SPF Economie, PME, Classes
Moyennes & Energie
Office de la Propriété intellectuelle

(11) 1027121 A1

(12) DEMANDE DE BREVET D'INVENTION BELGE

(41) Date de publication : 07/10/2020

(21) Numéro de demande : BE2019/5160

(22) Date de dépôt : 15/03/2019

(62) Divisée de la demande de base :

(62) Date de dépôt demande de base :

(51) Classification internationale : G07C 13/00

(30) Données de priorité :

(71) Demandeur(s) :

DUTORDOIR Christophe

1180, BRUXELLES
Belgique

(72) Inventeur(s) :

DUTORDOIR Christophe
1180 BRUXELLES
Belgique

(54) Système de vote électronique sur internet

(57)L'invention concerne un système de vote par internet comprenant un mot de passe de vote à utiliser par l'électeur pour accéder au dit vote. Un mot de passe de vérification demandé par le système est introduit par l'électeur, ledit mot de passe de vérification, joint à un paramètre non confidentiel propre à l'électeur (par exemple numéro de registre national), servant à créer un nom de fichier construit avec une fonction SHA-256 ou équivalente. Ce fichier reprend en clair (non crypté) le contenu du vote et est accessible par l'électeur sur un site de vérification en introduisant le paramètre non confidentiel et son mot de passe de vérification.

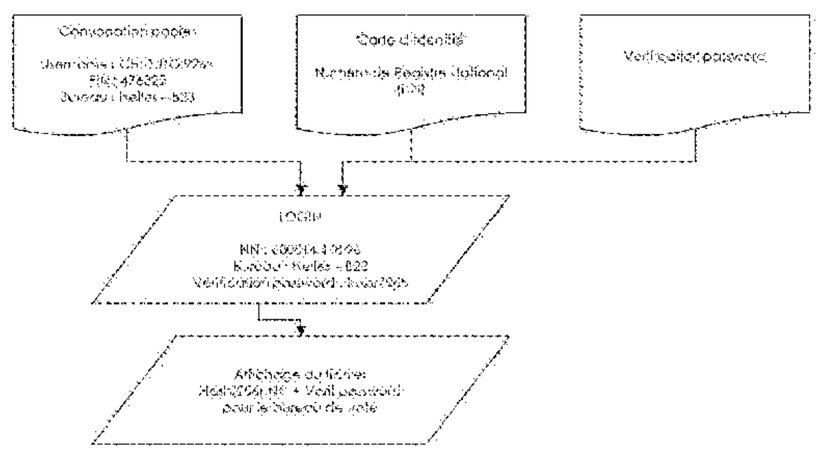

FIG. 3

Système de vote électronique sur internet

Le vote sur internet intéresse les divers intervenants des scrutins électoraux sur la planète entière, et cela depuis de nombreuses années.

Le vote par internet comporte en effet de nombreux avantages :

Pour l'électeur :

- Liberté du lieu et du moment du vote (pendant la durée de l'élection)
- Pas de nécessité de déplacement
- Pas de souci d'inconfort, ou de sécurité
- Pas de solution à trouver pour compenser l'absence de l'électeur (garde d'enfant, de personnes âgées, occupation professionnelle, …)
- …

Pour les organisateurs :

- Pas – ou moins - de mise en place de bureaux de vote
- Pas – ou moins - de ressources à trouver : présidents, assesseurs, forces de l'ordre, huissiers, …
- Elimination ou diminution de la charge de travail, de l'aspect fastidieux du dépouillement
- Elimination du risque d'erreur, d'invalidité ou de fraude
- Facilité de la transmission des résultats du vote, et de leur publication
- Diminution des coûts liés à l'organisation
- …

Malheureusement, les expériences mises en place dans de nombreux pays jusqu'à présent se sont soldées par des échecs. Souvent pour des raisons techniques, mais plus encore à cause d'un manque de confiance en ces systèmes de vote électronique que beaucoup perçoivent comme une insondable « boite noire », exposée à toutes les manipulations. De nombreux candidats, partis politiques et électeurs ne se sont pas cachés du sentiment de défiance que leur inspire ces systèmes.

La présente invention propose un système qui concilie à la fois les avantages évidents décrits ci-dessus, avec une transparence complète, une capacité à vérifier l'enregistrement des votes, tout en ne compromettant pas l'indispensable confidentialité attachée au vote. On comprendra que système peut s'appliquer à des situations autres que celles des scrutins électoraux.

ART ANTERIEUR

On décrit ci-dessous trois exemples de système de vote « reconnus », et les améliorations visées par le système selon l'invention.

V² Secure®

Election-Europe (https://www.election-europe.com) se présente comme le leader européen de l'organisation des élections professionnelles et publiques.

Cette société utilise un système de vote en ligne breveté, V² Secure®, décrit comme le premier système mondial de « vote vérifiable sécurisé ».

En pratique, ce système donne la possibilité à l'électeur de voir un « reflet éphémère » (selon leurs propres termes) de son vote, alors que celui-ci est en attente de confirmation

dans l'urne électronique. Un fois ce vote validé, l'utilisateur ne pourra plus retrouver son bulletin de vote. Il va de soi que ce système ouvre la porte à de nombreuses manipulations et n'est en tout cas pas à même de réinstaurer la confiance de l'électeur dans le vote électronique par internet.

A la différence de V² Secure®, le système de l'invention permet de vérifier son bulletin de vote à n'importe quel moment, et ce directement à la source du choix de l'électeur, comme par exemple parmi les bulletins distribués aux observateurs.

Scytl

Scytl se définit comme le « leader mondial du vote électronique ». Cette société est, par exemple, la sous-traitante du moment de l'ECES (European Center for Electoral Support). La méthodologie de Scytl comporte 3 désavantages importants par rapport à notre système de vote :

1. L'usage impératif de certificats numériques, encryptés par un système de clefs : complexes d'utilisation, les certificats numériques n'apportent pas un d'avantage réel en termes de sécurisation. Tous les systèmes de gestion bancaire par internet ont abandonné cette voie
2. Le système envoie à l'électeur un lien vers son bulletin de vote, preuve que ce lien (entre électeur et bulletin) existe bien !
3. Seul le « mélange des bulletins » en fin de parcours, ne permet plus le lien entre l'électeur et son bulletin.

