Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3098631 A1 2019/11/07

(21) 3 098 631

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2019/04/30
(87) Date publication PCT/PCT Publication Date: 2019/11/07
(85) Entrée phase nationale/National Entry: 2020/10/28
(86) N° demande PCT/PCT Application No.: FR 2019/000064
(87) N° publication PCT/PCT Publication No.: 2019/211533
(30) Priorité/Priority: 2018/04/30 (FR1870507)

(51) Cl.Int./Int.Cl. *G06F 21/44* (2013.01), *H04W 12/06* (2009.01)

(71) Demandeur/Applicant:
LEDGER SAS, FR

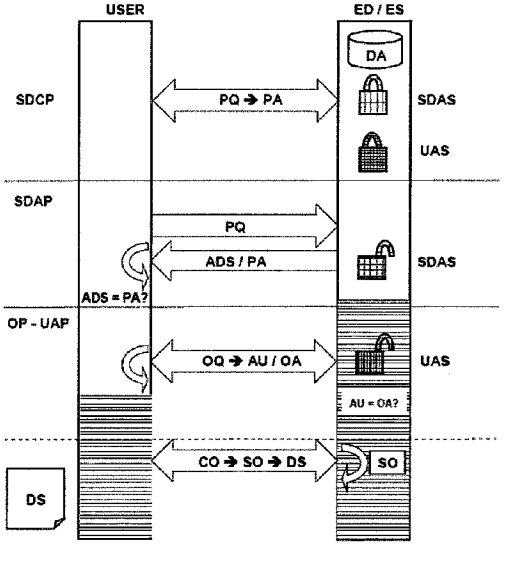
(72) Inventeurs/Inventors:
BACCA, NICOLAS, FR;
TOMAZ, OLIVIER, FR

(74) Agent: LAVERY, DE BILLY, LLP

(54) Titre : AUTHENTIFICATION MUTUELLE D'UN DISPOSITIF OU D'UN SYSTEME CONTENANT DES DONNEES SENSIBLES OU CONFIDENTIELLES COMMANDABLE PAR UN UTILISATEUR

(54) Title: MUTUAL AUTHENTICATION OF A USER-CONTROLLABLE DEVICE OR SYSTEM CONTAINING SENSITIVE OR CONFIDENTIAL DATA

Figure 1 :



(57) Abrégé/Abstract:
Procédé d'authentification mutuelle d'un dispositif (DE) électronique commandable et de son utilisateur (USER) pouvant le commander afin qu'il lui procure un service (DS), le dispositif (DE) contenant des données sensibles ou confidentielles (DA) et étant agencé de manière à - dans une phase opérationnelle (OP) incluant une étape préliminaire d'authentification de l'utilisateur (UAP) -, exécuter une opération (SO) pour procurer le service (DS), comportant, en outre, une phase préalable d'authentification du dispositif (SDAP) dans laquelle est vérifiée l'authenticité du dispositif (DE), de sorte que si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (DE) est avéré authentique, l'utilisateur (USER) peut exécuter la phase opérationnelle (OP), alors que si le dispositif (DE) n'est pas avéré authentique, l'utilisateur (USER) peut empêcher l'exécution de la phase opérationnelle (OP).

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
07 novembre 2019 (07.11.2019)

WIPO | PCT

(10) Numéro de publication internationale
WO 2019/211533 A1

(51) Classification internationale des brevets :
G06F 21/44 (2013.01) *H04W 12/06* (2009.01)

(21) Numéro de la demande internationale :
PCT/FR2019/000064

(22) Date de dépôt international :
30 avril 2019 (30.04.2019)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1870507 30 avril 2018 (30.04.2018) FR

(71) Déposant : **LEDGER SAS** [FR/FR] ; 1, rue du Mail, 75002 Paris (FR).

(72) Inventeurs : **BACCA, Nicolas** ; 125 bd de Verdun, 92400 Courbevoie (FR). **TOMAZ, Olivier** ; 1 bis rue du Bocage, 91400 Orsay (FR).

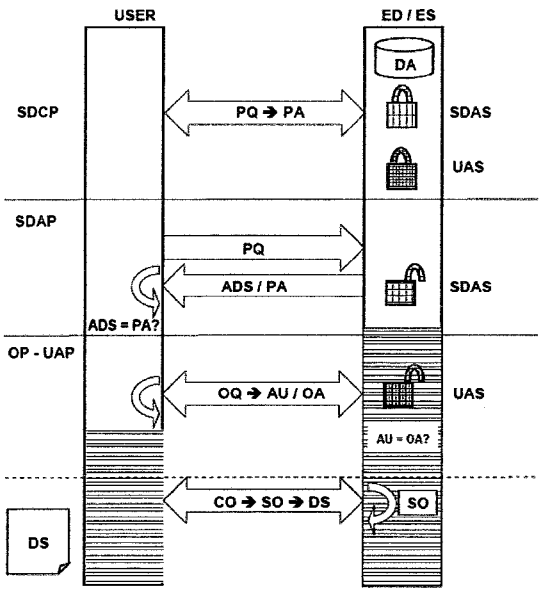
(74) Mandataire : **SELARL FELTESSE WARUSFEL PASQUIER & ASSOCIES - FWPA** ; WARUSFEL, Bertrand, 18 rue des Pyramides, 75001 Paris (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,

(54) **Title:** MUTUAL AUTHENTICATION OF A USER-CONTROLLABLE DEVICE OR SYSTEM CONTAINING SENSITIVE OR CONFIDENTIAL DATA

(54) **Titre :** AUTHENTIFICATION MUTUELLE D'UN DISPOSITIF OU D'UN SYSTÈME CONTENANT DES DONNÉES SENSIBLES OU CONFIDENTIELLES COMMANDABLE PAR UN UTILISATEUR

Figure 1 :



(57) **Abstract:** Method of mutual authentication of a controllable electronic device (DE) and of its user (USER) able to control it so that it procures him a service (DS), the device (DE) containing sensitive or confidential data (DA) and being arranged so as to - in an operational phase (OP) including a preliminary step of authentication of the user (UAP) -, execute an operation (SO) so as to procure the service (DS), comprising, furthermore, a prior phase of authentication of the device (SDAP), in which the authenticity of the device (DE) is verified, so that if on completion of the prior phase of authentication of the device (SDAP), the device (DE) is confirmed to be authentic, the user (USER) can execute the operational phase (OP), whilst if the device (DE) is not confirmed to be authentic, the user (USER) can prevent the execution of the operational phase (OP).

(57) **Abrégé :** Procédé d'authentification mutuelle d'un dispositif (DE) électronique commandable et de son utilisateur (USER) pouvant le commander afin qu'il lui procure un service (DS), le dispositif (DE) contenant des données sensibles ou confidentielles (DA) et étant agencé de manière à - dans une phase opérationnelle (OP) incluant une étape préliminaire d'authentification de l'utilisateur (UAP) -, exécuter une opération (SO) pour procurer le service (DS), comportant, en outre, une phase préalable d'authentification du dispositif (SDAP) dans laquelle est vérifiée l'authenticité du dispositif (DE), de sorte que si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (DE) est avéré authentique, l'utilisateur (USER) peut exécuter la phase opérationnelle (OP), alors que si le dispositif (DE) n'est pas avéré authentique, l'utilisateur (USER) peut empêcher l'exécution de la phase opérationnelle (OP).

WO 2019/211533 A1

[Suite sur la page suivante]

WO 2019/211533 A1

SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

Description

Titre de l'invention : Authentification mutuelle d'un dispositif ou d'un système contenant des données sensibles ou confidentielles commandable par un utilisateur

Authentification mutuelle d'un dispositif ou d'un système contenant des données sensibles ou confidentielles commandable par un utilisateur

L'invention est relative à l'authentification d'un dispositif ou d'un système contenant des données sensibles ou confidentielles et elle a plus spécialement pour objet un procédé d'authentification mutuelle d'un dispositif ou d'un système électronique (également informatique et communicant) fonctionnel, commandable par un utilisateur, un procédé d'exploitation d'un tel dispositif ou d'un tel système, et un dispositif ou un système spécialement agencé pour la mise en œuvre du procédé d'authentification ou du procédé d'exploitation.

