveur, un test de sécurité à compléter par l'utilisateur via un canal sécurisé ; et compléter le test de sécurité par l'utilisateur sur l'appareil de confiance ; transmettre le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé pour validation et transmission du courrier à l'utilisateur par le serveur si le test est validé par l'utilisateur.

Brève description des dessins

[0021] D'autres caractéristiques, détails et avantages de l'invention ressortiront à la lecture de la description faite en référence aux dessins annexés donnés à titre d'exemple et qui représentent, respectivement :

[0022] [Fig.1] une représentation schématique d'un exemple de système permettant l'envoi sécurisé d'un courrier électronique ;

[0023] [Fig.2a] un exemple de procédé d'envoi sécurisé d'un courrier électronique ;

[0024] [Fig.2b] un exemple de procédé d'envoi sécurisé d'un courrier électronique ;

[0025] [Fig.3a] représente un exemple de procédé de réception sécurisée d'un courrier électronique ; et

[0026] [Fig.3b] représente un exemple de procédé de réception sécurisée d'un courrier électronique.

DESCRIPTION DETAILLEE

[0027] La [Fig.1] illustre un exemple de système 100 permettant l'envoi sécurisé d'un courrier électronique.

[0028] Le système 100 comprend un serveur de messagerie électronique 102. Un utilisateur a un compte de messagerie électronique sur le serveur 102. L'utilisateur s'est préalablement identifié au compte de messagerie électronique. Le serveur peut être, par exemple, sur un réseau local de l'utilisateur. Le serveur 102 étant configuré pour recevoir une requête provenant de l'utilisateur pour envoyer le courrier électronique. Par exemple, le serveur de messagerie électronique 102 peut être un serveur 102 auquel l'utilisateur accède par un ordinateur personnel ou un ordinateur de travail, lui permettant d'accéder à une ou plusieurs boites aux lettres électroniques. Afin d'utiliser sa messagerie électronique liée au serveur 102, l'utilisateur s'est préalablement authentifié grâce à un nom d'utilisateur et un mot de passe. Lorsque l'utilisateur tente d'envoyer un courrier électronique qu'il/elle a rédigé depuis sa messagerie électronique, une requête pour envoyer le courrier électronique est transmise au serveur 102.

[0029] De plus, le système 100 comprend un appareil de confiance 104 associé à l'utilisateur, l'appareil de confiance 104 étant configuré pour recevoir un test de sécurité envoyé par le serveur à compléter par l'utilisateur et envoyer le test complété

au serveur 102 via un canal sécurisé. Par exemple, l'appareil de confiance 104 peut être un téléphone portable, tel qu'un un smartphone, ou une tablette ou encore une montre intelligente associé à l'utilisateur. L'appareil de confiance 104 peut également être une clé USB ayant un dispositif permettant d'entrer une entrée biométrique.

[0030] Le test de sécurité peut comprendre une comparaison entre une entrée biométrique avec des données biométriques associées à l'utilisateur et stockées sur l'appareil de confiance 104 associé à l'utilisateur. Par exemple, l'appareil de confiance 104 peut comprendre un dispositif permettant de générer des données biométriques tel qu'un capteur d'empreintes digitales, de reconnaissance faciale, de balayage de l'iris ou d'analyse vocale. L'appareil de confiance 104 peut demander à l'utilisateur de rentrer ses données biométriques, par exemple son empreinte digitale en posant son doigt sur le capteur biométrique via son téléphone portable ou sa clé USB. Dans un autre exemple, les données biométriques peuvent être une reconnaissance faciale ou un signe de vie tel que le pouls ou la respiration de l'utilisateur. L'appareil de confiance 104 vérifie que l'empreinte digitale correspond à celle de l'utilisateur. Par exemple, l'appareil de confiance 104 peut stocker des données biométriques associées à un ou plusieurs utilisateurs préalablement entrées par l'utilisateur, afin de les comparer aux données biométriques générées lors du test de sécurité. L'appareil de confiance 104 peut émettre un résultat du test complété. Par exemple, si les données biométriques rentrées par l'utilisateur correspondent aux données stockées, l'appareil de confiance 104 peut émettre un résultat indiquant que les données sont celles de l'utilisateur. Au contraire, si les données biométriques rentrées par l'utilisateur ne correspondent pas aux données stockées, l'appareil de confiance 104 peut émettre un résultat indiquant que les données ne sont pas celles de l'utilisateur. Dans un exemple, l'appareil de confiance 104 peut déterminer que les biométriques rentrées par l'utilisateur correspondent aux données stockées lorsque que l'appareil de confiance 104 détermine que l'entrée biométrique satisfait un critère de similarité prédéfini par rapport aux données biométriques associées à l'utilisateur. Par exemple, le critère de similarité peut correspondre à un seuil de similarité entre l'entrée biométrique et les données biométriques associées à l'utilisateur. Dans un autre exemple, le test de sécurité peut comprendre un mot de passe. Par exemple, l'utilisateur peut recevoir une notification sur l'appareil de confiance 104 lui indiquant de rentrer un mot de passe. Le mot de passe peut être un de passe temporaire envoyé sur l'appareil de confiance 104, tel qu'un nombre envoyé sur le téléphone portable de l'utilisateur et utilisable pour quelques minutes. Dans un autre exemple, le mot de passe peut être un mot de passe permanent créé préalablement par l'utilisateur. Dans un autre exemple, le test peut être de répondre à une question dont la réponse a été préalablement enregistrée sur l'appareil de confiance 104 associé à l'utilisateur.

[0031] Dans un exemple, l'appareil de confiance 104 comprend une application permettant de compléter le test de sécurité. L'application peut être installée préalablement sur l'appareil de confiance 104. L'application peut par exemple stocker les données biométriques associées à l'utilisateur. Par exemple, l'application peut être associée avec une interface de programmation permettant à l'utilisateur d'enregistrer préalablement ses données biométriques.