Belenios

Belenios est un système de vote sur internet développé par l'INRIA (Institut National de Recherche en Sciences Numériques), en partenariat avec le CNRS.

Dans ce système, le vote est encrypté à l'aide d'une clef publique. Un numéro de suivi (tracking number) est ensuite envoyé à l'électeur, lui permettant de vérifier que son vote se trouve bien dans l'urne électronique. En pratique, cela signifie que le numéro de suivi est stocké par le système, et donc, que la relation peut être établie entre un électeur et son vote !

Le système de la présente invention, en revanche, est :

- sécurisé par SSL (comme les banques en ligne)
- ne nécessite pas de certificat numérique, ni de clef publiques ou privées
- ne stocke jamais le lien entre la fiche de l'électeur et son bulletin de vote
- permet la distribution des bulletins de vote entièrement dépersonnalisés au plus grand nombre (observateurs)
- permet la vérification par l'électeur de son propre bulletin de vote, d'où il veut, quand il veut, en s'alimentant à la source de son choix

EXPOSE DE L'INVENTION

Le processus de scrutin proposé débute de manière connue et classique, par une convocation à participer à l'élection sur base d'une liste électorale.

Il est entendu que la partie convocation - inscription décrite ici ne fait pas partie de la présente invention. Elle décrit un cas de figure possible, réunissant des critères de sécurité optimale, mais peut bien sûr être modifiée en fonction des desiderata ou des nécessités particulières de certains scrutins (dispositions légales, ou simplification, par exemple).

La présente invention concerne en effet le processus de scrutin au moment du vote proprement dit, ainsi qu'après le vote (vérification - publication des résultats).

A titre d'exemple les étapes suivantes sont réalisées de manière connue ou non inventive, en début de procédure.

1. Convocation

Une convocation papier est envoyée à l'électeur, contenant son nom d'utilisateur, son code PIN, et le bureau dans lequel il est appelé à voter.

===== Exemple ==========

Nom d'utilisateur : CH.DUTO.9267
PIN code : 476325
Bureau de vote : Ixelles 23

==========

2. Inscription

Muni de ces informations, ainsi que de sa carte d'identité, l'électeur se rend ensuite sur le site web du vote, également renseigné sur la convocation, afin de s'y inscrire. Il se connecte sur le site en entrant les paramètres suivants :

===== Exemple ==========

Nom d'utilisateur : CH.DUTO.9267
PIN code : 476325
Numéro de Reg. Nat. : 680814.478.96

| Envoyer |

==========

Il est demandé ensuite d'entrer l'adresse e-mail qu'il désire utiliser pour le vote :

===== Exemple ==========

Adresse e-mail : ch.duto@gmail.com

Confirmation : ch.duto@gmail.com

| Envoyer |

==========

Ce qui a pour effet de lui envoyer, dans sa boite e-mail, son mot de passe de vote :

===== Exemple ==========

Voici le mot de passe à utiliser pour les élections xxx du jj/mm/aaaa :

5Gt7e9K3Fp46

==========

Vote

Durant la période du vote, l'électeur est appelé à se

rendre sur le site web, muni de sa convocation, de sa carte d'identité, ainsi que de l'e-mail contenant son mot de passe de vote :

===== Exemple ==========

Nom d'utilisateur : CH.DUTO.9267

Numéro de Reg. Nat. : 680814.478.96

Mot de passe de vote : 5Gt7e9K3Fp46

| Envoyer |

==========

Les différentes listes ou propositions de vote lui sont présentées sur l'écran. L'électeur les remplit, exprimant ainsi son choix électoral.

PARTICULARITES DE L'INVENTION :

Avant de soumettre son vote, le système demande à l'électeur d'entrer un mot de passe de vérification, connu de lui seul. Ce mot de passe ne sera pas enregistré dans la base de données du vote.

===== Exemple ==========

Récapitulatif de votre choix :

Liste X

Candidat A

Candidat B

Candidat C

…

Veuillez entrer votre mot de passe de vérification :

louxor76.78

(ce mot de passe ne sera pas enregistré par le système)

| Modifier le vote | | Enregistrer le vote |

==========

Le mot de passe est entré, et validé. Le vote est soumis au système, ce qui aura deux conséquences :

- D'une part, dans la base de données, le statut de l'électeur passe à « a voté », sans que l'heure précise du vote ne soit inscrite, rendant impossible toute corrélation entre les bulletins de vote et les informations contenues dans la base de données des électeurs
- D'autre part, un fichier sera créé, reprenant « en clair » le contenu du vote. Ce fichier sera envoyé dans le répertoire correspondant au bureau de vote. Le nom de ce fichier sera construit avec une fonction SHA-256, constitué sur base du Numéro de registre national de l'électeur, ainsi que de son mot de passe de vérification.

3 exemples de noms de fichiers :

-
732210b19c8998853557e94a996790ffc38f3b851324e2405b7e09
05c6e2cf10.txt
-

16c8fb7e6291d2d109952742967394d284a65fb88a926212ce24b3
01382e9e4.txt
-
ed2456914e48c1e17b7bd922177291ef8b7f553edf1b1f66b6fc1a
076524b22f.txt

3. Vérification

Une fois son vote validé, l'électeur – et lui seul – aura la possibilité de vérifier que son bulletin de vote aura été correctement entré dans le système. Pour ce faire, il se rendra sur le site de vérification, introduira son bureau de vote, son numéro de registre national et son mot de passe de vérification.

===== Exemple ==========

Bureau de vote : Ixelles 23
Numéro de Reg. Nat. : 680814.478.96
Mot de passe de vérification : louxor76.78

| Envoyer |

==========

Ceci aura pour effet de lui afficher son bulletin de vote :

===== Exemple ==========

Liste X
Candidat A

Candidat B

Candidat C

==========

Afin de respecter toujours la confidentialité du vote, le serveur permettant la vérification du vote n'inscrira pas les paramètres de recherche dans ses fichiers d'évènements (log files).

4. Publication des résultats

Lors de la création du bulletin de vote, les résultats intermédiaires seront mis à jour en temps réel (ou en léger différé, toujours pour assurer la confidentialité du vote). Nous obtiendrons ainsi un dépouillement en temps réel. Libre aux administrateurs de l'élection de diffuser ces informations immédiatement, ou bien en différé - afin de se conformer aux dispositions légales en vigueur.