Dans le cadre de l'invention, l'expression « dispositif électronique fonctionnel » doit être comprise comme étant par exemple un terminal de paiement, alors que l'expression « système électronique fonctionnel » doit être comprise comme signifiant un ensemble fonctionnel comportant plusieurs dispositifs pouvant être associés fonctionnellement entre eux notamment en chaîne fonctionnelle, tel que par exemple un terminal de paiement et un serveur distant.
Le terme « fonctionnel » qualifiant un tel dispositif ou un tel système doit être compris comme signifiant, au sens large, que, dans une phase opérationnelle, il fonctionne pour exécuter une certaine opération (que l'on peut aussi appeler tâche, transaction, ou analogue), laquelle opération est spécifique et de nature à procurer finalement à l'utilisateur un service déterminé, comme par exemple une commande, un paiement, ou analogue.
Le terme « commandable » associé à utilisateur et relativement à un dispositif ou un système doit être compris comme signifiant que ce dispositif ou ce système est agencé de sorte que son fonctionnement est déclenché par l'utilisateur, notamment dans la phase opérationnelle.
Les termes « dispositif » et « système » signifient par ellipse, respectivement, dispositif électronique fonctionnel et système électronique fonctionnel.

Dans le cadre de l'invention, le terme « authentification » doit être compris comme signifiant un processus de vérification de l'authenticité. Le terme « authenticité » doit être compris comme signifiant légitimité, conformité à ce qui est attendu, qui est véridique, fait foi et ne peut être mis en doute, ou encore auquel on peut se fier. L'expression « authentification mutuelle » concernant le dispositif ou le système électronique fonctionnel commandable par un utilisateur doit être compris comme se rapportant à la vérification de l'authenticité du dispositif ou du système par l'utilisateur et,

en combinaison, la vérification de l'authenticité de l'utilisateur par le dispositif ou le système. Ainsi, l'authentification, objet de l'invention, est, d'abord, la vérification que le dispositif ou le système est bien le bon dispositif ou le bon système et, ensuite, que l'utilisateur est bien le bon utilisateur. Par suite, l'authentification mutuelle vise à sécuriser l'opération exécutée et le service finalement procuré à l'utilisateur, y compris pour l'utilisateur.

Dans le cadre de l'invention, le terme « donnée » doit être compris comme signifiant toute information, code, ou autre, qui est spécifique et conditionne le fonctionnement du dispositif ou du système en vue d'exécuter l'opération spécifique pour procurer à l'utilisateur le service déterminé.
Les termes « sensible » et « confidentiel » doivent être compris comme qualifiant une donnée qui ne doit pas être connue, révélée ou accessible, selon les cas, autrement que par le dispositif ou le système authentique ou bien par l'utilisateur authentique, faute de quoi l'opération exécutée et finalement le service procuré à l'utilisateur ne seraient pas ou pourraient ne pas être sécurisés.

Tel est le contexte de l'invention et telle est l'interprétation des termes utilisés dans l'ensemble du texte.

L'homme du métier connaît déjà des processus d'authentification pour des systèmes informatiques et de télécommunication. Par exemple l'utilisateur authentique d'un téléphone portable pourvu d'une carte SIM (pour Subscriber Identity Module) dispose d'un code PIN personnel (pour Personal Identification Number) qui protège la carte SIM contre toute utilisation non autorisée. Le cas échéant, il est prévu un second code, le code PUK (pour PIN Unlock Key), qui a pour seule fonction de débloquer la carte SIM lorsqu'elle a été bloquée par suite d'une séquence de (trois par exemple) saisies erronées. Le document US 3 905 461 décrit par exemple un équipement de contrôle d'accès au moyen d'un jeton codé dont dispose l'utilisateur authentique. Ou, un certificat d'authenticité active un cadenas dans le but d'assurer une connexion sécurisée comme typiquement pour des transactions financières, du transfert de données, etc. Le document EP 2 431 904 décrit un système d'authentification connu sous l'expression authentification question-réponse, qui repose sur une question de défi et la vérification de l'exactitude de la réponse à cette question de défi. Le document EP 3 035 640 décrit un procédé d'authentification d'un premier dispositif exécuté par un second dispositif par un processus d'authentification question-réponse. La simple identification, par exemple d'un utilisateur, de sorte à établir son identité ne vaut pas authentification de l'utilisateur (voir EP 2 278 538). De la même manière, la simple identification par l'utilisateur d'un dispositif ou d'un système ne garantit pas à l'utilisateur que ce dispositif ou ce système soit authentique. Par suite, si, par exemple, le dispositif ou le système authentique a été remplacé par un dispositif ou système factice, l'exploitation par l'utilisateur de ce dispositif ou de ce système va conduire l'utilisateur à communiquer à ce dispositif ou à ce système un code secret ou des données sensibles ou

confidentielles, ou analogue, qui pourront alors être récupérés par un attaquant qui pourra les utiliser frauduleusement, au lieu et place de l'utilisateur authentique.

Le problème à la base de l'invention est, donc, s'agissant d'un dispositif ou d'un système électronique fonctionnel, commandable par un utilisateur, d'assurer une authentification mutuelle, c'est-à-dire de vérifier que le dispositif ou le système est bien le bon dispositif ou le bon système et que l'utilisateur est bien le bon utilisateur, de sorte que l'opération exécutée par ce dispositif ou par ce système et finalement le service procuré à l'utilisateur soient garantis sécurisés, y compris pour l'utilisateur.

L'invention apporte une solution à ce problème en prévoyant, avant la phase opérationnelle d'exécution d'une opération, laquelle phase opérationnelle inclut une étape où le dispositif ou le système authentifie l'utilisateur, et dans laquelle les données sensibles ou confidentielles sont accessibles, une phase préalable d'authentification du dispositif ou du système, dans laquelle l'utilisateur vérifie l'authenticité du dispositif ou du système, la phase opérationnelle étant conditionnelle dans la mesure où elle ne peut être réalisée que si et seulement si la phase préalable d'authentification du dispositif ou du système a été préalablement exécutée et que, dans cette phase préalable d'authentification du dispositif ou du système, le dispositif ou le système a été effectivement authentifié par l'utilisateur. C'est ainsi qu'est réalisée une double authentification et qu'est assurée la sécurisation de l'opération exécutée par le dispositif ou par le système et finalement le service procuré à l'utilisateur.

Ci-après, un exposé de l'invention.

Selon un premier aspect, l'invention a pour objet un procédé d'authentification mutuelle d'un dispositif électronique fonctionnel commandable et de son utilisateur, comprenant une phase préliminaire de configuration (SDCP) du dispositif (DE) définissant les modalités de la vérification de son authenticité, l'utilisateur pouvant commander ensuite le dispositif afin qu'il lui procure un service déterminé, le dispositif contenant des données sensibles ou confidentielles et étant agencé de manière à - dans une phase opérationnelle déclenchée par l'utilisateur et incluant une étape préliminaire d'authentification de l'utilisateur par le dispositif -, exécuter une opération spécifique appropriée pour procurer le service, le procédé comportant, en outre, avant toute phase opérationnelle, une phase préalable d'authentification du dispositif dans laquelle est vérifiée l'authenticité du dispositif, de sorte que :

- si à l'issue de la phase préalable d'authentification du dispositif, le dispositif est avéré authentique, l'utilisateur peut exécuter la phase opérationnelle,
- si à l'issue de la phase préalable d'authentification du dispositif, le dispositif n'est pas avéré authentique, l'utilisateur en est alerté par un moyen quelconque de manière à pouvoir empêcher l'exécution de la phase opérationnelle,

en sorte que, d'abord le dispositif, puis l'utilisateur, sont authentifiés et que l'opération exécutée et le service procuré sont sécurisés.