[0032] Ainsi, lorsque que la requête pour envoyer le courrier électronique est transmise au serveur 102, le serveur 102 envoie le test de sécurité à compléter par l'utilisateur à l'appareil de confiance 104 associé à l'utilisateur via un canal sécurisé. Le canal sécurisé est un canal encrypté. Par exemple, le serveur 102 et l'appareil de confiance 104 peuvent communiquer en cryptant le test de sécurité l'un pour l'autre à l'aide d'une clé de session. De plus, dans un exemple, un algorithme de chiffrement par bloc (tel que SEED) peut être utilisé afin d'établir un cryptage du canal sécurisé. Par exemple, l'utilisateur peut recevoir une notification de l'application de l'appareil de confiance 104 lui indiquant qu'il/elle doit entrer ses données biométriques afin de compléter le test. L'utilisateur peut alors ouvrir l'application et compléter le test de sécurité, en entrant par exemple ses données biométriques. Une fois complété, le test de sécurité est renvoyé par l'appareil de confiance 104 au serveur 102 via le canal sécurisé. Par exemple, le résultat du test peut être envoyé par l'appareil de confiance 104 au serveur 102 via le canal sécurisé. Dans un exemple, le test de sécurité complété peut être crypté à l'aide d'une clé de session. Par exemple, l'appareil de confiance 104 peut générer aléatoirement la clé de session qui est cryptée avec une clé publique. Lorsque le serveur 102 reçoit le test de sécurité, le serveur 102 peut décrypter la clé de session à l'aide d'une clé privée.

[0033] Le serveur 102 peut ensuite valider le test de sécurité complété par l'utilisateur. Dans un exemple, l'appareil de confiance 104 peut envoyer au serveur 102 les données biométriques entrées par l'utilisateur et des données stockées sur l'appareil de confiance 104 représentant des données biométriques associées à l'utilisateur. Le serveur 102 peut ensuite comparer les données entrées et les données stockées et vérifier la correspondance entre les données. Dans un autre exemple, l'appareil de confiance 104 compare les données biométriques et des données stockées sur l'appareil de confiance 102 représentant des données biométriques associées à l'utilisateur et génère un résultat correspondant à un taux de correspondance entre les données entrées par l'utilisateur et les données stockées. Le taux de correspondance peut être ensuite envoyé au serveur 102. Le serveur 102 peut ensuite comparer le taux de correspondance avec un seuil. Dans un autre exemple, l'appareil de confiance 104 compare les données biométriques et des données stockées sur l'appareil de confiance 104 représentant des données biométriques associées à l'utilisateur et génère une indication

booléenne (par exemple : « validé » ou « non validé »). L'appareil de confiance 104 envoie ensuite l'indication booléenne au serveur 102. Par exemple, lorsque le résultat du test reçu par le serveur 102 indique que les données sont celles de l'utilisateur, le serveur 102 envoie le courrier électronique. Au contraire, lorsque le résultat du test reçu par le serveur 102 indique que les données ne sont pas celles de l'utilisateur, le serveur n'envoie pas le courrier électronique (par exemple surprime le courrier électronique), ou alternativement le courrier électronique est renvoyé à l'utilisateur au lieu d'être envoyé au destinataire du courrier électronique. Dans un exemple, le serveur 102 peut émettre un message d'erreur.

[0034] De plus, le système 100 comprend une unité de destination 106 configurée pour recevoir l'email si le test de sécurité est validé par le serveur 102. Par exemple, l'unité de destination 106 peut être un ordinateur d'un autre utilisateur étant le destinateur du courrier électronique envoyé par l'utilisateur.

[0035] Le système 100 décrit ci-dessus permet d'utiliser une double authentification de l'utilisateur : l'authentification à l'aide d'un identifient et mot de passe pour accéder à la boite email et l'authentification au moment de l'envoie un courrier électronique avec l'utilisation d'un test de sécurité. Ainsi, le système 100 est avantageux car il permet de s'assurer que l'utilisateur envoie le courrier électronique lui-même et évitant ainsi le hameçonnage ou le piratage informatique.

[0036] La [Fig.2a] illustre un exemple de procédé 200a d'envoi sécurisé d'un courrier électronique. Le procédé 200a peut être implémenté par le serveur 102 décrit ci-dessus.

[0037] Au bloc 202a, le procédé 200a comprend recevoir au niveau d'un serveur 102 de messagerie électronique une requête provenant d'un utilisateur pour envoyer le courrier électronique, l'utilisateur ayant un compte de messagerie électronique sur le serveur 102 de messagerie électronique, l'utilisateur s'étant préalablement identifié au compte de messagerie électronique. L'utilisateur peut s'identifier en utilisant un nom d'utilisateur et un mot de passe. Par exemple, l'utilisateur rédige un courrier électronique qu'il/elle souhaite envoyer. Lorsque l'utilisateur souhaite envoyer le courrier électronique (par exemple en cliquant sur « envoyer »), une requête est envoyée au serveur 102. Il est noté qu'à ce stade, le courrier électronique n'est pas encore envoyé au destinataire. Le serveur 102 peut être sur un réseau local de l'utilisateur

[0038] Au bloc 204a, le procédé 200a comprend en réponse à la réception de la requête, envoyer par le serveur 102 un test de sécurité à compléter par l'utilisateur à un appareil de confiance 104 associé à l'utilisateur via un canal sécurisé. Dans un exemple, l'appareil de confiance 104 associé à l'utilisateur est un téléphone portable, comme par exemple un smartphone possédant un dispositif permettant de générer des données biométriques. Dans un autre exemple, l'appareil de confiance 104 est une tablette ou une montre intelligente. Dans un exemple, l'appareil de confiance 104 comprend une ap-

plication permettant de compléter le test de sécurité. Par exemple, l'utilisateur reçoit une notification sur son téléphone portable pour entrer son empreinte digitale.

[0039] Au bloc 206a, le procédé 200a comprend recevoir le test de sécurité complété par l'utilisateur au serveur 102 via le canal sécurisé. Par exemple, le serveur 102 reçoit l'entrée biométrique entrée par l'utilisateur.

[0040] Au bloc 208a, le procédé 200a comprend vérifier le test de sécurité complété par l'utilisateur par le serveur 102. Par exemple, une comparaison entre l'entrée biométrique entrée par l'utilisateur avec des données biométriques associées à l'utilisateur. Par exemple, si l'entrée biométrique entrée par l'utilisateur correspond aux données biométriques associées à l'utilisateur, le test est validé. Au contraire, si l'entrée biométrique entrée par l'utilisateur ne correspond pas aux données biométriques associées à l'utilisateur, le test n'est pas validé.