Un autre avantage de ce système de scrutin selon l'invention consiste en la possibilité d'envoyer, en temps réel ou en différé, une copie de tous les bulletins de vote vers les serveurs d'observateurs dument référencés. Ces observateurs pourraient être, par exemple :

- Des partis politiques, tant de la majorité que de l'opposition
- Des observateurs indépendants
- Des autorités gouvernementales
- Des médias

Ceux-ci auront ainsi tout loisir d'effectuer les

comptages qu'ils désirent, validant pour leur propre compte les chiffres annoncés par le système de vote.

Le nombre de ces observateurs recevant une copie de l'ensemble des bulletins de vote sera limité par d'évidentes contraintes techniques. 1 million de votes représente 1 million de fichiers, d'une taille minimale sur disque dur de généralement de 4.096 octets, soit 4 Gigabytes d'informations. Cette taille restant malgré tout raisonnable, elle permettra l'envoi des bulletins de vote à suffisamment d'acteurs que pour assurer la pluralité des vérifications, et restaurer la confiance de tous dans l'intégrité du processus électoral.

Le transfert des bulletins de vote vers les serveurs des observateurs pourra être assuré via un VPN, ou de services Cloud tels que Dropbox, OneDrive ou Google Drive. Encore une fois, ces fichiers étant dépersonnalisés, ils ne posent pas de problème de sécurité.

Le système selon l'invention réunit donc bien, pour la première fois, les critères essentiels du vote démocratique, à savoir :

- Le secret absolu du vote
- La possibilité pour le votant et lui seul de vérifier son vote
- La possibilité pour « tous » de vérifier l'ensemble de bulletins de vote, et de procéder à tout recomptage souhaité

Un grand avantage du présent système est sa simplicité. L'électeur se connecte au site de vote directement depuis

son navigateur internet via une connexion sécurisée (SSL), mais sans programme à installer, code java, calculette, infrastructure clef publique / clef privée ou autres certificats de sécurité.

L'invention sera davantage comprise à l'examen des diagrammes de blocs annexé.

La Fig. 1 illustre un exemple de processus d'inscription.

La Fig. 2 illustre un exemple du processus de vote.

La Fig. 3 illustre un exemple du processus de vérification selon l'invention.

La Fig. 4 illustre un exemple de publication des résultats.

Notons enfin concernant l'exemple illustré que le même système peut être utilisé dans l'isoloir, pour peu que celui-ci soit équipé d'un ordinateur avec une connexion à internet, ainsi que d'un navigateur internet.

En résumé l'invention concerne un système de vote par internet comprenant un mot de passe de vote à utiliser par l'utilisateur pour accéder au dit moyen de vote dans lequel un mot de passe de vérification demandé par le système est introduit par l'utilisateur. Ledit mot de passe de vérification, joint à un paramètre non confidentiel propre à l'électeur (par exemple numéro de registre national), sert à créer un nom de fichier construit avec une fonction cryptographique par exemple du type SHA-256 ou une fonction de hachage analogue, ledit fichier reprenant en clair (non crypté) le contenu du vote et étant accessible par l'utilisateur sur un site de vérification en introduisant ledit paramètre non confidentiel et son mot de passe de vérification.

On comprendra par ailleurs que le vote peut concerner un scrutin électoral (fédéral, européen, national, régional, municipal, communal, ...), l'élection de dirigeants

d'associations, de groupements, de sociétés, de syndicats, de clubs, le vote pour des candidats à des concours (personnes, produits, services, ...), le vote pour l'expression d'opinions politiques ou sociétales (votations, consultations, RIC, référendum, ...)

On comprendra aussi que l'encodage du nom de fichier peut se faire, non pas sur base d'un paramètre non-confidentiel et un mot de passe de vérification, mais bien sur deux paramètres confidentiels - par exemple deux mots de passe, ou encore un seul mot de passe - mais dont on devra, dans ce cas, s'assurer de l'unicité.

L'intérêt de cette disposition est un éventuel surcroît de confiance dans le système puisqu'aucun paramètre permettant d'identifier l'utilisateur n'est donné. Dans le système de base, on s'engage à ce que ces données ne soient pas conservées, ni au moment du vote, ni lors d'une vérification, mais encore faut-il que l'utilisateur ait confiance dans le respect de cette disposition. Ici, plus rien ne lie objectivement l'électeur à ses paramètres, surtout pour la vérification.

REVENDICATIONS

1. Système de vote par internet comprenant un mot de passe de vote à utiliser par l'électeur pour accéder au dit vote caractérisé en ce qu'un mot de passe de vérification demandé par le système est introduit par l'électeur, ledit mot de passe de vérification, joint à un paramètre non confidentiel propre à l'électeur (par exemple numéro de registre national , servant à créer un nom de fichier construit avec une fonction SHA-256 ou avec n'importe quelle autre fonction de hachage cryptographique (par exemple MD5, SHA-1, SHA-2, ...), ledit fichier reprenant en clair (non crypté) le contenu du vote et étant accessible par l'électeur sur un site de vérification en introduisant ledit paramètre non confidentiel et son mot de passe de vérification.

2. Système selon la revendication 1 dans lequel la base de données des votes ne comprend pas l'heure précise du vote.

3. Système selon la revendication 1 ou 2 dans lequel il y a plusieurs bureaux de vote et le fichier est envoyé dans le répertoire correspondant au bureau de vote de l'électeur.

4. Système selon n'importe laquelle des revendications précédentes dans lequel le serveur permettant la vérification du vote n'inscrit pas les paramètres de recherche dans ses fichiers d'évènements (log file).

5. Système selon n'importe laquelle des revendications précédentes dans lequel les résultats intermédiaires sont mis à jour en temps réel, permettant ainsi un dépouillement en temps réel (et diffusé tel quel ou en différé).

6. Système selon n'importe lequel des revendications précédentes dans lequel une copie de tous les fichiers comportant les votes en clair est envoyée en temps réel ou en différé vers des serveurs d'observateurs dûment référencés.