Selon une réalisation, la phase préalable d'authentification du dispositif est exécutée par l'utilisateur.

Selon une réalisation, le procédé, qui comporte dans le temps plusieurs phases opérationnelles, est tel qu'une phase préalable d'authentification du dispositif est exécutée avant chaque phase opérationnelle.

Selon une réalisation, la phase préalable d'authentification du dispositif par l'utilisateur, repose sur un processus d'authentification question-réponse, moyennant un secret d'authentification du dispositif qui est une question préalable de l'utilisateur au dispositif et une réponse préalable du dispositif à l'utilisateur à la question préalable, la question préalable et la réponse préalable étant secrètes pour n'être connues ou accessibles que du seul utilisateur authentique, de sorte que l'authenticité du dispositif n'est avérée que si et seulement si l'utilisateur vérifie qu'il y a identité entre, d'une part, la réponse apportée par le dispositif à la question préalable et, d'autre part, la réponse préalable.

Selon une variante de réalisation, si à l'issue de la phase préalable d'authentification du dispositif, le dispositif n'est pas avéré authentique, l'utilisateur peut être empêché par le dispositif lui-même d'exécuter la phase opérationnelle.

Selon une réalisation, le procédé comprend également une phase préliminaire de configuration, dans laquelle le dispositif est configuré avec le secret d'authentification du dispositif (SDAS).

Selon une réalisation, la phase préliminaire de configuration du dispositif est exécutée par l'utilisateur.

Selon une réalisation, la configuration du dispositif avec la question préalable et la réponse préalable est exécutée à partir d'une question de l'utilisateur, grâce à un processus générateur de question à réponse.

Selon une réalisation, la phase préalable d'authentification du dispositif est exécutée après que la phase préliminaire de configuration a été exécutée, et sous la condition de l'absence d'exécution, entre temps, de toute autre phase préalable d'authentification du dispositif ou d'une phase opérationnelle.

Selon les réalisations, la phase préalable d'authentification du dispositif est exécutée après que la phase préliminaire de configuration a été exécutée, et sous la condition de l'exécution entre temps, d'une ou de plusieurs autres phases préalables d'authentification du dispositif ou de phases opérationnelles.

Selon les réalisations, à une phase préliminaire de configuration est associée de façon nécessaire et suffisante soit une seule phase préalable d'authentification du dispositif soit une pluralité préfixée de phases préalables d'authentification du dispositif successives soit une pluralité illimitée de phases préalables d'authentification du dispositif successives.

Selon une réalisation, l'étape préliminaire d'authentification de l'utilisateur par le dispositif repose sur un secret d'authentification de l'utilisateur qui est une réponse opérationnelle de l'utilisateur au dispositif, secrète pour n'être connue et accessible que du seul utilisateur authentique, de sorte que l'authenticité de l'utilisateur n'est avérée que si et seulement si le dispositif vérifie qu'il y a identité entre, d'une part, la réponse apportée par l'utilisateur et, d'autre part, la réponse opérationnelle.

Selon une réalisation, la question préalable et la réponse opérationnelle sont différentes.

Selon une réalisation, le procédé comprend une étape de suppression des données sensibles ou confidentielles du dispositif, exécutée automatiquement à l'issue d'un nombre préfixé d'exécution de phases préalables d'authentification du dispositif successives où le dispositif n'est pas avéré authentique. En particulier, cette étape de suppression des données sensibles ou confidentielles efface également la question préalable et la réponse préalable lorsque, à l'issue d'un nombre préfixé d'exécution de phases préalables d'authentification du dispositif ou du système successives, l'utilisateur a échoué à fournir la question préalable correspondant à la réponse préalable, de telle sorte le dispositif ou le système considérera que l'utilisateur n'est pas l'utilisateur authentique.

Selon un deuxième aspect, l'invention a pour objet un procédé d'exploitation par un utilisateur d'un dispositif électronique fonctionnel commandable par l'utilisateur afin qu'il lui procure un service déterminé, le dispositif contenant des données sensibles ou confidentielles, dans lequel, dans une phase opérationnelle déclenchée par l'utilisateur et incluant une étape préliminaire d'authentification de l'utilisateur par le dispositif, le dispositif exécute une opération spécifique appropriée pour procurer le service, le procédé d'exploitation comportant, en outre, avant toute phase opérationnelle, une phase préalable d'authentification du dispositif dans laquelle est vérifiée l'authenticité du dispositif, de sorte que :

- si à l'issue de la phase préalable d'authentification du dispositif, le dispositif est avéré authentique, l'utilisateur peut exécuter la phase opérationnelle,
- si à l'issue de la phase préalable d'authentification du dispositif, le dispositif n'est pas avéré authentique, l'utilisateur en est alerté par un moyen quelconque de manière à pouvoir empêcher l'exécution de la phase opérationnelle,

en sorte que, d'abord le dispositif, puis l'utilisateur, sont authentifiés et que l'opération exécutée et le service procuré sont sécurisés.

Selon un troisième aspect, l'invention a pour objet un dispositif électronique fonctionnel, commandable par un utilisateur en vue d'un service déterminé, contenant des données sensibles ou confidentielles, spécialement agencé pour la mise en œuvre du procédé d'authentification mutuelle et pour la mise en œuvre du procédé d'exploitation précédemment décrits, notamment pour exécuter une phase préalable d'authentification du dispositif.

Selon une réalisation, le dispositif est configuré à l'issue d'une phase préliminaire de configuration avec le secret d'authentification du dispositif, qui est une question préalable de l'utilisateur au dispositif et une réponse préalable du dispositif à l'utilisateur à la question préalable.

Ainsi, le dispositif comprend et combine, d'une part, le secret d'authentification du dispositif et, d'autre part, le secret d'authentification de l'utilisateur.

Selon un quatrième aspect, l'invention a pour objet un procédé d'authentification mutuelle d'un système électronique fonctionnel, commandable par un utilisateur en vue d'un service déterminé, contenant des données sensibles ou confidentielles, comprenant une pluralité de dispositifs électroniques associés fonctionnellement entre eux, agencé de manière à - dans une phase opérationnelle déclenchée par l'utilisateur et incluant une étape où le système authentifie l'utilisateur -, exécuter une opération ou une série d'opérations spécifique appropriée pour procurer le service, le procédé comportant, en outre, avant toute phase opérationnelle, une phase préalable d'authentification du système, dans laquelle est vérifiée l'authenticité de tout ou partie de la pluralité des dispositifs que le système comprend, moyennant la mise en œuvre, pour chaque dispositif vérifié, du procédé d'authentification précédemment décrit.

Selon une réalisation avec une pluralité de dispositifs électroniques formant une ou plusieurs chaînes fonctionnelles avec un ou des dispositifs amont et un ou des dispositifs aval, le procédé est tel que :
- si à l'issue de la phase préalable d'authentification d'un dispositif amont d'une chaîne de dispositifs, ce dispositif est avéré authentique, il est procédé à l'authentification du ou des dispositifs aval de la même chaîne de dispositifs,
- si à l'issue de la phase préalable d'authentification d'un dispositif amont d'une chaîne de dispositifs, ce dispositif n'est pas avéré authentique, il n'est pas procédé à l'authentification du ou des dispositifs aval de la même chaîne de dispositifs, le système étant avéré non authentique.