[0041] Au bloc 210a, le procédé 200a comprend envoyer le courrier électronique par le serveur si le test est validé par l'utilisateur. En effet, si le test est validé, il est assuré que l'utilisateur qui envoie le courrier électronique est bien la personne associée à la boite email depuis laquelle le courrier électronique est envoyé.

[0042] Alternativement au bloc 201a, le procédé 200a peut comprendre rejeter le courrier électronique ou l'envoyer par le serveur à un autre destinataire que celui précisé dans le message si le test n'est pas validé par l'utilisateur. En effet, si le test n'est pas validé, cela signifie que l'utilisateur qui envoie le courrier électronique n'est pas la personne associée à la boite email depuis laquelle le courrier électronique est envoyé. Par exemple, le courrier électronique peut être est renvoyé à l'utilisateur qui a envoyé la requête au lieu d'être envoyé au destinataire du courrier électronique. Dans un exemple, un message d'erreur peut être envoyé à l'utilisateur.

[0043] Dans un exemple, le procédé 200a comprend des étapes supplémentaires comprenant : recevoir au niveau du serveur de messagerie électronique 102 une autre requête provenant de l'utilisateur pour envoyer un autre courrier électronique, vérifier un paramètre de sécurité prédéterminé et envoyer le courrier électronique par le serveur si le paramètre de sécurité prédéterminé est satisfait. Par exemple, le paramètre de sécurité peut comprendre un nombre de courriers électroniques, un temps écoulé entre la validation d'un dernier test de sécurité, un comportement suspect de l'utilisateur, et l'envoi d'une nouvelle requête, un changement d'adresse IP utilisée par l'utilisateur depuis la validation d'un dernier test de sécurité et une date à laquelle la requête est envoyée par l'utilisateur. Par exemple, l'utilisateur peut envoyer plusieurs courriers électroniques successivement ou simultanément. Si le nombre de courriers électroniques est en dessous d'un seuil prédéterminé, le serveur 102 envoie le courrier électronique. Au contraire, si le nombre de courriers électroniques dépasse du seuil prédéterminé, le serveur 102 n'envoie pas le courrier électronique. Dans un autre

exemple, une requête correspondant à un comportement suspect peut être une requête pour envoyer un courrier électronique à l'intégralité d'un répertoire de contacts de l'utilisateur. Dans un autre exemple, un comportement suspect correspond à une présence de certains mots clé dans le courrier électronique, les mots clé étant préalablement définis. Dans ce cas, si le serveur 102 détecte un comportement suspect, le serveur 102 n'envoie pas le courrier électronique. Dans un autre exemple, lorsque que le serveur 102 détermine que l'adresse IP de l'utilisateur est la même pour plusieurs courriers électroniques envoyés successivement ou simultanément, le serveur 102 envoie le courrier électronique. Au contraire, si l'adresse IP a changé, le serveur 102 n'envoie pas le courrier électronique. Dans un exemple, des adresses IP peuvent être préalablement enregistrées comme étant des adresses IP de confiance. Par exemple, un utilisateur peut avoir des adresses IP de confiance correspondant à son domicile et son lieu de travail. Lorsque le serveur détecte que la requête a été envoyée avec une adresse IP de confiance, le serveur 102 envoie le courrier électronique. De plus ou alternativement, lorsque le serveur 102 détermine qu'un temps inférieur à un seuil de temps est écoulé entre la validation d'un dernier test de sécurité et l'envoi d'une nouvelle requête, le serveur 102 envoie le courrier électronique. Au contraire, lorsque le serveur 102 détermine qu'un temps supérieur à un seuil de temps est écoulé entre la validation d'un dernier test de sécurité et l'envoi d'une nouvelle requête, le serveur 102 n'envoie pas le courrier électronique. Ainsi, il est possible de faciliter l'envoi de courriers électroniques dans certaines situations qui ne sont pas considérées à risque. Par exemple, si l'adresse IP est inchangée, il peut être supposé que l'utilisateur est également inchangé. De plus, en définissant un temps écoulé entre deux requêtes, cela permet à l'utilisateur d'envoyer successivement plusieurs emails sans avoir besoin de compléter un test de sécurité plusieurs fois dans une courte durée. Au contraire, si une situation est considérée à risque, il est préférable de vérifier que l'utilisateur est bien l'utilisateur associée à la boite email depuis laquelle le courrier électronique est envoyé.

[0044] Il est noté que les étapes décrites ci-dessus aux blocs 202a-210a peuvent être effectuée au moment où le client de messagerie envoie par STPM le courrier électronique au serveur 102. En effet, due à l'ancienneté de la technologie et des protocoles utilisés dans l'envoi des courriers électroniques, il y a un délai entre le moment où l'utilisateur clique sur « envoyer » et le moment où le destinataire reçoit le courrier électronique. Ainsi, il est possible de profiter de ce délai pour compléter ces étapes en évitant un délai supplémentaire.

[0045] La [Fig.2b] illustre un exemple de procédé 200b d'envoi sécurisé d'un courrier électronique. Le procédé 200b peut être implémenté par l'appareil de confiance 104 décrit ci-dessus.

[0046] Au bloc 202b, le procédé 200b comprend recevoir, à un appareil de confiance 104 associé à l'utilisateur en réponse à la réception d'une requête de transmission d'un courrier électronique par un serveur, un test de sécurité à compléter par l'utilisateur via un canal sécurisé. Par exemple, lorsque le serveur 102 reçoit la requête provenant de l'utilisateur pour envoyer le courrier électronique dans l'exemple du procédé 200a décrit ci-dessus, le serveur 102 envoie un test de sécurité à l'appareil de confiance 104 pour qu'il soit complété par l'utilisateur. Le test à compléter peut être par exemple une notification pour entrer des données biométriques.

[0047] Au bloc 204b, le procédé 200b comprend compléter comprend test de sécurité par l'utilisateur sur l'appareil de confiance 104. Par exemple, suite à la réception d'une notification sur son téléphone portable 104 pour entrer son empreinte digitale, l'utilisateur entre son empreinte digitale à l'aide du dispositif permettant de générer des données biométriques présent sur son téléphone portable 104.