7. Système selon n'importe lesquelles des revendications précédentes, utilisé dans un isoloir d'un bureau de vote.

8. Système de vote par internet comprenant un mot de passe de vote à utiliser par l'électeur pour accéder au dit vote caractérisé en ce que deux paramètres confidentiels constitués par exemple de deux mots de passe ou d'un seul mot de passe mais dont on devra, dans ce dernier cas, s'assurer de l'unicité, servent à créer un nom de fichier construit avec une fonction SHA-256 ou avec n'importe quelle autre fonction de hachage cryptographique (par exemple MD5, SHA-1, SHA-2, ...), ledit fichier reprenant en clair (non crypté) le contenu du vote et étant accessible par l'électeur sur un site de vérification en introduisant ledit paramètre non confidentiel et son mot de passe de vérification.

9. Système selon la revendication 8 incorporant les caractéristiques des revendications 2 à 7.

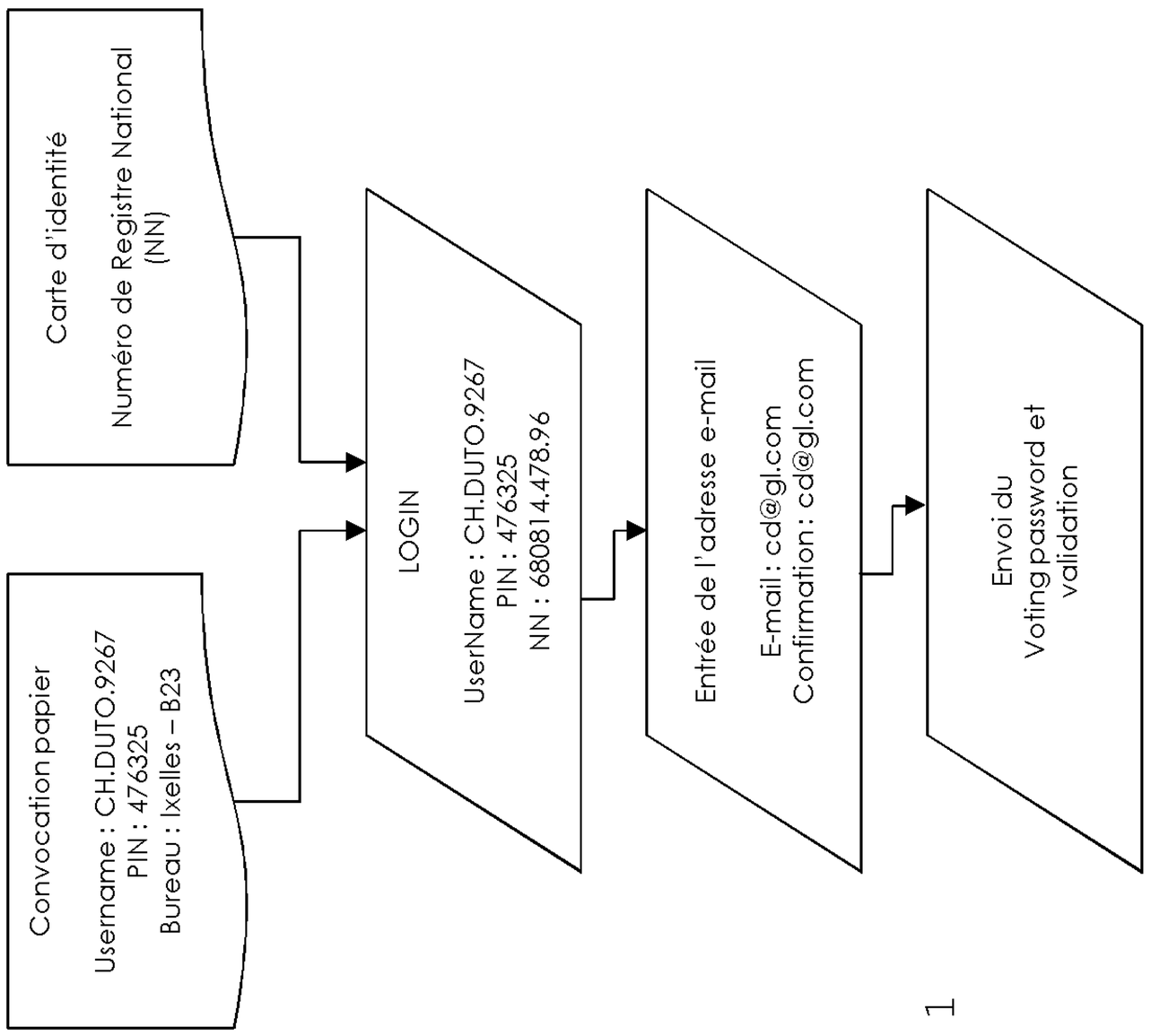
Carte d'identité
Numéro de Registre National
(NN)
Convocation papier
Username : CH.DUTO.9267
PIN : 476325
Bureau : Ixelles – B23
LOGIN
UserName : CH.DUTO.9267
PIN : 476325
NN : 680814.478.96
Entrée de l'adresse e-mail
E-mail : cd@gl.com
Confirmation : cd@gl.com
Envoi du
Voting password et
validation