Selon un cinquième aspect, l'invention a pour objet un procédé d'exploitation par un utilisateur d'un système électronique fonctionnel commandable par l'utilisateur afin qu'il lui procure un service déterminé, le système contenant des données sensibles ou confidentielles, comprenant une pluralité de dispositifs électroniques associés fonctionnellement entre eux, dans lequel - dans une phase opérationnelle déclenchée par l'utilisateur et incluant une étape préliminaire d'authentification de

l'utilisateur par le système -, le système exécute une opération ou une série d'opérations spécifique appropriée pour procurer le service, le procédé d'exploitation comportant, en outre, avant toute phase opérationnelle, une phase préalable d'authentification du système dans laquelle est vérifiée l'authenticité de tout ou partie de la pluralité des dispositifs que le système comprend, moyennant la mise en œuvre, pour chaque dispositif vérifié, du procédé d'authentification précédemment décrit, de sorte que :

- si à l'issue de la phase préalable d'authentification du système, le système est avéré authentique, l'utilisateur peut exécuter la phase opérationnelle,
- si à l'issue de la phase préalable d'authentification du système, le système n'est pas avéré authentique, l'utilisateur en est alerté par un moyen quelconque de manière à pouvoir empêcher l'exécution de la phase opérationnelle,

en sorte que d'abord le système puis l'utilisateur sont authentifiés et que l'opération exécutée et le service procuré sont sécurisés.

Selon un sixième aspect, l'invention a pour objet un système électronique fonctionnel, commandable par un utilisateur en vue d'un service déterminé, contenant des données sensibles ou confidentielles, comprenant une pluralité de dispositifs électroniques associés fonctionnellement entre eux, tels qu'il a été précédemment décrit, spécialement agencé pour la mise en œuvre du procédé d'authentification mutuelle tels qu'il a été précédemment décrit, et pour la mise en œuvre du procédé d'exploitation tels qu'il a été précédemment décrit, notamment pour exécuter une phase préalable d'authentification de tout ou partie de la pluralité des dispositifs que le système comprend.

On décrit maintenant brièvement la figure unique 1. Cette figure est un schéma général théorique indicatif et purement didactique des étapes d'une réalisation possible d'un procédé d'exploitation par un utilisateur d'un dispositif électronique fonctionnel commandable par l'utilisateur afin qu'il lui procure un service déterminé, le dispositif contenant des données sensibles ou confidentielles, illustrant :

- d'abord, une phase préliminaire de configuration reposant sur un secret d'authentification du dispositif, exécutée par l'utilisateur,
- puis, une phase préalable d'authentification du dispositif, dans laquelle est vérifiée l'authenticité du dispositif, reposant sur le secret d'authentification du dispositif,
- puis, dans la mesure où à l'issue de la phase préalable d'authentification du dispositif, le dispositif est avéré authentique, une phase opérationnelle déclenchée par l'utilisateur et incluant une étape préliminaire d'authentification de l'utilisateur par le dispositif reposant sur un secret d'authentification de l'utilisateur, phase opérationnelle dans laquelle le dispositif exécute une opération spécifique appropriée pour procurer le service.

Ci-après un exposé détaillé de modes d'exécution de l'invention et de différentes réalisations, assorti d'exemples et de référence à la figure. Cet exposé doit être compris dans le contexte de l'invention et avec l'interprétation des termes, comme il a été présenté précédemment, et qu'il est donc inutile de répéter.

L'invention concerne et met en œuvre un dispositif électronique (également informatique et communicant) fonctionnel ED commandable, qui contient des données sensibles ou confidentielles DA, et, plus généralement, un système électronique (également informatique et communicant) fonctionnel ES qui comprend une pluralité de dispositifs ED formant une ou plusieurs chaînes fonctionnelles avec un ou des dispositifs amont et un ou des dispositifs aval. Comme pour le dispositif ED, le système ES contient des données sensibles ou confidentielles DA. L'exposé de l'invention est plus spécialement détaillé pour un dispositif ED. Elle peut être transposée pour un système ES à savoir pour tout ou partie des dispositifs ED qu'il comporte, tout spécialement ceux contenant des données sensibles ou confidentielles DA ou dont l'authenticité doit être avérée.

L'invention implique un utilisateur USER qui commande le dispositif ED ou le système ES, moyennant une commande CO, afin qu'il lui procure un service déterminé DS et exécute les différentes phases ou étapes requises pour l'exploitation du dispositif ED ou du système ES.

L'invention vise, s'agissant tant du dispositif ED ou du système ES que de l'utilisateur USER, d'assurer une authentification mutuelle, c'est-à-dire que l'utilisateur USER puisse d'abord vérifier que le dispositif ED ou le système ES est bien le bon et ensuite que le dispositif ED ou le système ES puisse vérifier que l'utilisateur USER est bien le bon. C'est ainsi que l'opération spécifique SO exécutée par le dispositif ED ou par le système ES et finalement le service déterminé DS procuré à l'utilisateur USER sont garantis sécurisés, y compris pour l'utilisateur USER. Il faut comprendre par-là, que la commande du dispositif ED ou du système ES par l'utilisateur USER n'est possible que si le dispositif ED ou le système ES est authentique, et non pas un dispositif ou un système factice ou illicite, et si l'utilisateur USER est authentique, et non pas un utilisateur postiche ou illicite. S'il apparaît que le dispositif ED ou le système ES n'est pas authentique, l'utilisateur ne pourra exécuter l'opération spécifique SO en ce sens qu'il en sera empêché. Et de même, s'il apparaît que l'utilisateur n'est pas authentique, il ne pourra pas d'avantage exécuter l'opération spécifique SO en ce sens qu'il en sera empêché.

Par la suite, il est supposé que le dispositif ED ou le système ES est authentique, et que l'utilisateur USER est authentique. L'exposé de l'invention détaille ce qu'il advient lorsque le dispositif ED ou le système ES n'est pas authentique, et lorsque l'utilisateur USER n'est pas authentique.

Dans une réalisation, l'utilisateur USER est la personne même qui est authentique.

Dans une autre réalisation, l'utilisateur USER est un avatar de la personne qui est authentique. Cet avatar est licite pour l'exécution considérée et dispose licitement des codes, secrets, etc. que possède la personne qui est authentique, de sorte à pouvoir agir licitement en lieu et place de la personne qui est authentique.

On désigne par « phase opérationnelle », OP, une phase déclenchée par l'utilisateur USER par la commande CO, dans laquelle le dispositif ED ou le système ES exécute une opération spécifique appropriée SO spécialement conçue pour procurer à l'utilisateur USER le service DS.

On désigne par « étape préliminaire d'authentification de l'utilisateur », UAP, une étape préliminaire incluse dans la phase opérationnelle OP, dans laquelle le dispositif authentifie l'utilisateur USER, au moyen d'un secret d'authentification de l'utilisateur UAS.

On désigne par « phase préalable d'authentification du dispositif ou du système », SDAP, une phase dans laquelle est vérifiée par l'utilisateur USER, l'authenticité du dispositif ED ou du système ES, par exemple au moyen d'un secret d'authentification du dispositif ou du système SDAS.

On désigne par « phase préliminaire de configuration du dispositif ou du système », SDCP, une phase dans laquelle le dispositif ED ou le système ES est configuré avec le secret d'authentification du dispositif ou du système SDAS. Dans une réalisation, cette configuration est réalisée par l'utilisateur USER.

Le procédé d'exploitation du dispositif ED ou du système ES est tel qu'il comporte, avant toute phase opérationnelle OP, une phase préalable d'authentification du dispositif ou du système SDAP, qui est une phase qui s'ajoute à la phase opérationnelle OP, qui est exécutée avant elle, et qui conditionne la possibilité même de l'exécution de cette phase opérationnelle OP. En effet, si à l'issue de la phase préalable d'authentification du dispositif ou du système SDAP, le dispositif ED ou le système ES est avéré authentique, l'utilisateur USER peut exécuter la phase opérationnelle OP, alors que, si à l'issue de la phase préalable d'authentification du dispositif ou du système SDAP, le dispositif ED ou le système ES n'est pas avéré authentique, l'utilisateur USER peut empêcher l'exécution de la phase opérationnelle OP.