[0048] Au bloc 206b, le procédé 200b comprend transmettre le test de sécurité complété par l'utilisateur au serveur 102 via le canal sécurisé pour validation et transmission du courrier électronique par le serveur 102 si le test est validé par l'utilisateur. Par exemple, si le test de sécurité complété par l'utilisateur consiste à rentrer des données biométriques, l'appareil de confiance 104 transmet les données obtenues au serveur, ou encore la comparaison entre les données biométriques entrées par l'utilisateur avec des données stockées sur l'appareil de confiance 104 associées à l'utilisateur ou encore un résultat du test (par exemple « validé » ou « non validé »).

[0049] Les procédés 200a, 200b décrits ci-dessus permettent ainsi de s'assurer que l'utilisateur qui envoie le courrier électronique est bien la personne associée à la boite email depuis laquelle le courrier électronique est envoyé. Ainsi, les procédés 200a, 200b permettent d'éviter le hameçonnage et le piratage informatique de boite email.

[0050] La [Fig.3a] illustre un exemple de procédé 300a de réception sécurisée d'un courrier électronique par un utilisateur. Le procédé 300a peut être implémenté par le serveur 102 décrit ci-dessus. En effet, le serveur 102 peut être utilisé pour la transmission et la réception de courriers électroniques.

[0051] Au bloc 302a, le procédé 300a comprend recevoir au niveau d'un serveur de messagerie électronique une requête pour recevoir le courrier électronique, l'utilisateur ayant un compte de messagerie électronique sur le serveur de messagerie électronique, l'utilisateur s'étant préalablement identifié au compte de messagerie électronique. Par exemple, un expéditeur veut envoyer un courrier électronique à l'utilisateur. Cependant, par exemple en cas de confidentialité, il est important que ce courrier électronique soit reçu par le bon utilisateur.

[0052] Au bloc 304a, le procédé 300a comprend en réponse à la réception de la requête, envoyer par le serveur 102 un test de sécurité à compléter par l'utilisateur à un appareil

de confiance 104 associé à l'utilisateur via un canal sécurisé. Par exemple, l'utilisateur reçoit une notification sur son téléphone pour compléter un test de sécurité, tel que l'entrée de données biométriques.

[0053] Au bloc 306a, le procédé 300a comprend recevoir le test de sécurité complété par l'utilisateur au serveur 102 via le canal sécurisé. Par exemple, le serveur 102 reçoit les données biométriques entrées par l'utilisateur.

[0054] Au bloc 308a, le procédé 300a comprend vérifier le test de sécurité complété par l'utilisateur par le serveur. Par exemple, reçoit les données biométriques entrées par l'utilisateur sont comparées avec des données biométriques associées à l'utilisateur. Si les données sont similaires, le test est validé et l'utilisateur correspond au destinataire du courrier électronique. Au contraire, si les données sont différentes, le test n'est pas validé et l'utilisateur ne correspond pas au destinataire du courrier électronique.

[0055] Au bloc 310a, le procédé 300a comprend recevoir le courrier électronique par le serveur.

[0056] Au bloc 312a, le procédé 300a comprend envoyer le courrier électronique par le serveur à l'utilisateur si le test est validé par l'utilisateur. L'utilisateur peut donc ouvrir le courrier électronique. Au contraire, si le test n'est pas validé, le serveur 102 n'envoie pas l'email au destinataire et rejette le message. Par exemple, un message d'erreur s'affiche sur l'écran de l'ordinateur de l'utilisateur.

[0057] La [Fig.3b] illustre un exemple de procédé 300b de réception sécurisée d'un courrier électronique par un utilisateur. Le procédé 300b peut être implémenté par l'appareil de confiance 104 décrit ci-dessus. En effet, l'appareil de confiance 104 peut être utilisé pour la transmission et la réception de courriers électroniques.

[0058] Au bloc 302b, le procédé 300b comprend recevoir, à un appareil de confiance 104 associé à l'utilisateur, en réponse à la réception d'une requête de réception d'un courrier électronique par un serveur 102 un test de sécurité à compléter par l'utilisateur via un canal sécurisé. Par exemple, l'utilisateur reçoit une notification pour entrer ses données biométriques ou un mot de passe.

[0059] Au bloc 304b, le procédé 300b comprend compléter le test de sécurité par l'utilisateur sur l'appareil de confiance 104. Par exemple, l'utilisateur entre ses données biométriques sur son téléphone portable.

[0060] Au bloc 306b, le procédé 300b, le procédé 300b comprend transmettre le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé pour validation et transmission du courrier à l'utilisateur par le serveur si le test est validé par l'utilisateur. Par exemple, si le test de sécurité complété par l'utilisateur consiste à rentrer des données biométriques, l'appareil de confiance 104 transmet les données obtenues au serveur, ou encore la comparaison entre les données biométriques entrées par l'utilisateur avec des données stockées sur l'appareil de confiance 104 associées à

l'utilisateur ou encore un résultat du test (par exemple « validé » ou « non validé »).

[0061] Il est noté que le procédés 300a, 300b peuvent être implémentés en combinaison avec le procédés 200a, 200b ou séparément. De plus, les procédés 300a, 300b peuvent être implémentés par le système 100 décrit ci-dessus. Tout comme pour les procédés 200a, 200b, il est également possible de définir un paramètre de sécurité dans le procédé 300. Par exemple, un temps écoulé entre deux requêtes pour recevoir un courrier électronique peut être défini afin d'éviter à l'utilisateur de compléter un test lorsque que plusieurs emails sont reçus dans une courte durée. En effet, le procédé 300a peut également comprendre recevoir au niveau du serveur de messagerie électronique 102 une autre requête provenant de l'utilisateur pour envoyer un autre courrier électronique, vérifier un paramètre de sécurité prédéterminé et envoyer le courrier électronique par le serveur si le paramètre de sécurité prédéterminé est satisfait. Par exemple, le paramètre de sécurité peut comprendre un nombre de courriers électroniques, un temps écoulé entre la validation d'un dernier test de sécurité, un comportement suspect de l'utilisateur, et l'envoi d'une nouvelle requête, un changement d'adresse IP utilisée par l'utilisateur depuis la validation d'un dernier test de sécurité et une date à laquelle la requête est envoyée par l'utilisateur.