FIG. 1

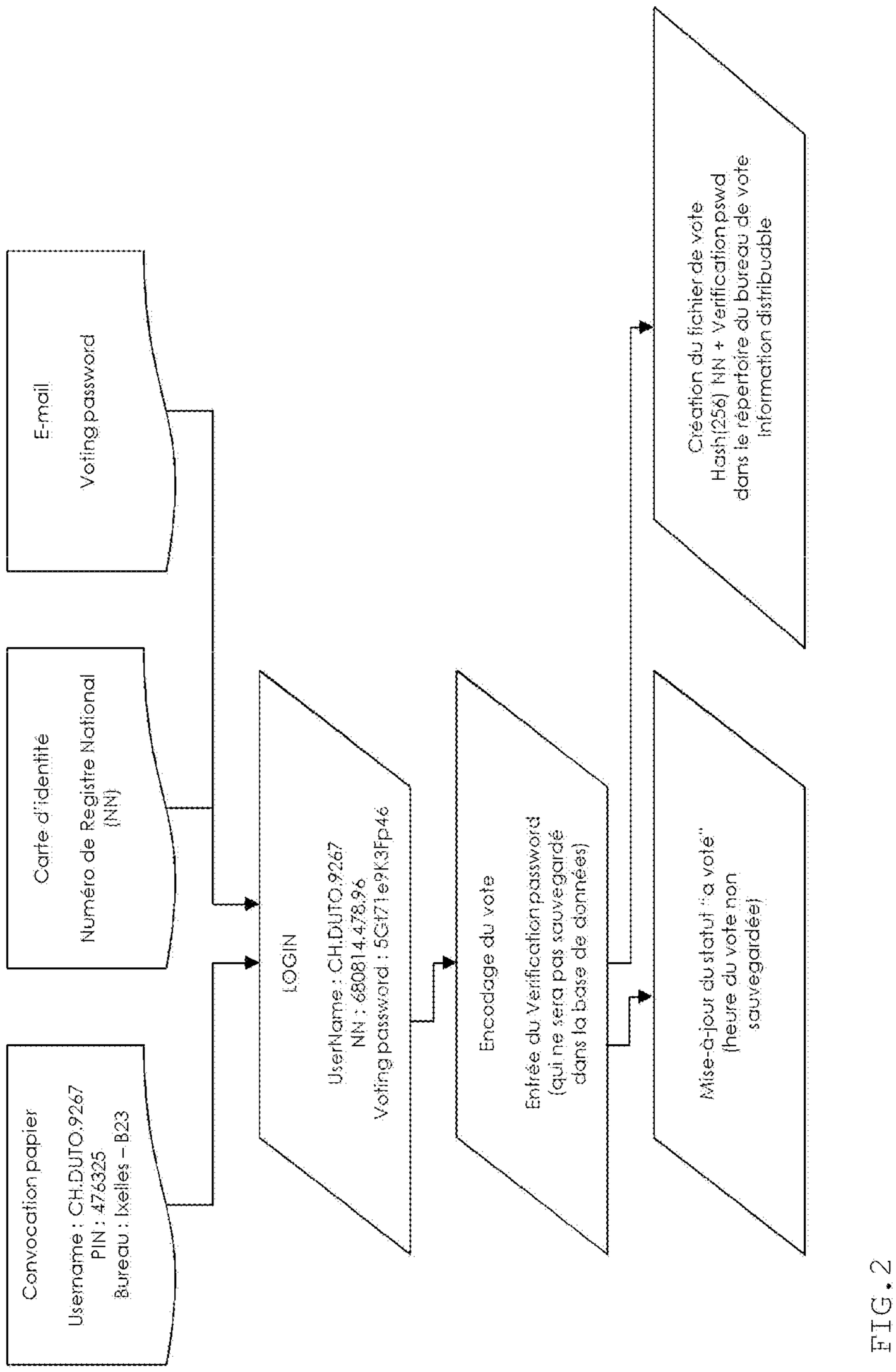
Convocation papier
Username : CH.DUTO.9267
PIN : 476325
Bureau : Ixelles – B23
Carte d'identité
Numéro de Registre National (NN)
E-mail
Voting password
LOGIN
UserName : CH.DUTO.9267
NN : 680814.478.96
Voting password : 5Gt71eRK3Fp46
Encodage du vote
Entrée du Verification password (qui ne sera pas sauvegardé dans la base de données)
Mise-à-jour du statut "a voté" (heure du vote non sauvegardée)
Création du fichier de vote
Hash(256) NN + Verification pswd
dans le répertoire du bureau de vote
Information distribuable

FIG.2

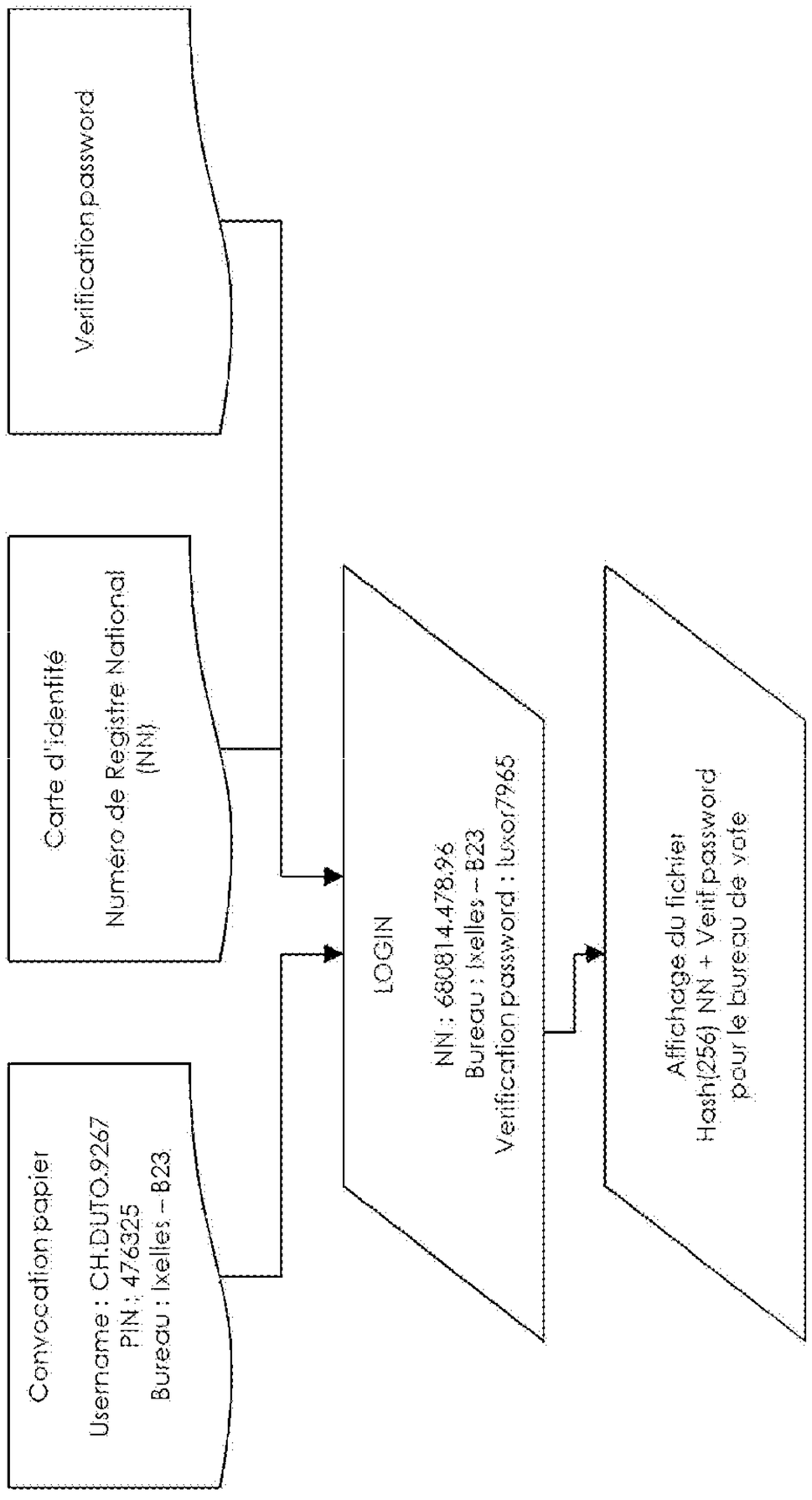
Verification password
Carte d'identité
Numéro de Registre National
(NN)
Convocation papier
Username : CH.DUTO.9267
PIN : 476325
Bureau : Ixelles – B23
LOGIN
NN : 680814.478.96
Bureau : Ixelles – B23
Verification password : luxor7965
Affichage du fichier
Hash(256) NN + Verif password
pour le bureau de vote