Ainsi, le procédé d'exploitation du dispositif ED ou du système ES intègre un procédé d'authentification mutuelle du dispositif ED ou du système ES et de son utilisateur USER. C'est ainsi que, d'abord le dispositif ED ou le système ED, puis l'utilisateur USER sont authentifiés. Et c'est ainsi que l'opération spécifique SO exécutée par le dispositif ED ou le système ED et que le service DS procuré à l'utilisateur USER sont sécurisés. L'invention peut aussi bien être vue sous l'angle d'un procédé d'exploitation d'un dispositif ED ou d'un système ES qui intègre ce procédé

d'authentification mutuelle, que sous l'angle de ce procédé d'authentification mutuelle, destiné à s'intégrer, et s'intégrant, dans un tel procédé d'exploitation.

Selon une réalisation, dans laquelle il est prévu plusieurs phases opérationnelles dans le temps, une phase préalable d'authentification du dispositif ou du système SDAP est exécutée avant chaque phase opérationnelle OP.

Dans une réalisation possible, la phase préalable d'authentification du dispositif ou du système SDAP par l'utilisateur USER, repose sur un processus d'authentification question-réponse, moyennant le secret d'authentification du dispositif ou du système SDAS, lequel est une question préalable PQ de l'utilisateur USER au dispositif ED ou au système ES et une réponse préalable PA du dispositif ED ou du système ES à l'utilisateur USER à la question préalable PQ. La question préalable PQ et la réponse préalable PA sont différentes et secrètes pour n'être connues ou accessibles que du seul utilisateur authentique USER. De la sorte, l'authenticité du dispositif ED ou du système ES n'est avérée que si et seulement si l'utilisateur USER vérifie qu'il y a identité entre la réponse ADS apportée par le dispositif ED ou le système ES à la question préalable PQ et la réponse préalable PA.

Il est entendu que l'authentification du dispositif ou du système SDAP par le processus d'authentification question-réponse qui vient d'être mentionné n'est pas exclusif et limitatif. D'autres processus procurant une authentification d'un niveau élevé peuvent être envisagées. L'invention inclut donc également les réalisations reposant sur un processus d'authentification équivalent du processus question-réponse. Il est entendu également que la phase préalable d'authentification du dispositif ou du système SDAP peut comporter une combinaison de plusieurs processus d'authentification, question-réponse ou équivalent, et ce dans le but d'avoir un niveau plus élevé d'authentification. C'est ainsi qu'il faut comprendre l'expression la phase préalable d'authentification du dispositif ou du système SDAP repose sur un processus d'authentification question-réponse.

Selon une réalisation possible, la configuration du dispositif ED ou du système ES avec le secret d'authentification du dispositif ou du système SDAS (question préalable PQ et réponse préalable PA) est exécutée à partir d'une question de l'utilisateur USER, grâce à un processus générateur de question à réponse, comme une fonction, un programme ou un algorithme.

Plusieurs réalisations peuvent être envisagées en ce qui concerne l'articulation entre les phases préliminaire de configuration du dispositif ou du système SDCP, préalable d'authentification du dispositif ou du système SDAP et opérationnelle OP. Ainsi, selon une réalisation, la phase préalable d'authentification du dispositif ou du système SDAP est exécutée après que la phase préliminaire de configuration du dispositif ou du système SDCP a été exécutée, moyennant l'absence d'exécution, entre temps, de toute autre phase préalable d'authentification du dispositif ou du système SDAP ou

d'une phase opérationnelle OP. Et, selon d'autres réalisations, la phase préalable d'authentification du dispositif ou du système SDAP est exécutée après que la phase préliminaire de configuration du dispositif ou du système SDCP a été exécutée, moyennant l'exécution entre temps, d'une ou de plusieurs autres phases préalables d'authentification du dispositif ou du système SDAP ou de phases opérationnelles OP. D'autre part, selon les réalisations, à une phase préliminaire de configuration du dispositif ou du système SDCP est associée de façon nécessaire et suffisante soit une seule phase préalable d'authentification du dispositif ou du système SDAP soit une pluralité préfixée de phases préalables SDAP successives soit une pluralité illimitée de phases préalables SDAP successives.

Le secret d'authentification de l'utilisateur UAS mis en œuvre dans l'étape d'authentification de l'utilisateur UAP est une réponse opérationnelle OA de l'utilisateur USER au dispositif ED ou au système ES qui est secrète pour n'être connue et accessible que du seul utilisateur authentique, de sorte que l'authenticité de l'utilisateur n'est avérée que si et seulement si le dispositif ED ou le système ES vérifie qu'il y a identité entre d'une part la réponse apportée AU par l'utilisateur et d'autre part la réponse opérationnelle OA.

La phase opérationnelle OP inclut de façon préliminaire l'étape d'authentification de l'utilisateur UAP, cette dernière conditionnant la possibilité même de l'exécution de cette phase opérationnelle OP. En effet, si à l'issue de l'étape préliminaire d'authentification de l'utilisateur UAP, l'utilisateur USER est avéré authentique, cet utilisateur USER peut exécuter la phase opérationnelle OP, alors que, si à l'issue de l'étape préliminaire d'authentification de l'utilisateur UAP, l'utilisateur n'est pas avéré authentique, cet utilisateur peut empêcher l'exécution de la phase opérationnelle OP.

Plusieurs réalisations peuvent être envisagées. Dans une réalisation, il est prévu une question opérationnelle OQ du dispositif ED ou du système ES à l'utilisateur USER, à laquelle celui-ci doit répondre par la réponse opérationnelle OA. Ou bien, c'est le lancement même de la phase opérationnelle OP qui oblige l'utilisateur USER à apporter au dispositif ED ou au système ES la réponse opérationnelle OA. Dans tous les cas, si la réponse apportée AU par l'utilisateur et la réponse opérationnelle OA ne sont pas identiques, le dispositif ED ou le système ES considérera que l'utilisateur n'est pas l'utilisateur authentique, ce qui aura pour effet que l'opération SO ne sera pas exécutée et que le service DS ne sera pas procuré.

A l'instar de l'authentification du dispositif ou du système, l'authentification de l'utilisateur par le processus d'authentification question-réponse qui vient d'être mentionné n'est pas exclusif et limitatif. D'autres processus procurant une authentification d'un niveau élevé peuvent être envisagées. L'invention inclut donc également les réalisations reposant sur un processus d'authentification équivalent du processus question-réponse. Il est entendu également que l'étape préliminaire d'authentification de l'utilisateur UAP peut comporter une combinaison de plusieurs processus

d'authentification, question-réponse ou équivalent, et ce dans le but d'avoir un niveau plus élevé d'authentification.

Selon une réalisation, la question préalable PQ et la réponse opérationnelle OA sont différentes.

Selon une réalisation, le procédé comprend une étape de suppression des données sensibles ou confidentielles DA du dispositif ED ou du système ES. Cette étape de suppression est exécutée automatiquement à l'issue d'un nombre préfixé d'exécution de phases préalables d'authentification du dispositif ou du système SDAP successives où le dispositif ED ou le système ES n'est pas avéré authentique.
Selon une réalisation complémentaire, l'étape de suppression des données sensibles ou confidentielles DA du dispositif ED ou du système ES supprime également la question préalable PQ et la réponse préalable PA lorsque à l'issue d'un nombre préfixé d'exécution de phases préalables d'authentification du dispositif ou du système SDAP successives, l'utilisateur USER a échoué à fournir la question préalable PQ correspondant à la réponse préalable PA, de telle sorte le dispositif ED ou le système ES considérera que l'utilisateur n'est pas l'utilisateur authentique.

Dans le cas où le procédé concerne un système ES, il est prévu, avant toute phase opérationnelle OP, une phase préalable d'authentification du système SDAP, dans laquelle est vérifiée l'authenticité de tout ou partie de la pluralité des dispositifs ED que le système ES comprend, moyennant la mise en œuvre, pour chaque dispositif ED vérifié, du procédé d'authentification précédemment décrit.