[0062] Le procédé 300a permet ainsi de s'assurer que le courrier électronique est reçu par la personne à qui il est destiné. Par exemple, si plusieurs utilisateurs utilisent un même appareil (tel qu'un ordinateur), il peut être important de s'assurer que seul un des utilisateurs puisse accéder à sa boite email et à des courriers électroniques confidentiels par exemple. De plus, le procédé 300a permet de s'assurer que l'utilisateur ne reçoit pas des courriers indésirables.

[0063] Il doit être compris que les modes de réalisation de la présente invention peuvent être mis en œuvre par un produit-programme d'ordinateur comprenant des instructions et étant exécuté par un ordinateur. Par exemple, les procédés 200a, 200b, 300a, 300b peuvent être mis en œuvre en utilisant des dispositifs informatiques, un logiciel et/ou une combinaison de ceux-ci. Par exemple, les dispositifs informatiques peuvent être mis en œuvre à l'aide de circuits de traitement tels que, mais sans s'y limiter, un processeur, une unité centrale de traitement (CPU), un contrôleur, une unité arithmétique et logique (ALU), un processeur de signal numérique, un micro-ordinateur, un champ un réseau de portes programmable (FPGA), un système sur puce (SoC), une unité logique programmable, un microprocesseur ou tout autre dispositif capable de répondre et d'exécuter des instructions d'une manière définie. Le logiciel peut inclure un programme informatique, un code de programme, des instructions, ou une combinaison de ceux-ci, pour instruire ou configurer indépendamment ou collectivement un dispositif matériel pour qu'il fonctionne comme souhaité. Le programme informatique et/ou le code de programme peuvent comprendre des instructions de

programme ou lisibles par ordinateur, des composants logiciels, des modules logiciels, des fichiers de données, des structures de données et/ou similaires, pouvant être mis en œuvre par un ou plusieurs dispositifs matériels, tels qu'un ou plus des périphériques matériels mentionnés ci-dessus. Lorsqu'un dispositif matériel est un dispositif de traitement informatique (par exemple, CPU, un contrôleur, une ALU, un processeur de signal numérique, un micro-ordinateur, un microprocesseur, etc.), le dispositif de traitement informatique peut être configuré pour exécuter un code de programme en effectuant des opérations arithmétiques, opérations logiques et d'entrée/sortie, selon le code du programme. L'unité de contrôle 106 peut également comprendre un ou plusieurs dispositifs de stockage. Le ou les dispositifs de stockage peuvent être des supports de stockage lisibles par ordinateur tangibles ou non transitoires, tels qu'une mémoire vive (RAM), une mémoire morte (ROM), un dispositif de stockage de masse permanent (tel qu'un lecteur de disque), un (par exemple, flash NAND) et/ou tout autre mécanisme de stockage de données similaire capable de stocker et d'enregistrer des données. Le ou les dispositifs de stockage peuvent être configurés pour stocker des programmes informatiques, un code de programme, des instructions ou une combinaison de ceux-ci, pour un ou plusieurs systèmes d'exploitation et/ou pour mettre en œuvre les exemples de modes de réalisation décrits ici. Les programmes informatiques, le code de programme, les instructions ou une combinaison de ceux-ci peuvent également être chargés à partir d'un support de stockage lisible par ordinateur séparé dans le ou les dispositifs de stockage et/ou un ou plusieurs dispositifs de traitement informatique à l'aide d'un mécanisme d'entraînement. Un tel support de stockage lisible par ordinateur séparé peut comprendre une clé USB (Universal Serial Bus), une clé mémoire, un lecteur Blu-ray/DVD/CD-ROM, une carte mémoire et/ou d'autres supports de stockage lisibles par ordinateur.

[0064] Bien que l'invention ait été illustrée et décrite en détail à l'aide de modes de réalisations préférés, l'invention n'est pas limitée aux exemples divulgués. D'autres variantes peuvent être déduites par l'homme du métier sans sortir du cadre de protection de l'invention revendiquée. Par exemple, bien que les procédés 200a, 200b et les procédés 300a, 300b aient été décrits séparément, ils peuvent être utilisés par un même système. De plus, bien que l'ordinateur sur lequel l'utilisateur rédige son courrier électronique et l'appareil de confiance aient été décrits comme étant deux dispositifs différents, ils peuvent être un même dispositif.

Revendications

[Revendication 1] Procédé d'envoi sécurisé d'un courrier électronique, le procédé comprenant :
- recevoir au niveau d'un serveur de messagerie électronique une requête provenant d'un utilisateur pour envoyer le courrier électronique, l'utilisateur ayant un compte de messagerie électronique sur le serveur de messagerie électronique, l'utilisateur s'étant préalablement identifié au compte de messagerie électronique ;
- en réponse à la réception de la requête, envoyer par le serveur un test de sécurité à compléter par l'utilisateur à un appareil de confiance associé à l'utilisateur via un canal sécurisé ;
- recevoir le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé ;
- vérifier le test de sécurité complété par l'utilisateur par le serveur ; et
- envoyer le courrier électronique par le serveur si le test est validé par l'utilisateur.

[Revendication 2] Procédé d'envoi sécurisé d'un courrier électronique, le procédé comprenant :
- recevoir, à un appareil de confiance associé à l'utilisateur en réponse à la réception d'une requête de transmission d'un courrier électronique par un serveur, un test de sécurité à compléter par l'utilisateur via un canal sécurisé ;
- compléter le test de sécurité par l'utilisateur sur l'appareil de confiance ;
- transmettre le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé pour validation et transmission du courrier électronique par le serveur si le test est validé par l'utilisateur.

[Revendication 3] Procédé de détection d'une requête pour l'envoi d'un courrier électronique, le procédé comprenant :
- recevoir au niveau d'un serveur de messagerie électronique une requête provenant d'un utilisateur pour envoyer le courrier électronique, l'utilisateur ayant un compte de messagerie électronique sur le serveur de messagerie électronique, l'utilisateur s'étant préalablement identifié au compte de messagerie électronique ;
- en réponse à la réception de la requête, envoyer par le serveur un test de sécurité à compléter par l'utilisateur à un appareil de confiance associé à l'utilisateur via un canal sécurisé ;

- recevoir le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé ;
- vérifier le test de sécurité complété par l'utilisateur par le serveur ; et
- rejeter le courrier électronique ou l'envoyer par le serveur à un autre destinataire que celui précisé dans le message si le test n'est pas validé par l'utilisateur.