FIG. 3

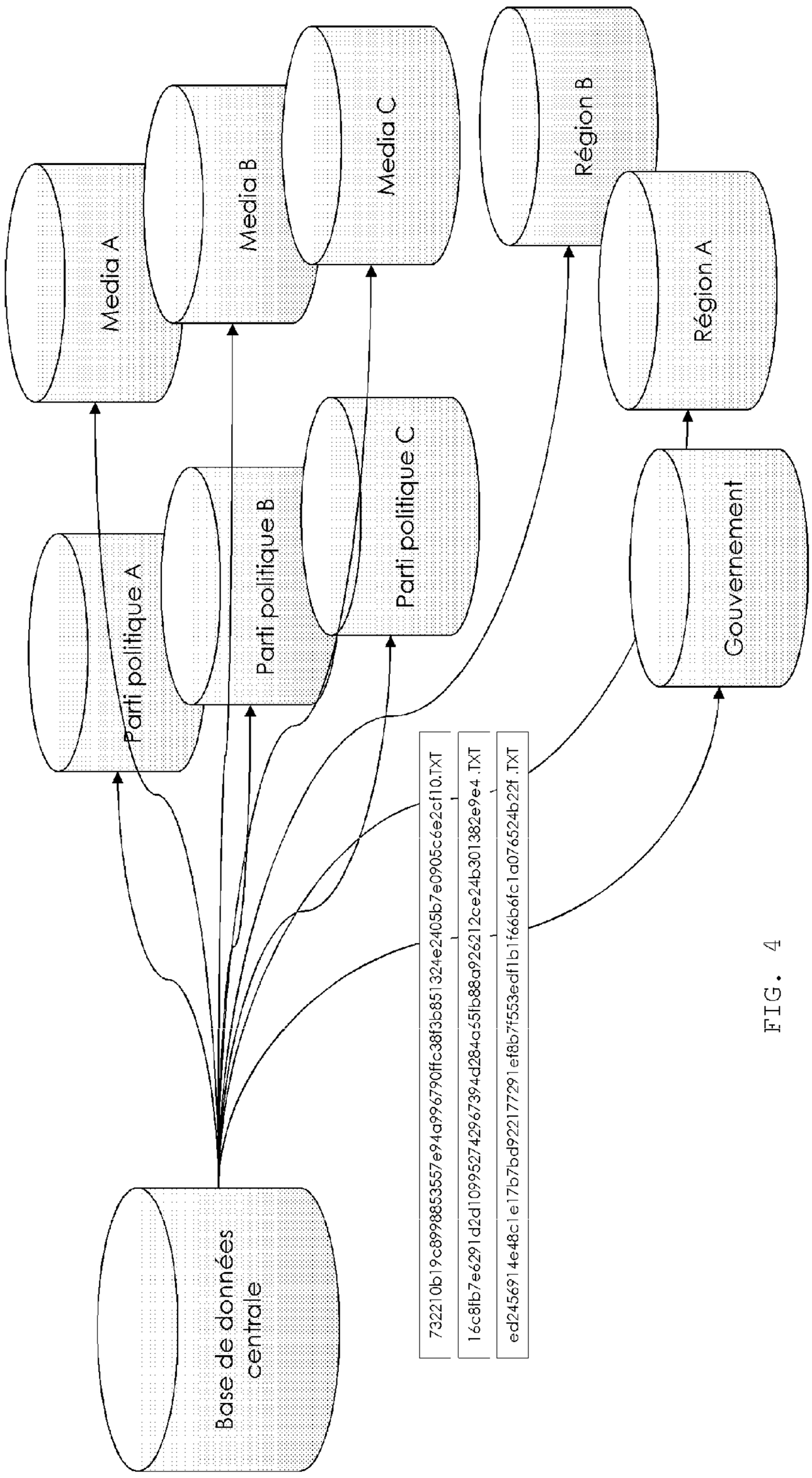
Media A
Media B
Media C
Région B
Région A
Parti politique A
Parti politique B
Parti politique C
Gouvernement
Base de données centrale
732210b19c8998853557e94a996790ffc38f3b851324e2405b7e0905c6e2cf10.TXT
16c8fb7e6291d2d1099527429673 94d284a65fb88a926212ce24b301382e9e4 .TXT
ed245694e48c1e17b7bd922177291ef8b7f553edf1b1f66b6fc1a076524b22f .TXT

FIG. 4

TRAITE DE COOPERATION EN MATIERE DE BREVETS

RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL ÉTABLI EN VERTU DE L'ARTICLE XI.23., §10 DU CODE DE DROIT ÉCONOMIQUE BELGE