Dans un tel système ES, il se peut que la pluralité de dispositifs ED forment une ou plusieurs chaînes fonctionnelles avec un ou des dispositifs ED amont et un ou des dispositifs ED aval. Dans ce cas, il peut être prévu, d'une part, que si à l'issue de la phase préalable d'authentification SDAP d'un dispositif ED amont d'une chaîne de dispositifs ED, ce dispositif ED est avéré authentique, il est procédé à l'authentification SDAP du ou des dispositifs ED aval de la même chaîne de dispositifs ED, d'autre part, que si à l'issue de la phase préalable d'authentification SDAP d'un dispositif ED amont d'une chaîne de dispositifs ED, ce dispositif ED n'est pas avéré authentique, il n'est pas procédé à l'authentification SDAP du ou des dispositifs ED aval de la même chaîne de dispositifs ED, le système ES étant avéré non authentique.

Un dispositif ED ou un système ES conforme à l'invention est spécialement agencé pour la mise en œuvre du procédé d'authentification mutuelle et pour la mise en œuvre du procédé d'exploitation précédemment décrits, notamment pour exécuter une phase préalable d'authentification du dispositif ou du système SDAP. Ce dispositif ED ou ce système ES est configuré avec – et donc comprend et combine - le secret d'authentification du dispositif ou du système SDAS, d'une part, et le secret d'authentification de l'utilisateur UAS, d'autre part.

On se réfère maintenant au schéma de la figure unique 1. Il représente l'utilisateur USER et le dispositif ED ou le système ES sous la forme de deux colonnes, respectivement à gauche et à droite. Il présente trois blocs se succédant du haut vers le bas sur l'axe du temps, à savoir la phase préliminaire de configuration SDCP, la phase préalable d'authentification du dispositif ou du système SDAS et enfin la phase opérationnelle OP qui est elle-même décomposée en deux blocs, le premier correspondant à l'étape préliminaire d'authentification de l'utilisateur UAP et le second à la phase opérationnelle proprement dite. Comme il a été exposé précédemment, ces deux blocs peuvent être plus ou moins imbriqués.

Le schéma illustre que le dispositif ED ou le système ES contient des données sensibles ou confidentielles DA et comprend et combine, d'une part, le secret d'authentification du dispositif ou du système SDAS et, d'autre part, le secret d'authentification de l'utilisateur UAS (représentés symboliquement par des cadenas fermés).

Le schéma illustre que ces deux secrets sont ouverts successivement, d'abord le secret d'authentification du dispositif ou du système SDAS et, d'autre part, le secret d'authentification de l'utilisateur UAS (représentés symboliquement par des cadenas ouverts).

Le dispositif ED ou le système ES une fois authentifié est représenté avec des rayures horizontales et, de même, l'utilisateur une fois authentifié est représenté avec des rayures horizontales.

Le schéma illustre que la commande CO de l'utilisateur en vue de l'exécution par le dispositif ED ou le système ES de l'opération spécifique SO destinée à procurer à l'utilisateur le service déterminé DS, n'intervient qu'une fois que, en combinaison, le dispositif ED ou le système ES est authentifié (par l'utilisateur) et l'utilisateur authentifié.

Revendications

1. Procédé d'authentification mutuelle d'un dispositif (DE) électronique fonctionnel commandable et de son utilisateur (USER) comprenant une phase préliminaire de configuration (SDCP) du dispositif (DE) définissant les modalités de la vérification de son authenticité, l'utilisateur (USER) pouvant ensuite commander le dispositif (DE) afin qu'il lui procure un service déterminé (DS), le dispositif (DE) contenant des données sensibles ou confidentielles (DA) et étant agencé de manière à - dans une phase opérationnelle (OP) déclenchée par l'utilisateur (USER) et incluant une étape préliminaire d'authentification de l'utilisateur (UAP) par le dispositif (DE) -, exécuter une opération spécifique (SO) appropriée pour procurer le service (DS), le procédé comportant, en outre, avant toute phase opérationnelle (OP), une phase préalable d'authentification du dispositif (SDAP) dans laquelle est vérifiée l'authenticité du dispositif (ED), de sorte que :

- si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (DE) est avéré authentique, l'utilisateur (USER) peut exécuter la phase opérationnelle (OP),
- si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (ED) n'est pas avéré authentique, l'utilisateur (USER) peut empêcher l'exécution de la phase opérationnelle (OP),

en sorte que, d'abord le dispositif (DE), puis l'utilisateur (USER), sont authentifiés et que l'opération exécutée et le service (DS) procuré sont sécurisés.

2. Procédé selon la revendication 1, dans lequel la phase préalable d'authentification du dispositif (SDAP) est exécutée par l'utilisateur (USER).

3. Procédé selon l'une des revendications 1 et 2, qui comporte dans le temps plusieurs phases opérationnelles (OP), dans lequel une phase préalable d'authentification du dispositif (SDAP) est exécutée avant chaque phase opérationnelle (OP).

4. Procédé selon l'une des revendications 2 et 3 en ce qu'elle dépend de la revendication 2, dans lequel la phase préalable d'authentification du dispositif (SDAP) par l'utilisateur (USER), repose sur un processus d'authentification question-réponse, moyennant un secret d'authentification du dispositif (SDAS) qui est une question préalable (PQ) de l'utilisateur (USER) au dispositif (DE) et une réponse préalable (PA) du dispositif (DE) à l'utilisateur (USER) à la question préalable (PQ), la question préalable (PQ) et la réponse préalable (PR) étant secrètes pour n'être connues ou accessibles que du seul utilisateur (USER) authentique, de sorte que l'authenticité du dispositif (DE) n'est avérée que si et seulement si l'utilisateur (USER) vérifie qu'il y a identité entre, d'une part, la réponse apportée (ADS) par le dispositif (DE) à la question préalable (PQ) et d'autre part la réponse préalable (PA).

5. Procédé selon l'une des revendications 1 à 4, dans lequel la phase préliminaire de configuration (SDCP) configure le dispositif (ED) avec le secret d'authentification du dispositif (SDAS).

6. Procédé selon la revendication 5, dans lequel la phase préliminaire de configuration (SDCP) du dispositif (DE) est exécutée par l'utilisateur (USER).

7. Procédé selon l'une des revendications 5 et 6 en ce qu'elle dépend de la revendication 5, tel que la configuration du dispositif (DE) avec la question préalable (PQ) et la réponse préalable (PA) est exécutée à partir d'une question de l'utilisateur (USER), grâce à un processus générateur de question à réponse.

8. Procédé selon l'une des revendications 5 à 7 en ce qu'elles dépendent de la revendication 5, dans lequel la phase préalable d'authentification du dispositif (SDAP) est exécutée après que la phase préliminaire de configuration (SDCP) a été exécutée, et sous la condition de l'absence d'exécution, entre temps, de toute autre phase préalable d'authentification du dispositif (SDAP) ou d'une phase opérationnelle (OP).

9. Procédé selon l'une des revendications 5 à 7 en ce qu'elles dépendent de la revendication 5, dans lequel la phase préalable d'authentification du dispositif (SDAP) est exécutée après que la phase préliminaire de configuration (SDCP) a été exécutée, et sous la condition de l'exécution entre temps, d'une ou de plusieurs autres phases préalables d'authentification du dispositif (SADP) ou de phases opérationnelles (OP).

10.Procédé selon l'une des revendications 5 à 7 en ce qu'elles dépendent de la revendication 5, dans lequel à une phase préliminaire de configuration (SDCP) est associée de façon nécessaire et suffisante soit une seule phase préalable d'authentification du dispositif (SDAP) soit une pluralité préfixée de phases préalables d'authentification du dispositif (SDAP) successives soit une pluralité illimitée de phases préalables d'authentification du dispositif (SDAP) successives.

11.Procédé selon l'une des revendications 1 à 10, dans lequel l'étape préliminaire d'authentification de l'utilisateur (UAP) par le dispositif (DE) repose sur un secret d'authentification de l'utilisateur (UAS) qui est une réponse opérationnelle de l'utilisateur (OA) au dispositif (DE), secrète pour n'être connue et accessible que du seul utilisateur (USER) authentique, de sorte que l'authenticité de l'utilisateur (USER) n'est avérée que si et seulement si le dispositif (DE) vérifie qu'il y a identité entre, d'une part, la réponse apportée par l'utilisateur (AU) et, d'autre part, la réponse opérationnelle (OA).