[Revendication 4] Procédé d'envoi sécurisé d'un courrier électronique selon la revendication 1, dans lequel le procédé comprend en outre :
- recevoir au niveau du serveur de messagerie électronique une autre requête provenant de l'utilisateur pour envoyer un autre courrier électronique ;
- vérifier un paramètre de sécurité prédéterminé ;
- envoyer le courrier électronique par le serveur si le paramètre de sécurité prédéterminé est satisfait.

[Revendication 5] Procédé d'envoi sécurisé d'un courrier électronique selon la revendication 4, le paramètre de sécurité comprenant : un temps écoulé entre l'envoie de la requête et de l'autre requête, un changement d'adresse IP utilisée par l'utilisateur et une date à laquelle la requête est envoyée par l'utilisateur.

[Revendication 6] Procédé d'envoi sécurisé d'un courrier électronique selon l'une des revendications précédentes, dans lequel le test de sécurité comprend une comparaison d'une entrée biométrique avec des données biométriques associées à l'utilisateur et stockées sur l'appareil de confiance associé à l'utilisateur.

[Revendication 7] Procédé d'envoi sécurisé d'un courrier électronique selon l'une des revendications précédentes, dans lequel l'appareil de confiance associé à l'utilisateur est un téléphone portable ou une clé USB.

[Revendication 8] Procédé d'envoi sécurisé d'un courrier électronique selon l'une des revendications précédentes, dans lequel l'appareil de confiance comprend une application permettant de compléter le test de sécurité.

[Revendication 9] Produit-programme d'ordinateur comprenant des instructions qui, lorsque le programme est exécuté par un ordinateur, amènent l'ordinateur à mettre en œuvre le procédé de l'une quelconque des revendications précédentes.

[Revendication 10] Un serveur permettant l'envoi sécurisé d'un courrier électronique, le serveur étant configuré pour mettre en œuvre le procédé de la revendication 1.

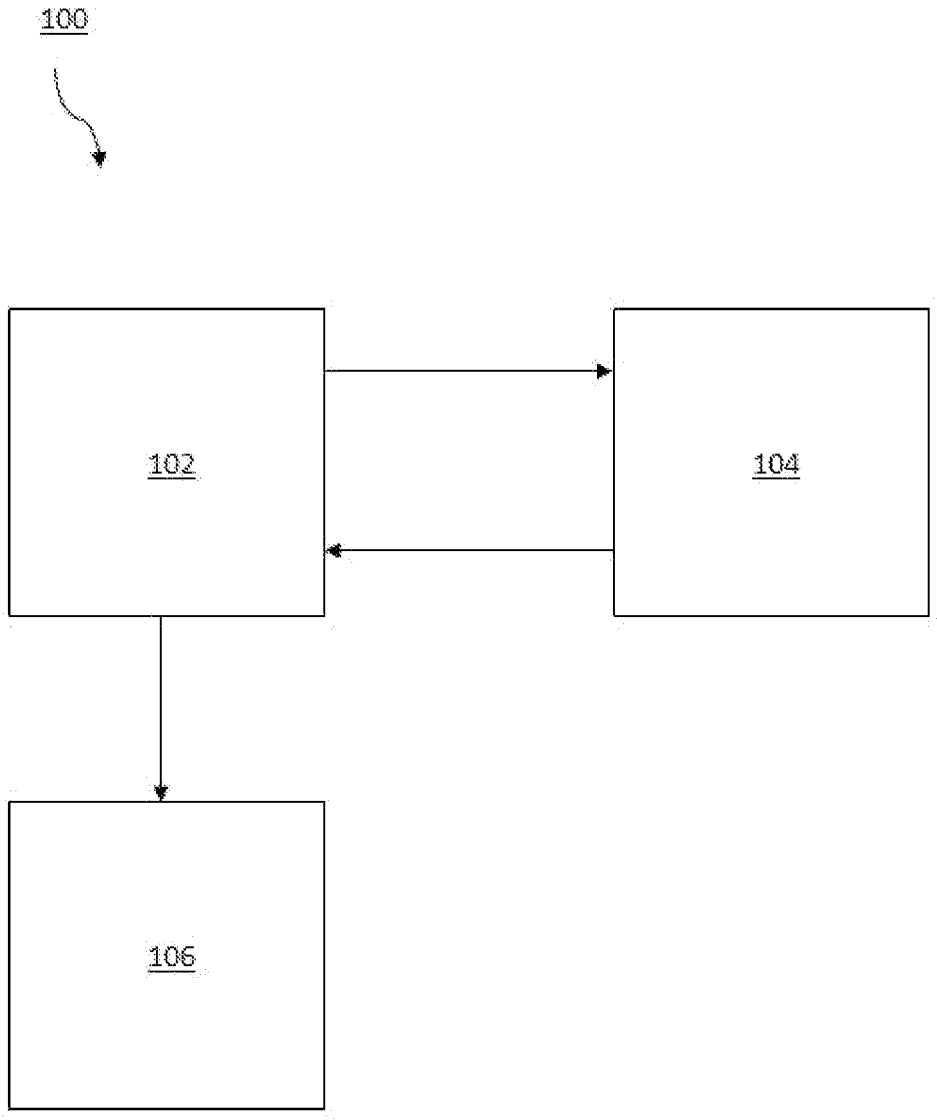
[Revendication 11] Un appareil de confiance permettant l'envoi sécurisé d'un courrier élec-

tronique, l'appareil de confiance étant configuré pour mettre en œuvre le procédé de la revendication 2.