IDENTIFICATION DE LA DEMANDE INTERNATIONALE	REFERENCE DU DEPOSANT OU DU MANDATAIRE **B49880b**
Demande nationale belge n° **201905160**	Date du dépôt **15-03-2019**
	Date de priorité revendiquée
Déposant (Nom) **DUTORDOIR Christophe**	
Date de la requête d'une recherche de type international **06-04-2019**	Numéro attribué par l'administration chargée de la recherche internationale à la requête d'une recherche de type international **SN73339**

I. CLASSEMENT DE L'OBJET DE LA DEMANDE (en cas de plusieurs symboles de la classification, les indiquer tous)

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

G07C13/00

II. DOMAINES RECHERCHES

Documentation minimale consultée

Système de classification	Symboles de la classification
IPC	**G07C:G06F;H04L**

Documentation consultée autre que la documentation minimale dans la mesure où ces documents fort partie des domaines consultés

III. ☐ **IL A ETE ESTIME QUE CERTAINES REVENDICATIONS NE POUVAIENT FAIRE L'OBJET D'UNE RECHERCHE** (Observations sur la feuille supplémentaire)

IV. ☐ **ABSENCE D'UNITE DE L'INVENTION ET/OU CONSTATATION RELATIVE A L'ETENDUE DE LA RECHERCHE** (Observations sur la feuille supplémentaire)

RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL

Demande de recherche No
BE 201905160

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G07C13/00
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G07C G06F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 2008/065349 A1 (IRVINE DAVID [GB]) 5 juin 2008 (2008-06-05) * page 30 - page 31 * -----	1-9
X	US 2010/025466 A1 (CARDONE RICHARD J [US] ET AL) 4 février 2010 (2010-02-04) * figure 13D * * alinéa [0161] - alinéa [0166] * -----	1-9
A	FR 2 912 520 A1 (STG INTERACTIVE SA [FR]) 15 août 2008 (2008-08-15) * revendication 1 * -----	1-9

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"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

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche de type international a été effectivement achevée	Date d'expédition du rapport de recherche de type international
31 octobre 2019	

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hniene, Badr

Formulaire PCT/ISA/201 (deuxième feuille) (Janvier 2004)

RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL

Renseignements relatifs aux membres de familles de brevets

Demande de recherche n
BE 201905160

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2008065349	A1 05-06-2008	AUCUN	
US 2010025466	A1 04-02-2010	AUCUN	
FR 2912520	A1 15-08-2008	CA 2678186 A1	25-09-2008
		CN 101669118 A	10-03-2010
		EP 2130147 A2	09-12-2009
		FR 2912520 A1	15-08-2008
		JP 5123318 B2	23-01-2013
		JP 2010518501 A	27-05-2010
		KR 20090116743 A	11-11-2009
		KR 20130130876 A	02-12-2013
		US 2010106696 A1	29-04-2010
		WO 2008113921 A2	25-09-2008

OPINION ÉCRITE

Dossier N°	Date du dépot *(jour/mois/année)*	Date de priorité *(jour/mois/année)*	Demande n°
SN73339	15.03.2019		BE201905160

Classification internationale des brevets (CIB)
INV. G07C13/00

Déposant
DUTORDOIR Christophe

La présente opinion contient des indications et les pages correspondantes relatives aux points suivants :

- ☒ Cadre n° I Base de l'opinion
- ☐ Cadre n° II Priorité
- ☐ Cadre n° III Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- ☐ Cadre n° IV Absence d'unité de l'invention
- ☒ Cadre n° V Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- ☐ Cadre n° VI Certains documents cités
- ☐ Cadre n° VII Irrégularités dans la demande
- ☒ Cadre n° VIII Observations relatives à la demande

Examinateur
Hniene, Badr

Demande n°

OPINION ÉCRITE

BE201905160

Cadre n° I Base de l'opinion

1. Cette opinion a été établie sur la base des revendications déposées avant le commencement de la recherche.

2. En ce qui concerne **la ou les séquences de nucléotides ou d'acides aminés** divulguées dans la demande, le cas échéant, cette opinion a été effectuée sur la base des éléments suivants :

a. Nature de l'élément:

☐ un listage de la ou des séquences

☐ un ou des tableaux relatifs au listage de la ou des séquences

b. Type de support:

☐ sur papier

☐ sous forme électronique

c. Moment du dépôt ou de la remise:

☐ contenu(s) dans la demande telle que déposée

☐ déposé(s) avec la demande, sous forme électronique

☐ remis ultérieurement

3. ☐ De plus, lorsque plus d'une version ou d'une copie d'un listage des séquences ou d'un ou plusieurs tableaux y relatifs a été déposée, les déclarations requises selon lesquelles les informations fournies ultérieurement ou au titre de copies supplémentaires sont identiques à celles initialement fournies et ne vont pas au-delà de la divulgation faite dans la demande internationale telle que déposée initialement, selon le cas, ont été remises.

4. Commentaires complémentaires :

Demande n°

OPINION ÉCRITE

BE201905160

Cadre n° V Opinion motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-9
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-9
Possibilité d'application industrielle	Oui :	Revendications	1-9
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

Cadre n° VIII Observations relatives à la demande

voir feuille séparée

1 **Ad point VIII**

Certaines observations relatives à la demande

1.1 Les revendications 1 et 8 revendiquent des systèmes de vote. Cependant, aucun composant des systèmes revendiqués n'est spécifié, et aucune étape de vote n'est revendiquée.

1.2 Bien que les revendications 1 et 8 aient été rédigées en tant que revendications indépendantes distinctes, elles semblent avoir le même objet et ne différer les unes des autres que par la définition de l'objet pour lequel la protection est demandée et/ou par la terminologie utilisée pour définir les caractéristiques de cet objet. Par conséquent, ces revendications manquent de concision.

1.3 Il n'est pas clair du passage "`[...]` **`deux paramètres confidentiels`** `constitués par exemple de deux mots de passe ou` **`d'un seul mot de passe`**" de la revendication 8 comment un seul mot de passe peut constituer deux paramètres confidentiels.

1.4 La revendication 8 ne satisfait pas à l'exigence de clarté, car l'objet de la protection demandée n'est pas clairement défini. Le passage "`[...] d'un seul mot de passe mais dont on devra, dans ce dernier cas, s'assurer de l'unicité`" de cette revendication tente de définir l'objet par le résultat recherché, ce qui revient simplement à énoncer le problème sous-jacent, sans indiquer les caractéristiques techniques nécessaires pour parvenir à ce résultat.

1.5 Il n'est pas clair du passage "`[...]` **`deux paramètres confidentiels`** `[...] ledit fichier reprenant en clair (non crypté) le contenu du vote et étant accessible par l'électeur sur un site de vérification en introduisant ledit` **`paramètre non confidentiel et son mot de passe de vérification`**" de la revendication 8 comment obtenir le paramètre non confidentiel et le mot de passe, qui n'ont pas d'antécédents dans cette revendication, l'usage des paramètres confidentiels n'est également pas spécifié.

1.6 Le terme "`la base de données`" cité dans la revendication 2 n'a pas d'antécédent.

1.7 Le terme "`le répertoire correspondant au bureau de vote de l'électeur`" cité dans la revendication 3 n'a pas d'antécédent.

1.8 Le terme "`le serveur`" cité dans la revendication 4 n'a pas d'antécédent.

2 **Ad point V**

Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle ; citations et explications à l'appui de cette déclaration

2.1 Il est fait référence aux documents suivants :

D1 WO 2008/065349 A1 (IRVINE DAVID [GB]) 5 juin 2008 (2008-06-05)

D2 US 2010/025466 A1 (CARDONE RICHARD J [US] ET AL) 4 février 2010 (2010-02-04)

D3 FR 2 912 520 A1 (STG INTERACTIVE SA [FR]) 15 août 2008 (2008-08-15)

2.2 Nonobstant les objections de manque de clarté du paragraphe 1, la présente demande ne remplit pas les conditions de brevetabilité, l'objet de la revendications indépendantes 1 et 8 n'impliquant pas d'activité inventive.

2.3 Revendication 1:

2.3.1 D1, qui est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1, divulgue (les références entre parenthèses s'appliquent à ce document):

Un système de vote par internet **(page 30, Alinéa 5: Voting System; page 31, Alinéas 4-5: A non anonymous user logged into the net [...] An anonymous user may be logged onto the net [...])** comprenant un mot de passe de vote à utiliser par l'électeur pour accéder au dit vote caractérisé en ce qu'un mot de passe de vérification demandé par le système est introduit par l'électeur, ledit mot de passe de vérification, joint à un paramètre non confidentiel propre à l'électeur (par exemple numéro de registre national), servant à créer un **identifiant** ~~nom de fichier~~ construit avec une fonction SHA-256 ou avec n'importe quelle autre fonction de hachage cryptographique (par exemple MD5, SHA-1, SHA-2, ...) **(page 32, Alinéa 3: The users system creates a one time ID + key pair to vote. This public key can be hashed and stored on the net as with a MAID or PMID so as to allow checking of any signed or encrypted votes sent back; page 32, Alinéa 6: The vote is received and a receipt chunk put on the net. This is a chunk called with the user's temp (or voting) ID hash [...])**, ledit identifiant

~~fichier~~ reprenant en clair (non crypté) le contenu du vote et étant accessible par l'électeur sur un site de vérification en introduisant ledit paramètre non confidentiel et son mot de passe de vérification **(page 32, Alinéa 3: The users system creates a one time ID + key pair to vote. This public key can be hashed and stored on the net as with a MAID or PMID so as to allow checking of any signed or encrypted votes sent back; page 32, Alinéas 6-8: The vote is received and a receipt chunk put on the net. This is a chunk called with the user's temp (or voting) ID hash [...] The authority can then publish a list of who voted for what (i.e. a list of votes and the voting ID's) [...] The user's system checks the list for the ID that was used being present in the list and validates that the vote was cast properly)**.

2.3.2 Par conséquent, l'objet de la revendication 1 diffère de D1 en ce que le vote est mis dans un fichier dont le nom est construit en appliquant une fonction de hachage au mot de passe de l'utilisateur joint à un paramètre non confidentiel. D1 divulgue seulement que le résultat du hachage est enregistré avec le contenu du vote, et que ces deux éléments sont récupérés en utilisant un mot de passe afin de vérifier le vote.

2.3.3 La différence citée ci-dessus ne résout aucun problème technique qui va au delà du simple choix du mode de stockage d'informations dans un serveur ou une base de données. Le fait que le contenu du vote soit soit écrit dans un fichier dont le nom correspond au résultat du hachage, ou par exemple dans une base de donnée dans une ligne avec le résultat du hachage comme clé, n'a aucun impact sur le contenu récupéré par le votant et par conséquent sur la vérification du vote. En outre, l'utilisation de fonctions de hachage afin de transformer les noms de fichiers/répertoires et y accéder ensuite, est bien connue dans l'art **(voir D3: revendication 1 à titre d'exemple)** et serait sélectionnée par l'homme du métier sans avoir recours à un esprit inventif.

2.3.4 La solution proposée dans la revendication 1 de la présente demande ne peut être considérée comme impliquant une activité inventive.

2.4 Dans la mesure où la revendication 8 peut être comprise, l'objet de la revendication 8 ne semble différer de celui de la revendication 1 que par le fait que deux mots de passes sont utilisés en entrée de la fonction de hachage au lieu d'un mot de passe et d'un paramètre non confidentiel. Par conséquent, le raisonnement du paragraphe 2.3 s'applique aussi à l'objet de la revendication indépendante 8, dont l'objet n'implique également pas d'activité inventive.

2.5 Les revendications dépendantes:

2.5.1 Les caractéristiques supplémentaires des revendications 2-4 ne sont que des détails d'implémentation que l'homme du métier sélectionnerait sans avoir recours à un esprit inventif.

2.5.2 Les caractéristiques supplémentaires de la revendication 5 ne résolvent pas de problème technique, mais uniquement un problème administratif. Elles n'impliquent donc pas d'activité inventive.

2.5.3 La caractéristique supplémentaire de la revendication 6 correspond à une simple redondance de fichiers qui n'implique pas d'activité inventive.

2.5.4 La caractéristique supplémentaire des revendications 7 et 9 est implicitement divulguée dans D1 **(voir pages 30-32**) et n'implique donc pas d'activité inventive.