12.Procédé selon l'une des revendications 4 à 11 en ce qu'elles dépendent de la revendication 4, dans lequel la question préalable (PQ) et la réponse opérationnelle (OA) sont différentes.

13.Procédé selon l'une des revendications 1 à 12, qui comprend une étape de suppression des données sensibles ou confidentielles (DA) du dispositif (DE), exécutée automatiquement à l'issue d'un nombre préfixé d'exécution de phases préalables d'authentification du dispositif (SDAP) successives où le dispositif (DE) n'est pas avéré authentique.

14. Procédé selon la revendication 13 dont l'étape de suppression des données sensibles ou confidentielles (DA) du dispositif (DE) efface également la question préalable (PQ) et la réponse préalable (PA) lorsque à l'issue d'un nombre préfixé d'exécution de phases préalables d'authentification du dispositif ou du système SDAP successives, l'utilisateur USER a échoué à fournir la question préalable (PQ) correspondant à la réponse préalable (PA), de telle sorte le dispositif ED ou le système ES considérera que l'utilisateur n'est pas l'utilisateur authentique.

15.Procédé d'exploitation par un utilisateur (USER) d'un dispositif (DE) électronique fonctionnel commandable par l'utilisateur (USER) afin qu'il lui procure un service déterminé (DS), le dispositif (DE) contenant des données sensibles ou confidentielles (DA), dans lequel - dans une phase opérationnelle (OP) déclenchée par l'utilisateur (USER) et incluant une étape préliminaire d'authentification de l'utilisateur (UAP) par le dispositif (DE) -, le dispositif (DE) exécute une opération spécifique (SO) appropriée pour procurer le service (DS), le procédé d'exploitation étant caractérisé en ce qu'il comporte, en outre, avant toute phase opérationnelle (OP), une phase préalable d'authentification du dispositif (SDAP) dans laquelle est vérifiée l'authenticité du dispositif (DE), de sorte que :

- si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (DE) est avéré authentique, l'utilisateur (USER) peut exécuter la phase opérationnelle (OP),
- si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (DE) n'est pas avéré authentique, l'utilisateur (USER) peut empêcher l'exécution de la phase opérationnelle (OP), en sorte que, d'abord le dispositif (DE), puis l'utilisateur (USER), sont authentifiés et que l'opération exécutée et le service (DS) procuré sont sécurisés.

16.Dispositif (DE) électronique fonctionnel, commandable par un utilisateur (USER) en vue d'un service déterminé (DS), contenant des données sensibles ou confidentielles (DA), spécialement agencé pour la mise en œuvre du procédé d'authentification mutuelle selon l'une quelconque des revendications 1 à 13 et pour la mise en œuvre du procédé d'exploitation selon la revendication 15, notamment pour exécuter une phase préalable d'authentification du dispositif (SDAP).

17.Dispositif (DE) selon la revendication 16, configuré à l'issue d'une phase préliminaire de configuration (SDCP) avec le secret d'authentification du dispositif (SDAS), qui est une question

préalable de l'utilisateur (PQ) au dispositif (DE) et une réponse préalable du dispositif (PA) à l'utilisateur (USER) à la question préalable (PQ).

18.Dispositif (DE) selon la revendication 16, comprenant, d'une part, le secret d'authentification du dispositif (SDAS) et, d'autre part, le secret d'authentification de l'utilisateur (UAS).

19.Procédé d'authentification mutuelle d'un système (ES) électronique fonctionnel, commandable par un utilisateur (USER) en vue d'un service déterminé (DS), contenant des données sensibles ou confidentielles (DA), comprenant une pluralité de dispositifs (DE) électroniques associés fonctionnellement entre eux, agencé de manière à - dans une phase opérationnelle (OP) déclenchée par l'utilisateur (USER) et incluant une étape où le système (ES) authentifie l'utilisateur (USER) -, exécuter une opération (SO) ou une série d'opérations (SO) spécifique appropriée pour procurer le service (DS), le procédé comportant, en outre, avant toute phase opérationnelle (OP), une phase préalable d'authentification du système (ES), dans laquelle est vérifiée l'authenticité de tout ou partie de la pluralité des dispositifs (DE) que le système (ES) comprend, moyennant la mise en œuvre, pour chaque dispositif (DE) vérifié, du procédé d'authentification selon l'une des revendications 1 à 13.

20.Procédé selon la revendication 19, avec une pluralité de dispositifs (DE) électroniques formant une ou plusieurs chaînes fonctionnelles avec un ou des dispositifs (DE) amont et un ou des dispositifs (DE) aval, dans lequel :

- si à l'issue de la phase préalable d'authentification d'un dispositif (DE) amont d'une chaîne de dispositifs (DE), ce dispositif (DE) est avéré authentique, il est procédé à l'authentification du ou des dispositifs (DE) aval de la même chaîne de dispositifs (DE),
- si à l'issue de la phase préalable d'authentification d'un dispositif (DE) amont d'une chaîne de dispositifs (DE), ce dispositif (DE) n'est pas avéré authentique, il n'est pas procédé à l'authentification du ou des dispositifs (DE) aval de la même chaîne de dispositifs (DE), le système (ES) étant avéré non authentique.

21.Procédé d'exploitation par un utilisateur (USER) d'un système (ES) électronique fonctionnel commandable par l'utilisateur (USER) afin qu'il lui procure un service déterminé (DS), le système (ES) contenant des données sensibles ou confidentielles (DA), comprenant une pluralité de dispositifs (DE) électroniques associés fonctionnellement entre eux, dans lequel - dans une phase opérationnelle (OP) déclenchée par l'utilisateur (USER) et incluant une étape préliminaire d'authentification de l'utilisateur (UAP) par le système (ES) -, le système (ES) exécute une opération (SO) ou une série d'opérations (SO) spécifique appropriée pour procurer le service (DS), le procédé d'exploitation étant caractérisé en ce qu'il comporte, en outre, avant toute phase opérationnelle (OP), une phase préalable d'authentification du système (SDAP) dans laquelle est vérifiée l'authenticité de tout ou partie de la pluralité des dispositifs (DE) que le système (ES) comprend, moyennant la mise en œuvre, pour

chaque dispositif (DE) vérifié, du procédé d'authentification selon l'une des revendications 1 à 13, de sorte que :

- si à l'issue de la phase préalable d'authentification du système (ES), le système (ES) est avéré authentique, l'utilisateur (USER) peut exécuter la phase opérationnelle (OP),
- si à l'issue de la phase préalable d'authentification du système (ES), le système (ES) n'est pas avéré authentique, l'utilisateur (USER peut empêcher l'exécution de la phase opérationnelle (OP),

en sorte que d'abord le système (ES) puis l'utilisateur (USER) sont authentifiés et que l'opération exécutée (SO) et le service (DS) procuré sont sécurisés.

22.Système (ES) électronique fonctionnel, commandable par un utilisateur (USER) en vue d'un service déterminé (DS), contenant des données sensibles ou confidentielles (DA), comprenant une pluralité de dispositifs (DE) électroniques associés fonctionnellement entre eux, selon l'une des revendications 16 à 18, spécialement agencé pour la mise en œuvre du procédé d'authentification mutuelle selon l'une des revendications 19 et 20 et pour la mise en œuvre du procédé d'exploitation selon la revendication 21, notamment pour exécuter une phase préalable d'authentification (SDAP) de tout ou partie de la pluralité des dispositifs (DE) que le système (ES) comprend.