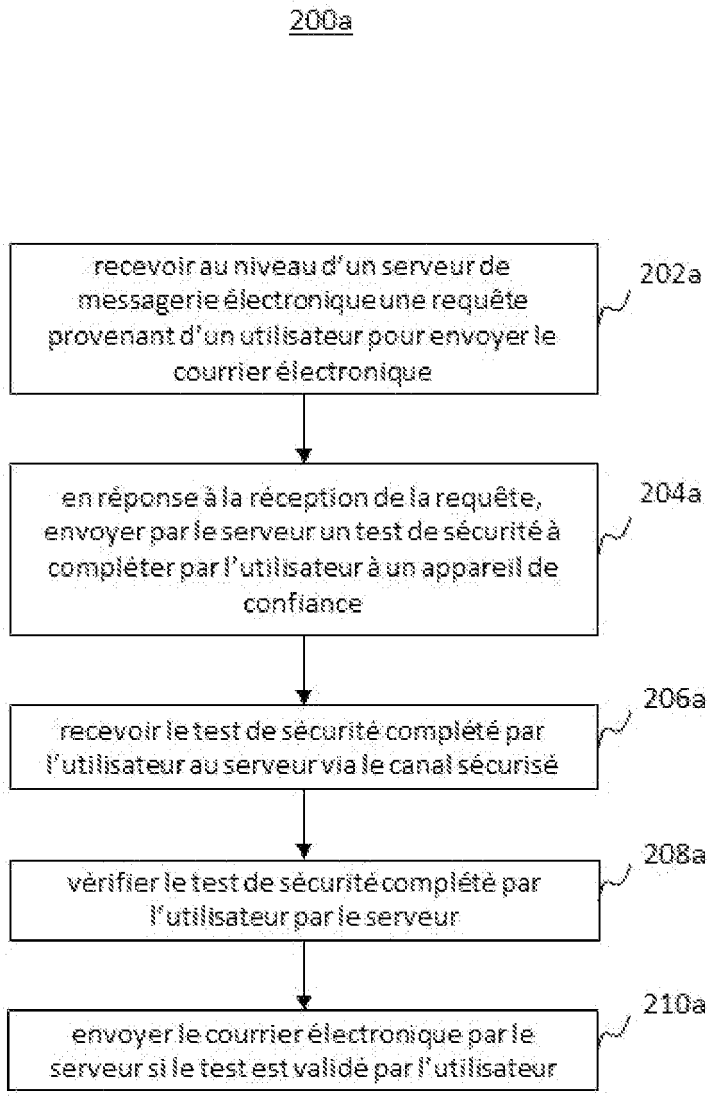
[Revendication 12] Procédé de réception sécurisée d'un courrier électronique par un utilisateur, le procédé comprenant :
- recevoir au niveau d'un serveur de messagerie électronique une requête pour recevoir le courrier électronique, l'utilisateur ayant un compte de messagerie électronique sur le serveur de messagerie électronique, l'utilisateur s'étant préalablement identifié au compte de messagerie électronique ;
- en réponse à la réception de la requête, envoyer par le serveur un test de sécurité à compléter par l'utilisateur à un appareil de confiance associé à l'utilisateur via un canal sécurisé ;
- recevoir le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé ;
- vérifier le test de sécurité complété par l'utilisateur par le serveur ;
- recevoir le courrier électronique par le serveur ; et
- envoyer le courrier électronique par le serveur à l'utilisateur si le test est validé par l'utilisateur.

[Revendication 13] Procédé de réception sécurisée d'un courrier électronique par un utilisateur, le procédé comprenant :
- recevoir, à un appareil de confiance associé à l'utilisateur, en réponse à la réception d'une requête de réception d'un courrier électronique par un serveur, un test de sécurité à compléter par l'utilisateur via un canal sécurisé ; et
- compléter le test de sécurité par l'utilisateur sur l'appareil de confiance ;
- transmettre le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé pour validation et transmission du courrier à l'utilisateur par le serveur si le test est validé par l'utilisateur.

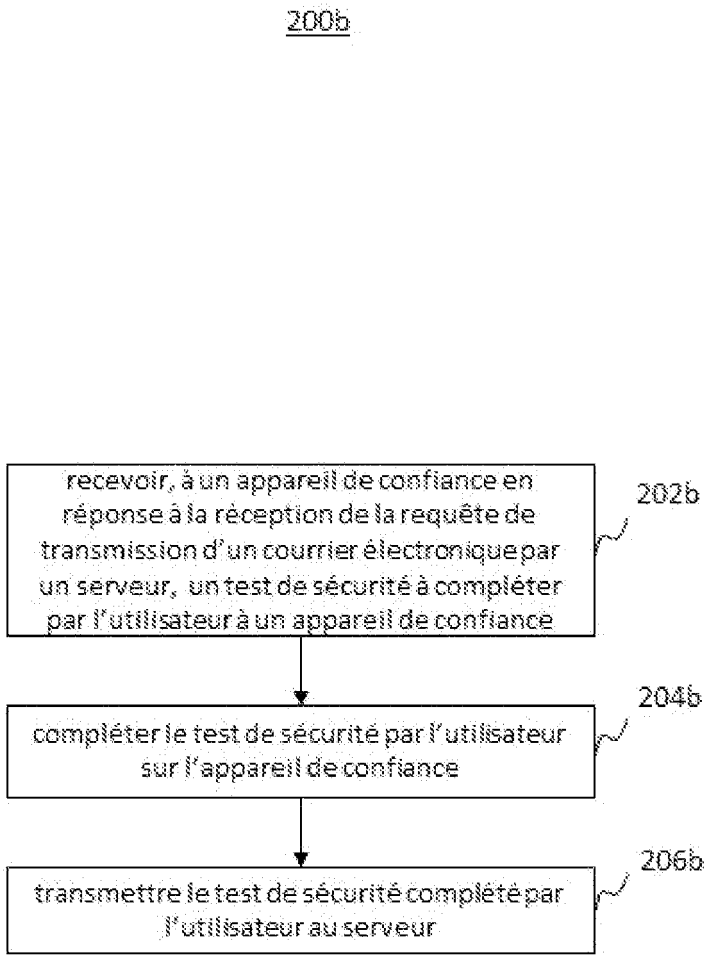
[Fig. 1]