Figure 1 :

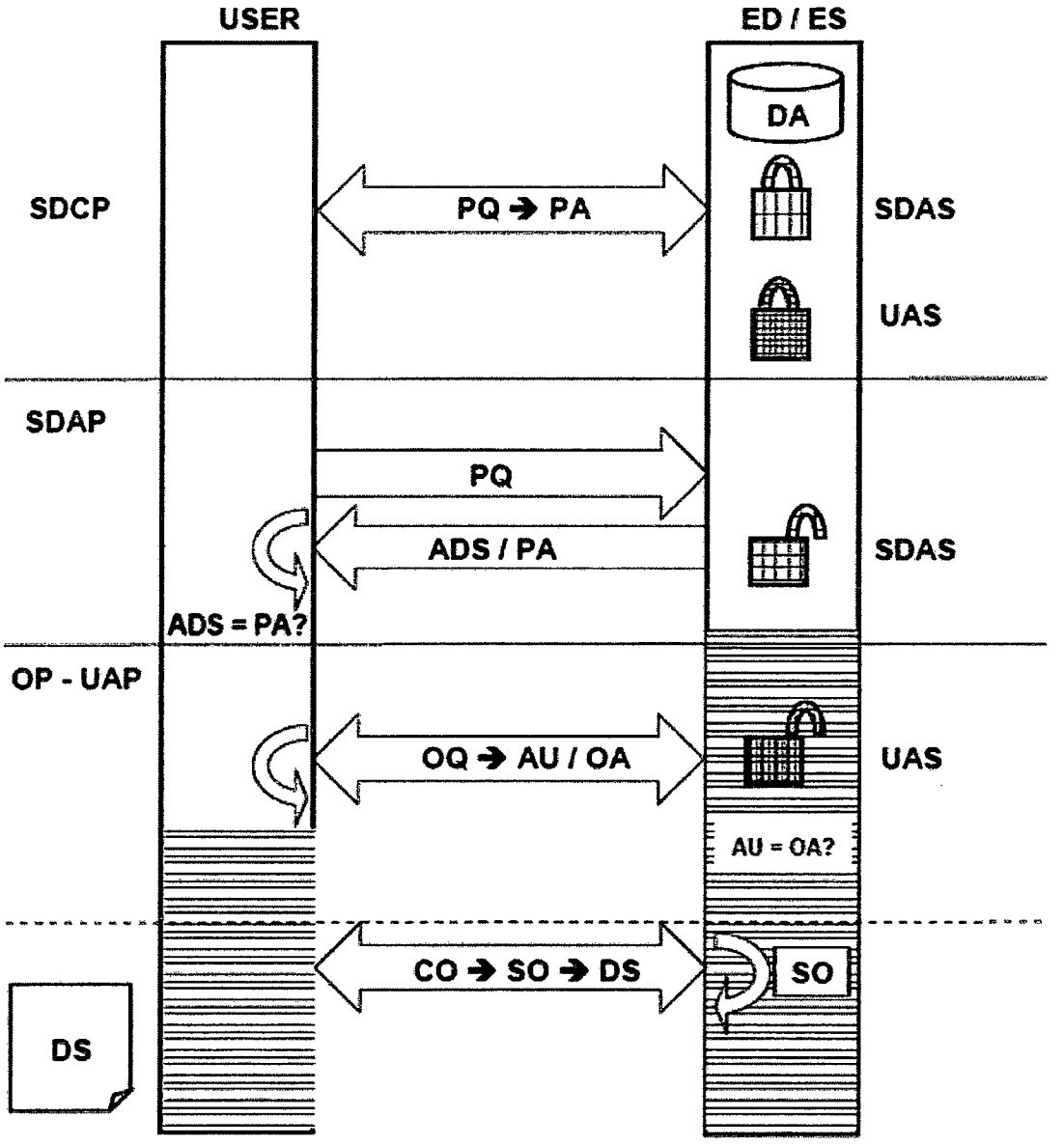
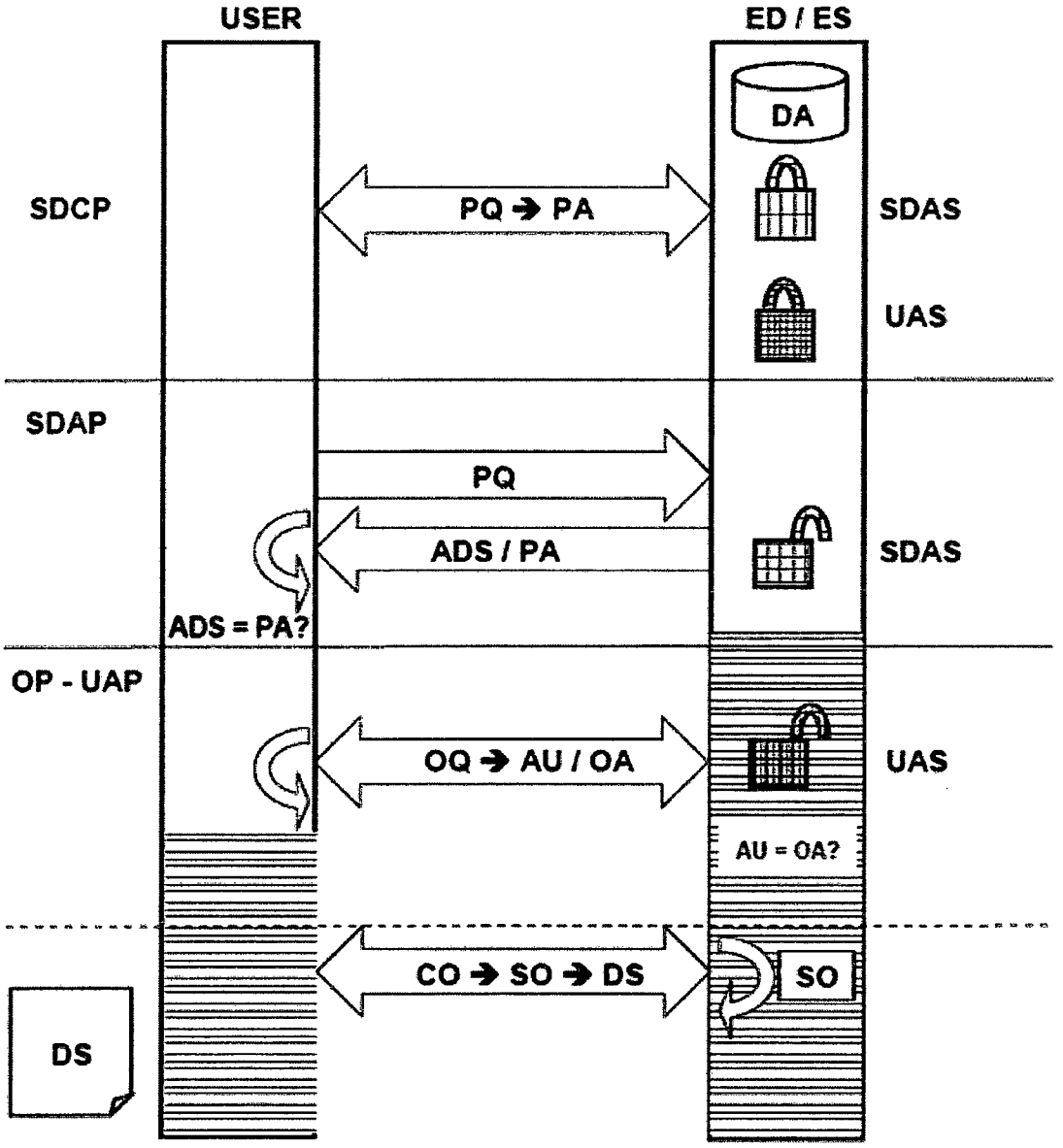

USER
ED / ES
DA
SDCP
PQ → PA
SDAS
UAS
SDAP
PQ
ADS / PA
SDAS
ADS = PA?
OP - UAP
OQ → AU / OA
UAS
AU = OA?
CO → SO → DS
SO
DS

Figure 1 :


USER
ED / ES
DA
SDCP
PQ → PA
SDAS
UAS
SDAP
PQ
ADS / PA
SDAS
ADS = PA?
OP - UAP
OQ → AU / OA
UAS
AU = OA?
CO → SO → DS
SO
DS