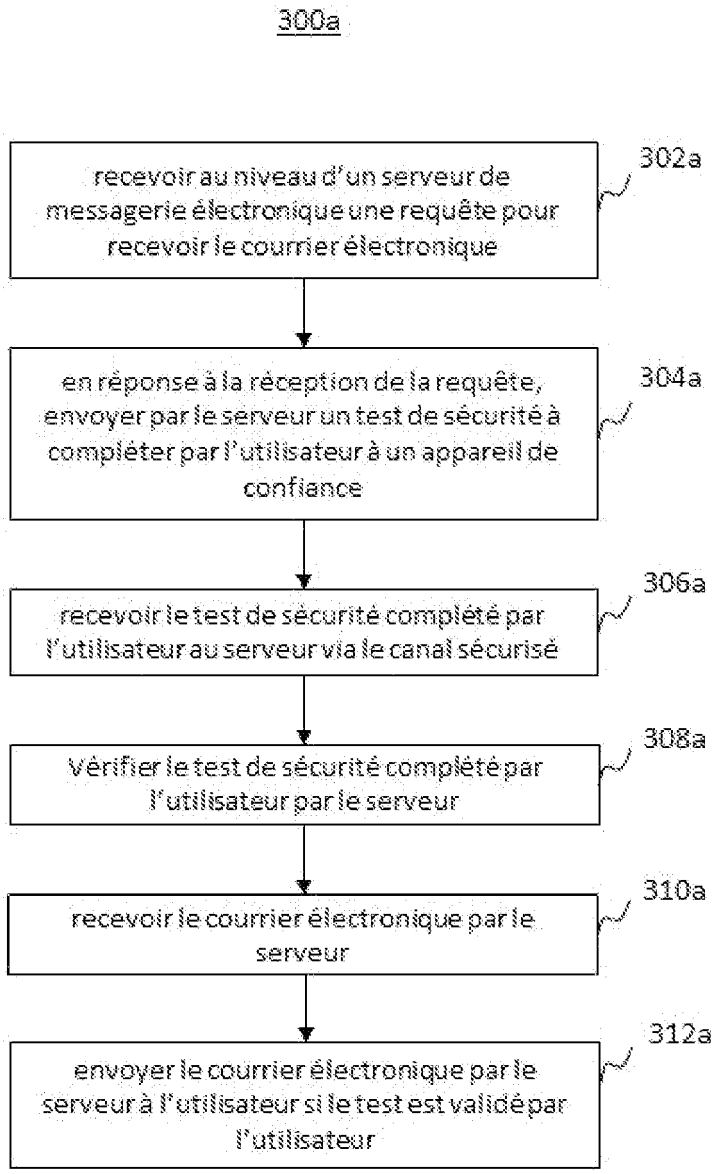
[Fig. 2a]


200a
recevoir au niveau d'un serveur de messagerie électronique une requête provenant d'un utilisateur pour envoyer le courrier électronique
202a
en réponse à la réception de la requête, envoyer par le serveur un test de sécurité à compléter par l'utilisateur à un appareil de confiance
204a
recevoir le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé
206a
vérifier le test de sécurité complété par l'utilisateur par le serveur
208a
envoyer le courrier électronique par le serveur si le test est validé par l'utilisateur
210a

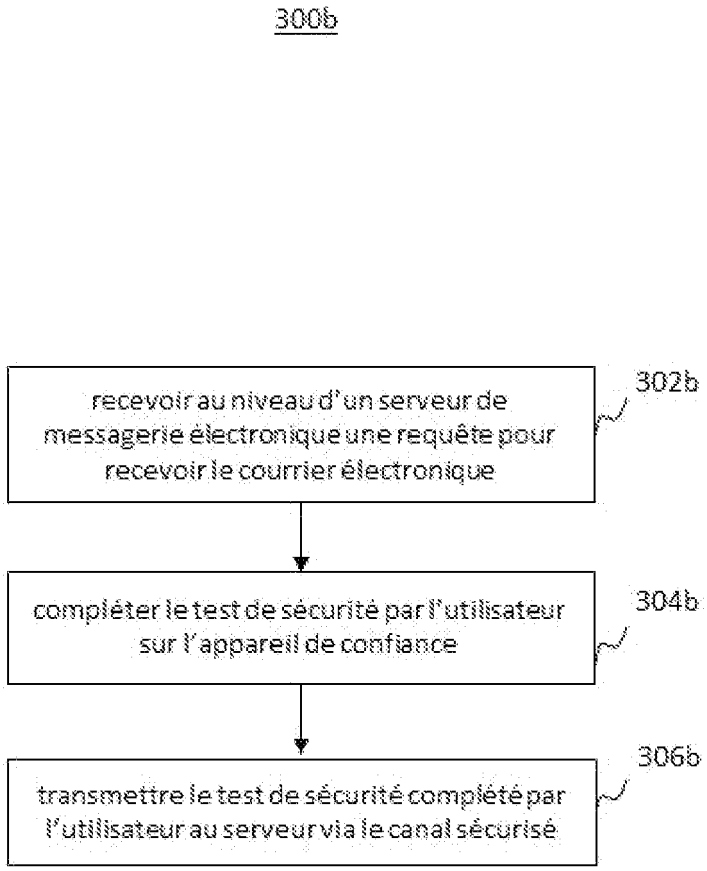
[Fig. 2b]


200b
recevoir, à un appareil de confiance en réponse à la réception de la requête de transmission d'un courrier électronique par un serveur, un test de sécurité à compléter par l'utilisateur à un appareil de confiance
202b
compléter le test de sécurité par l'utilisateur sur l'appareil de confiance
204b
transmettre le test de sécurité complété par l'utilisateur au serveur
206b

[Fig. 3a]


300a
recevoir au niveau d'un serveur de messagerie électronique une requête pour recevoir le courrier électronique
302a
en réponse à la réception de la requête, envoyer par le serveur un test de sécurité à compléter par l'utilisateur à un appareil de confiance
304a
recevoir le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé
306a
Vérifier le test de sécurité complété par l'utilisateur par le serveur
308a
recevoir le courrier électronique par le serveur
310a
envoyer le courrier électronique par le serveur à l'utilisateur si le test est validé par l'utilisateur
312a

[Fig. 3b]


300b
recevoir au niveau d'un serveur de messagerie électronique une requête pour recevoir le courrier électronique
302b
compléter le test de sécurité par l'utilisateur sur l'appareil de confiance
304b
transmettre le test de sécurité complété par l'utilisateur au serveur via le canal sécurisé
306b

RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

[x] Le demandeur a maintenu les revendications.

☐ Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

☐ Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

[x] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

NEANT

2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

US 2020/336451 A1 (JAKOBSSON BJORN MARKUS [US]) 22 octobre 2020 (2020-10-22)

US 2021/184851 A1 (BLYTHE SIMON [GB]) 17 juin 2021 (2021-06-17)

CN 109 039 860 B (BEIJING XIAOMI MOBILE SOFTWARE CO LTD) 30 juillet 2021 (2021-07-30)

3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT