

PROCÉDE DE CONTROLE D'INDIVIDUS A AUTHENTIFICATION SIMPLIFIEE

DOMAINE DE L'INVENTION

L'invention concerne un procédé de contrôle d'un individu disposant d'un document d'identité sur un support comprenant une puce électronique dans laquelle est stockée une donnée biométrique de référence de l'individu et apte à afficher une zone de lecture automatique représentant une donnée de lecture optique du document d'identité. L'invention s'applique notamment au contrôle d'individus pour l'accès à une zone ou un service protégé tel que l'accès à l'embarquement d'un avion.

10

ETAT DE LA TECHNIQUE

Un contrôle d'identité est parfois exigé lorsqu'un individu accède à une zone ou à un service protégé, comme par exemple lors du passage d'une frontière ou lors d'un embarquement dans un avion.

Des documents d'identité électroniques tels que passeports ou cartes d'identités électroniques permettent de mettre en œuvre un contrôle d'identité par authentification biométrique, c'est-à-dire par comparaison d'une donnée biométrique acquise sur un trait biométrique de l'individu à une donnée biométrique préenregistrée dans une puce contenue dans le document d'identité.

De tels documents permettent un accroissement de sécurité car la donnée biométrique qui est contenue dans le document peut être protégée et signée par une entité officielle ayant délivré le document, ce qui peut être vérifié lors du contrôle.

Ils permettent également d'automatiser les contrôles d'identité effectués, au moyen de dispositifs de contrôle dédiés, en laissant les individus manipuler eux-mêmes leurs passeports pour les soumettre, pour lecture, à un dispositif de contrôle.

Cependant, la manipulation physique de documents d'identités, et notamment de documents sous forme de livret comme les passeports, peut poser des difficultés à l'individu souhaitant s'identifier.

En effet, les données biométriques contenues dans les documents d'identité sont protégées en lecture. Il est nécessaire pour y accéder d'obtenir le numéro du document d'identité, qui figure sur une zone de lecture automatique, également appelée MRZ (pour l'acronyme de l'anglais Machine-Readable Zone). Une telle zone de lecture automatique est une partie de la surface du document (ou, le cas échéant, d'une de ses pages) comportant du texte imprimé dans un format normalisé, de sorte

à pouvoir être lu par un ordinateur et déchiffré par reconnaissance optique des caractères imprimés.

Par conséquent, pour pouvoir réaliser l'authentification, l'individu doit présenter le document à la page particulière sur laquelle se trouve la zone de lecture automatique, dans une direction spécifique permettant à un lecteur du dispositif de contrôle de la lire. Une fois le numéro acquis, il peut être utilisé pour accéder au contenu de la puce.

Par conséquent, à défaut de présenter correctement le document d'identité, l'authentification de l'individu peut échouer.

Cette étape de manipulation physique est chronophage et tend à engorger les files d'attentes, par exemple dans les aéroports. Elle est de plus la cause d'une proportion substantielle des échecs à l'authentification des individus.

Il est par conséquent nécessaire, pour désengorger les files d'attente au niveau des points de passage, de limiter autant que possible les manipulations de ces documents pour authentifier un individu lors d'un contrôle.

Une solution à cette problématique a déjà été proposée. Elle prévoit de scinder en deux l'étape de contrôle de l'individu, en une première étape lors de laquelle une manipulation du document d'identité est nécessaire, et une seconde étape lors de laquelle l'authentification a lieu, sans manipulation du document d'identité.

Plus précisément, lors d'une première étape, un individu manipule son passeport pour le positionner correctement sur un lecteur d'un dispositif de contrôle, qui lit la zone de lecture automatique du passeport, et accède à la donnée biométrique, en l'occurrence une image du visage de l'individu, contenue dans le passeport.

Un numéro est associé à cette donnée biométrique, et un ticket portant ce numéro est délivré à l'individu. La donnée ainsi que le numéro sont enregistrés dans une base de données.

Lors de la deuxième étape, l'individu présente le ticket à un deuxième dispositif de contrôle. Ce dispositif lit le numéro inscrit sur le ticket et accède à la base de données pour récupérer la donnée biométrique correspondante.

Dans le même temps, une photographie de l'individu est prise par le dispositif de contrôle, et cette photographie est comparée à la donnée biométrique récupérée de la base (et qui correspond à celle stockée dans le passeport) pour faire l'authentification biométrique de l'individu.

Cette solution permet donc de déplacer l'étape chronophage de manipulation du passeport en amont de l'étape d'authentification qui permet l'accès à la zone sécurisée, et de désengorger la file d'attente pour cette étape.

Cependant, cette solution ne résout pas complètement le problème, car le
5 ticket délivré à l'individu représente un document supplémentaire à conserver, qui peut être perdu ou échangé. De plus, il est tout de même nécessaire de manipuler ce ticket lors de la deuxième étape, ce qui peut encore prendre du temps et provoquer des erreurs.

Plus récemment, il a été proposé dans le document EP3249569 une
10 optimisation du processus. Pour cela, lors de chaque étape on prend une photographie de l'individu, pour que lors de la deuxième étape on récupère, dans la base de données, le numéro de document d'identité correspondant au trait biométrique de l'individu.

Ainsi on supprime la manipulation du document d'identité ou même d'un
15 document supplémentaire (ticket) lors de la deuxième étape comprenant l'authentification biométrique de l'individu, ce qui simplifie et accélère le franchissement de cette étape.

Cette solution apporte entière satisfaction, mais il serait souhaitable de
l'alléger encore, et ce tout en conservant une sécurité totale.

20

PRESENTATION DE L'INVENTION

L'invention a pour but de remédier à la problématique décrite ci-avant. En particulier, l'un des buts de l'invention est de proposer un procédé de contrôle automatique minimisant la manipulation de documents par l'individu.

25 Un autre but de l'invention est de réduire le temps nécessaire pour la mise en œuvre de l'étape d'authentification.

Un autre but de l'invention est de proposer un procédé de contrôle qui soit de mise en œuvre simple et pratique pour les individus.

30 A cet égard l'invention a pour objet un procédé de contrôle d'un individu disposant d'un document d'identité sur un support comprenant une puce électronique dans laquelle est stockée une donnée biométrique de référence de l'individu et apte à afficher une zone de lecture automatique représentant une donnée de lecture

optique du document d'identité, le procédé comprenant la mise en œuvre par un dispositif de contrôle d'étapes de :

- (a) acquisition d'une donnée biométrique candidate sur un trait biométrique de l'individu ;
- 5 (b) à partir de la donnée biométrique candidate, récupération, dans une mémoire, d'une donnée de lecture optique associée à la donnée biométrique de référence correspondant au trait biométrique de l'individu ;
- 10 (c) ouverture d'un canal de communication sécurisé avec la puce électronique du support du document d'identité de l'individu en utilisant ladite donnée de lecture optique récupérée.

Selon des caractéristiques avantageuses et non-limitatives :

15 L'étape (c) ne comprend ni la récupération de la donnée biométrique de référence de l'individu depuis ladite puce électronique via ledit canal de communication sécurisé ni la lecture de ladite zone de lecture automatique du support du document d'identité.

L'étape (c) comprend la mise en œuvre d'une authentification de ladite puce électronique via ledit canal de communication sécurisé.

20 Ladite puce électronique stocke une paire d'une clé privée et d'une clé publique, ladite authentification de ladite puce électronique étant choisie parmi une authentification active et une authentification matérielle.

Ladite authentification de ladite puce électronique est une authentification active comprenant la vérification en utilisant ladite clé publique d'une signature électronique reçue depuis la puce électronique en réponse à l'envoi d'un nonce.

Aucune donnée autre que les données nécessaires à ladite authentification de la puce électronique n'est transmise via ledit canal de communication sécurisé.

Ledit canal sécurisé est ouvert conformément à un protocole choisi parmi Basic Access Control, BAC, et Password Authenticated Connection Establishment, PACE, en utilisant une clé dérivée de ladite donnée de lecture optique récupérée.

L'étape (b) comprend :

- une comparaison des données biométriques de référence stockées dans la mémoire avec la donnée biométrique candidate, et

- la sélection d'au moins une donnée de lecture optique de document d'identité correspondant à au moins une donnée biométrique de référence présentant un taux de similarité avec la donnée biométrique candidate supérieure à un seuil prédéterminé.

5 Si plus d'une donnée de lecture optique de document d'identité a été sélectionnée, l'étape (c) est tentée pour chaque donnée de lecture optique sélectionnée jusqu'à l'ouverture du canal de communication sécurisée.

Le dispositif de contrôle comprend des moyens de communication sans contact, l'étape (c) étant mise en œuvre en approchant ledit support du dispositif de
10 contrôle dans une orientation quelconque.

Le procédé comprend une étape (a0) préalable mise en œuvre par un dispositif d'enrôlement, de récupération de la donnée biométrique de référence de l'individu depuis ladite puce électronique ; d'acquisition de la donnée de lecture optique du document d'identité par lecture de la zone de lecture automatique ; et
15 d'enregistrement, dans ladite mémoire (20) distante, de la donnée de lecture optique du document d'identité en lien avec la donnée biométrique de référence de l'individu.

Le document d'identité est un passeport, et :

- lors de l'étape (a0), le passeport est présenté ouvert à la page de la zone de lecture automatique auprès dispositif du d'enrôlement pour la mise en œuvre
20 de l'acquisition de la donnée de lecture optique du document d'identité, et
- lors de l'étape (c), le passeport est présenté fermé auprès du dispositif de contrôle.

Selon un deuxième aspect, l'invention concerne un dispositif de contrôle d'un
25 individu disposant d'un document d'identité sur un support comprenant une puce électronique dans laquelle est stockée une donnée biométrique de référence de l'individu et apte à afficher une zone de lecture automatique représentant une donnée de lecture optique du document d'identité, configuré pour la mise en œuvre d'étapes de :

- 30 (a) acquisition d'une donnée biométrique candidate sur un trait biométrique de l'individu ;
- (b) à partir de la donnée biométrique candidate, récupération, dans une mémoire, d'une donnée de lecture optique associée à une donnée

biométrique de référence correspondant au trait biométrique de l'individu ;

- (c) ouverture d'un canal de communication sécurisé avec la puce électronique du support du document d'identité de l'individu en utilisant ladite donnée de lecture optique récupérée.

Selon un troisième aspect, l'invention concerne un système de contrôle d'individus, comprenant :

- une mémoire,
- un dispositif de contrôle selon le deuxième aspect, et
- un dispositif d'enrôlement, configuré pour la mise en œuvre d'étapes de récupération de la donnée biométrique de référence de l'individu depuis ladite puce électronique ; d'acquisition de la donnée de lecture optique du document d'identité par lecture de la zone de lecture automatique ; et d'enregistrement, dans ladite mémoire distante, de la donnée de lecture optique du document d'identité en lien avec la donnée biométrique de référence de l'individu.

Selon un quatrième et un cinquième aspect, l'invention concerne un produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon le premier aspect de contrôle d'un individu ; et un moyen de stockage lisible par un équipement informatique sur lequel un produit programme d'ordinateur comprend des instructions de code pour l'exécution d'un procédé selon le premier aspect de contrôle d'un individu.

DESCRIPTION DES FIGURES

D'autres caractéristiques, buts et avantages de la présente invention apparaîtront à la lecture de la description détaillée qui va suivre, au regard des figures annexées, données à titre d'exemples non limitatifs et sur lesquelles :

- La figure 1 représente schématiquement un système de contrôle pour la mise en œuvre du procédé selon l'invention,
- La figure 2 représente schématiquement les principales étapes d'un mode de réalisation préféré du procédé de contrôle selon l'invention.

DESCRIPTION DETAILLEE D'AU MOINS UN MODE DE REALISATION DE L'INVENTION

Architecture

5

En référence à la figure 1, un système de contrôle d'individus 1 est représenté. Ce système permet de réaliser l'authentification biométrique d'individus pour autoriser ou interdire l'accès d'individus à une zone ou à un service sécurisé.

Pour pouvoir effectuer le contrôle, l'individu doit disposer d'un document d'identité physique ou dématérialisé. Dans les deux cas il dispose d'un support physique du document d'identité

Selon un premier mode de réalisation, le document d'identité est un document physique (i.e. le support est le document), tel qu'un passeport ou une carte d'identité, voire une carte à puce (« smartcard »), comprenant une puce électronique, par exemple une puce RFID, dans laquelle est stockée au moins une donnée biométrique, acquise à partir d'un trait biométrique de l'individu.

La donnée biométrique contenue dans le document d'identité est dans la suite qualifiée de donnée biométrique de référence (par opposition à une donnée biométrique candidate, acquise à la volée sur l'individu).

La puce électronique stocke généralement également des données alphanumériques variées de l'individu, qui sont en pratique imprimées sur le support du document d'identité s'il est « physique », dites « données visuelles », choisies notamment parmi :

- Numéro complet du document d'identité ;
- Date d'expiration ;
- Date de délivrance ;
- Nom ;
- Prénom(s) ;
- Nationalité ;
- Date de Naissance ;
- Lieu de Naissance ;
- Sexe ;
- Taille ;
- Adresse ;

○ Etc.

Chaque document d'identité dispose en outre d'une zone de lecture automatique représentant une donnée de lecture optique (c'est-à-dire destinée à être facilement transmise de manière visuelle à des ordinateurs), par exemple de type
5 MRZ, QR code ou PDF417, également imprimée sur le support pour un document physique. La zone de lecture automatique d'un document est réservée à la lecture, à l'identification et à la validation de ce document.

On distinguera la donnée de lecture optique, qui est une donnée numérique (laquelle est généralement également stockée dans la puce électronique) codant pour
10 un ensemble d'information et en particulier certaines desdites données visuelles (au moins le numéro du document d'identité, la date de naissance de l'individu, et/ou la date d'expiration du document d'identité, en pratique leur concaténation), référencées « DG1 » dans les spécifications de l'ICAO (la donnée biométrique de référence est référencée « DG2 », et un certain nombre d'informations optionnelles sont
15 référencées DG3 à DG16) ; de sa représentation pour lecture optique, qui est la zone de lecture automatique, en un format lisible par un ordinateur ou toute unité de traitement équivalente pouvant mettre en œuvre une acquisition optique et une extraction de la donnée de lecture optique et son décodage. En d'autres termes, la donnée de lecture optique est le contenu de la zone de lecture optique.

20 Dans le cas de MRZ, la représentation de la donnée de lecture optique est une chaîne de caractère (et sa lecture implique une reconnaissance optique de caractères) et dans le cas de QR code il s'agit d'un code barre 2D. Dans la suite de la présente description, on décrira l'exemple préféré de la MRZ, et par abus de langage, on désignera MRZ la donnée de lecture optique correspondante. La MRZ
25 (en français ZLA) est normalisée par l'OACI (OACI/ICAO 9303), reprise dans la norme ISO/CEI 7501-1:2008 (et le supplément OACI).

Dans le cas préféré d'un passeport, ce document se présente sous la forme d'un livret comprenant des couvertures et un ensemble de pages, la zone de lecture automatique (au format MRZ) figurant sur l'une des pages du livret, impliquant
30 l'ouverture à la bonne page et le positionnement correct du passeport pour la lecture de cette zone.

Selon un deuxième mode de réalisation, le document d'identité est dématérialisé sur un terminal de l'utilisateur tel qu'un smartphone ou une montre

connectée, i.e. le support du document est ledit terminal, mais on retrouve en pratique également une puce électronique (un processeur du terminal et des moyens de stockage - par exemple une mémoire flash) et les mêmes données. Un tel terminal comprend préférentiellement des moyens de communication sans contact
5 (typiquement NFC, mais également BLE, voire UWB, et de façon générale toute communication radio de proximité) permettant de reproduire exactement le fonctionnement d'une puce RFID telle que celle d'un passeport.

La seule différence avec un document d'identité physique est que si le document « dématérialisé » comporte également la même donnée de lecture optique,
10 la zone de lecture automatique (sa représentation MRZ, QR code ou PDF417), n'est pas imprimée sur le support et seulement affichable sur demande. Plus précisément, cette donnée est également stockée dans les moyens de stockage du terminal, pour affichage sur une interface du terminal. Cet affichage vient avantageusement reproduire l'aspect original d'un document d'identité physique, par exemple en
15 affichant toute la page du passeport équivalent.

En résumé, on comprendra que quel que soit son format, le support du document d'identité de l'individu comprend toujours une puce électronique dans laquelle est stockée une donnée biométrique de référence de l'individu, et permet toujours la fourniture visuelle d'une donnée de lecture optique du document d'identité,
20 qu'elle soit simplement affichée ou physiquement imprimée sur le support.

Le système de contrôle d'individus peut par exemple permettre de contrôler des individus avant d'embarquer à bord d'un avion ou avant de franchir la frontière d'un pays.

25 Le système de contrôle d'individus 1 comprend un dispositif de contrôle 30, une mémoire 20, et potentiellement un dispositif d'enrôlement 10.

Le dispositif de contrôle 30 est avantageusement disposé en entrée d'une zone d'accès sécurisé. Il peut prendre la forme d'un portique dont le franchissement par l'individu n'est autorisé qu'en cas de succès du contrôle.

30 Le dispositif d'enrôlement 10 est avantageusement une structure de contrôle fixe telle qu'un kiosque, possiblement située dans la même infrastructure (par exemple le même bâtiment) que le dispositif de contrôle 30 et à distance de celui-ci (dans le cas d'un contrôle dans un aéroport précédant l'embarquement dans un avion, le dispositif d'enrôlement peut être situé dans le même terminal de départ que le

dispositif de contrôle. Cependant, il n'est pas situé dans la file d'attente du dispositif de contrôle pour pouvoir scinder le flux des individus utilisant les deux dispositifs), mais alternativement dans un bâtiment officiel tel qu'une mairie ou tout autre entité de confiance. En effet, comme l'on verra, il n'y a besoin que d'une seule utilisation
5 initiale du dispositif d'enrôlement, qui doit être sécurisée, et ensuite le présent procédé de contrôle d'un individu peut être mis en œuvre un grand nombre de fois. Pour reformuler, il n'y a pas besoin d'un enrôlement avant chaque contrôle, contrairement aux procédés connus de l'état de la technique

10 Le dispositif d'enrôlement 10 comporte un calculateur 11, tel que par exemple un processeur, un microprocesseur, un contrôleur, etc.

Il comporte également un module 12 de lecture du contenu de la donnée de lecture optique d'un document. Le module 12 peut par exemple comprendre un capteur d'image 13, tel que par exemple un appareil photographique numérique ou
15 une caméra numérique, adapté pour acquérir une image de la zone de lecture automatique, et un module 14 de reconnaissance de caractères. Le module 14 peut être une application logicielle exécutable par le calculateur 11 ou alternativement un module matériel. Ceci peut être le cas lorsque par exemple le dispositif de contrôle est le téléphone mobile ou la tablette ou l'ordinateur personnel de l'individu, et que ce
20 dispositif est configuré pour réaliser la reconnaissance de caractères. En variante, le traitement de l'image de la zone de lecture automatique peut être réalisé à distance si le dispositif de l'individu ne dispose pas de cette fonctionnalité. Dans ce cas, le module 14 peut être une application logicielle exécutable par un calculateur d'une autre unité de traitement distante du dispositif d'enroulement (non représentée), et le
25 dispositif d'enrôlement 10 comprend alors une interface de communication avec l'unité de traitement distante permettant de lui envoyer l'image de la zone de lecture automatique sur laquelle la reconnaissance de caractères doit être effectuée.

Le dispositif d'enrôlement 10 comprend en outre un lecteur 16 de puce d'un document d'identité. Typiquement, soit la puce contenue dans le support du
30 document d'identité est une puce radiofréquence (par exemple une étiquette de radio-identification RFID ou une puce UHF), soit le support comprend des moyens de communication sans contact (de type NFC, etc.), et le lecteur 16 est adapté pour lire le contenu de la puce à distance, par une communication radiofréquences avec la puce.

Enfin le dispositif d'enrôlement 10 comprend une interface de communication 15 à distance avec une mémoire 20 du système de contrôle 1. Cette interface permet au calculateur 11 d'échanger des informations avec la mémoire 20. La mémoire 20 est avantageusement distante du dispositif d'enrôlement 10. Par conséquent

5 l'interface de communication 15 est de préférence la combinaison d'une interface de communication filaire, par exemple Ethernet, ou sans fil, par exemple de type Wifi ou Bluetooth ou réseau de téléphonie mobile (GPRS, 3G, 4G ou autre) et de tout autre réseau de communication aval faisant le lien avec le mémoire 20.

Avantageusement, mais facultativement, le dispositif d'enrôlement 10 peut

10 enfin comprendre une interface de saisie d'informations 17 telle qu'un clavier, un écran tactile, etc.

Le dispositif de contrôle 30 comprend un calculateur 31, qui peut également être un processeur, microprocesseur, contrôleur, etc.

15 En outre le dispositif de contrôle 30 comprend un module 32 d'acquisition d'une donnée biométrique sur un trait biométrique d'un individu. Le trait biométrique peut par exemple être la forme du visage, une ou plusieurs empreintes digitales de l'individu, ou encore un ou plusieurs iris de l'individu. Il peut encore s'agir de la structure du réseau veineux d'un ou plusieurs doigts ou d'une ou des deux mains, ou

20 des tailles respectives de phalanges ou de doigts.

Le module d'acquisition de la donnée biométrique 32 comprend un capteur d'image 33, et un module 34 de traitement d'images adapté pour extraire une donnée biométrique à partir d'une image d'un trait biométrique. L'extraction de la donnée biométrique est mise en œuvre par un traitement de l'image du trait biométrique qui

25 dépend de la nature du trait biométrique. Des traitements d'images variés pour extraire des données biométriques sont connus de l'Homme du Métier. A titre d'exemple non limitatif, l'extraction de la donnée biométrique peut comprendre une extraction des minuties des empreintes digitales à partir d'une image d'empreintes digitales. En variante, elle peut comprendre une extraction de points particuliers ou

30 d'une forme du visage dans le cas où l'image est une image du visage de l'individu, etc. Alternativement, un réseau de neurones à convolution peut être utilisé.

La mémoire 20 du système de contrôle 1, déjà évoquée ci-avant, peut être une mémoire intégrée au dispositif de contrôle 30. En variante, elle peut être une mémoire distante du dispositif de contrôle 30, avantageusement une base de

données. Dans ce cas, ce dernier comprend également une interface de communication à distance 35 avec la mémoire 20.

Enfin le dispositif de contrôle 30 comprend un lecteur 36 de puce d'un document d'identité. Typiquement, soit la puce contenue dans le support document
5 d'identité est une puce radiofréquence (par exemple une étiquette de radio-identification RFID ou une puce UHF), soit le support comprend des moyens de communication sans contact (de type NFC, etc.), et le lecteur 36 est adapté pour lire le contenu de la puce à distance, par une communication radiofréquences avec la puce.

10 Le dispositif de contrôle 30 peut également comprendre une interface de saisie d'informations 37 telle qu'un clavier, un écran tactile, etc.

Le système 1 est adapté pour mettre en œuvre le procédé de contrôle décrit ci-dessous.

15

Enrôlement

En référence à la figure 2, on a représenté les principales étapes d'un procédé de contrôle d'un individu. Ce procédé permet de vérifier que l'individu qui se présente
20 pour le contrôle correspond à celui à qui le document d'identité a été délivré, en réalisant une authentification biométrique par comparaison d'une donnée biométrique fraîchement acquise sur l'individu avec la donnée biométrique d'authentification stockée dans la puce contenue dans le document.

Le procédé présente avantageusement une étape préalable (a0) d'enrôlement
25 mise en œuvre par le dispositif d'enroulement 10. Comme expliqué, cette étape n'a besoin d'être faite qu'une fois, et ensuite le procédé peut être mis en œuvre sans la comprendre. A noter que de préférence, on prévoira de la remettre en œuvre à intervalles réguliers, par exemple une fois par an, par sécurité.

L'étape (a0) vise à créer une entrée dans la mémoire 20 correspondant au
30 document d'identité de l'individu, et consiste typiquement en la génération d'un DTC de l'individu. Par DTC, Digital Travel Credentials, en français Certificat de Voyage Numérique, on entend un conteneur de la version virtuelle d'un document d'identité, sous une forme reconnue par l'ICAO, voir notamment la présentation <https://www.icao.int/Meetings/TRIP-Symposium->

2019/PublishingImages/Pages/Presentations/Digital%20Travel%20Credentials.pdf.

Pour reformuler, le DTC contient tout ou partie des données susmentionnées d'un document d'identité, en particulier la donnée de lecture optique (DG1) et la donnée biométrique de référence (DG2). Ainsi, l'étape (a0) peut être vue comme une

5 dématérialisation du document d'identité de l'individu. On notera que le fait d'utiliser un terminal comme support du document d'identité implique déjà que le DTC existe et est chargé dans la mémoire du terminal, de sorte que l'étape (a0) n'est théoriquement à mettre en œuvre que dans le cas d'un document d'identité physique.

Ainsi, l'étape (a0) comporte d'abord la récupération de la donnée biométrique

10 de référence de l'individu depuis ladite puce électronique et l'acquisition de la donnée de lecture optique du document d'identité par lecture de la zone de lecture automatique. Cette action est classique et peut être mise en œuvre de manière conventionnelle (c'est ce qui est aujourd'hui souvent fait aux dispositifs de contrôle des aéroports et génère des files d'attentes). Elle nécessite que l'individu manipule le

15 document d'identité pour présenter son document au capteur 13, à la page de la zone de lecture automatique, et avec la zone de lecture automatique en visée de la zone d'acquisition du capteur 13, c'est-à-dire présentée en une position et selon une direction permettant au capteur d'acquérir une image de la zone. Le module 12 de lecture du dispositif d'enrôlement 10 acquiert une image de la zone de lecture

20 automatique et extrait de cette zone la donnée de lecture optique du document. La récupération de la donnée biométrique de référence peut être sensiblement simultanée car la donnée de lecture optique peut être utilisée pour accéder au contenu de la puce et récupérer la donnée biométrique de référence.

En variante, plusieurs données biométriques de l'individu correspondant à

25 différents traits biométriques peuvent être disponibles et récupérées. Par exemple, une première donnée biométrique à partir de l'iris de l'individu, et une deuxième à partir du visage, ou de l'empreinte digitale, etc.

Puis, le dispositif d'enrôlement 10 enregistre, dans ladite mémoire 20, la donnée de lecture optique du document d'identité en lien avec la donnée biométrique

30 de référence de l'individu. A titre d'exemple non limitatif, une donnée peut être générée par le calculateur 11, comprenant la donnée de lecture optique et la donnée biométrique de référence, par exemple sous forme de doublet, et stockée dans la mémoire. Les deux données sont ainsi associées dans la mémoire 20.

Le fait d'enregistrer plusieurs données biométriques en lien avec la donnée de lecture optique du document d'identité peut permettre au procédé d'être compatible avec des technologies différentes mises en œuvre au niveau de points de contrôle différents, ou d'augmenter la sécurité du procédé en utilisant dans la suite du procédé plusieurs données biométriques pour retrouver la donnée de lecture optique.

Avantageusement, mais facultativement, l'étape (a0) du procédé peut également comprendre l'acquisition (ou la récupération depuis la puce électronique, comme pour la donnée biométrique de référence) de données supplémentaires comprenant :

- 10 - Des données d'identité relatives à l'individu, ces données pouvant par exemple être confrontées à des données figurant sur le document d'identité et permettant une sécurité accrue du contrôle (par exemple, nom, prénom(s), date et lieu de naissance),
- 15 - Des données permettant de discriminer l'individu parmi un ensemble d'individus franchissant le même contrôle. Par exemple, dans le cas d'un embarquement pour un vol, les données peuvent comprendre le numéro du vol, le nom de la compagnie aérienne, l'aéroport d'atterrissage et/ou de décollage, etc. En variante, dans le cas d'un passage de frontière, il peut s'agir d'un numéro de visa, d'un pays de provenance, etc. et/ou
- 20 - Une clé publique, par exemple référencée DG14 ou DG15, voir plus loin.

Cette acquisition de données supplémentaires est avantageusement mise en œuvre avant l'enregistrement dans la mémoire, et dans ce cas les données permettant de discriminer l'individu sont aussi enregistrées en même temps en lien avec la donnée de lecture optique du document d'identité et la donnée biométrique de référence de l'individu.

Procédé de contrôle d'individus

Le procédé de contrôle en lui-même est mise en œuvre par le dispositif de contrôle 30. Cette étape peut être mise en œuvre de manière complètement décorrélée de l'enrôlement (a0).

L'individu se présente auprès du dispositif de contrôle 30 et présente au module d'acquisition de donnée biométrique 32 le même trait biométrique que celui à

partir duquel la donnée biométrique de référence a été obtenue. Une donnée biométrique candidate est acquise sur ce trait lors d'une étape (a).

Lors d'une deuxième étape (b), le dispositif de contrôle 30 récupère dans la mémoire 20, à partir de cette donnée biométrique candidate, la donnée de lecture
5 optique du document préalablement enregistré pour le même individu. Pour ce faire, le dispositif recherche dans la mémoire 20 une donnée biométrique de référence correspondant à la donnée biométrique candidate, c'est-à-dire qui a été acquise sur le même trait, par comparaison de la donnée biométrique candidate avec les données biométriques de référence enregistrées dans la mémoire. Une correspondance est
10 établie si un taux de similarité entre deux données biométriques excède un seuil prédéterminé, qui dépend de la façon dont la comparaison est établie et de la nature du trait biométrique. Un exemple non limitatif de mise en œuvre de comparaison entre deux données est par un calcul de distance (distance euclidienne, distance de Hamming, etc.) entre les données.

15 Le dispositif de contrôle 30 récupère alors la donnée de lecture optique de document correspondant à chacune des données biométriques de référence présentant un niveau de correspondance avec la donnée biométrique candidate supérieure audit seuil. Le dispositif de contrôle 30 peut donc récupérer une ou plusieurs données de lecture optique de documents.

20 Si plusieurs données biométriques de référence correspondant à des traits biométriques différents ont été récupérées lors de l'enrôlement (a0), alors soit plusieurs données biométriques candidate sont acquises sur les mêmes traits à l'étape (a) et sont exploitées pour l'étape (b) de recherche de la donnée de lecture optique du document d'identité, ce qui augmente la sécurité, soit une seule donnée
25 biométrique candidate est acquise et utilisée pour l'étape (b). La diversité de données acquises à l'étape (a) permet dans ce cas d'augmenter la compatibilité du procédé avec différents dispositifs de contrôle 30.

Dans le cas où, au cours de l'enrôlement (a0), des données supplémentaires permettant de discriminer l'individu ont été enregistrées en lien avec la première
30 donnée biométrique et le numéro du document, l'étape (a) peut comprendre en outre l'acquisition des données supplémentaires, au cours de laquelle l'individu saisit à nouveau la ou les même(s) donnée(s) que lors de l'enrôlement (a0). Avantagusement, cette saisie n'est pas nécessaire si ces données supplémentaires sont intrinsèquement et donc préalablement connues par le dispositif de contrôle 30,

par exemple du fait de sa localisation si ces données désignent l'aéroport dans lequel est situé le dispositif de contrôle 30.

Les éventuelles données supplémentaires sont avantageusement utilisées à l'étape (b) pour restreindre l'ensemble des données biométriques de référence de la mémoire à comparer avec la donnée biométrique candidate, en ne sélectionnant que
5 les données biométriques enregistrées dans la mémoire en lien avec les mêmes données supplémentaires (par exemple, même pays d'origine, etc.).

Ceci accélère la mise en œuvre de l'étape (b) et réduit le nombre de données de lecture optique de documents obtenues à la fin de cette étape.

10 Puis le procédé comprend une étape (c) principale au cours de laquelle l'individu présente son document au lecteur 36 du dispositif de contrôle 30. Dans cette étape (c), le dispositif de contrôle 30 ouvre, ou du moins tente d'ouvrir, un canal de communication sécurisé avec la puce électronique du support du document d'identité de l'individu en utilisant ladite donnée de lecture optique récupérée.

15 L'astuce est que l'étape (c) ne comprend ni la récupération de la donnée biométrique de référence de l'individu depuis ladite puce électronique via ledit canal de communication sécurisé, ni la lecture de ladite zone de lecture automatique du support du document d'identité.

Tout d'abord, comme le lecteur 36 interagit seulement avec la puce
20 électronique, et pas la zone de lecture automatique, il n'est pas nécessaire de présenter le document ouvert ou dans une direction particulière. En particulier, le passeport peut être présenté fermé, dans n'importe quelle orientation. Ceci implique un gain de temps considérable pour l'individu, qui n'a pas besoin de manipulation particulière du document d'identité, ou de tout autre document dont une zone de
25 lecture ou un code-barres devrait être lu(e) et supprime les risques d'échecs liés à cette manipulation.

Mais surtout, en temps normal, le dispositif de contrôle 30 aurait du lire le contenu de la puce du document pour récupérer la donnée biométrique d'authentification à partir de la ou les données de lecture optique qu'il détient, ce qui
30 prend un temps assez long.

En l'espèce, l'authentification biométrique a en fait déjà eu lieu, puisqu'on a pu identifier au moins une donnée biométrique de référence correspondant à la donnée biométrique candidate, et on veut juste vérifier cette authentification (et

identifier l'individu de manière unique s'il y avait encore ambiguïté) et s'assurer que l'individu possède bien le document d'identité correspondant.

Ici on se contente de vérifier qu'on peut ouvrir le canal de communication sécurisé, sans récupérer de données dans la puce, ce qui ne prend qu'un temps très court, fluidifiant encore le passage des utilisateurs au dispositif de contrôle 30. L'utilisateur n'a en outre pas besoin de laisser son support posé plusieurs secondes sur le lecteur 36, il peut le passer brièvement à proximité (moins de 1s), réduisant en outre les contacts et les risques de contamination des surfaces.

Le lecteur 36 ouvre le canal en utilisant ladite donnée de lecture optique récupérée comme mot de passe. Dans le cas où il a récupéré à l'issue de l'étape (b) plusieurs numéros, le lecteur tente d'ouvrir le canal en essayant les données de lecture optique récupérées les unes après les autres jusqu'à essayer celles qui correspondent au document d'identité de l'individu et qui autorise l'accès au contenu de la puce.

De manière connue, ledit canal sécurisé est ouvert conformément à un protocole choisi parmi Basic Access Control, BAC, et Password Authenticated Connection Establishment, PACE, en utilisant une clé dérivée de ladite donnée de lecture optique récupérée. En particulier, ladite clé est préférentiellement, conformément aux spécifications de l'OACI, pour une donnée de lecture optique MRZ, un haché de la concaténation du numéro du document d'identité, de la date de naissance de l'individu, et de la date d'expiration du document d'identité.

Dans le cas où le support est un terminal mobile, l'étape (c) peut en fait comprendre l'ouverture de deux canaux imbriqués : un premier canal « protocolaire » entre le module de communication sans contact du terminal et le lecteur 16 (par exemple un canal BLE), et dans ce canal on vient ouvrir le canal de communication sécurisé « applicatif » utilisant ladite donnée de lecture optique récupérée.

De manière particulièrement préférée, l'étape (c) comprend la mise en œuvre d'une authentification de ladite puce électronique via ledit canal de communication sécurisé, en particulier une authentification active (« active authentication ») ou une authentification matérielle (« chip authentication »), et on citera également PACE avec mappage d'authentification de puce (PACE-CAM), voir pour ces trois mécanismes la partie 11 de la spécification OACI/ICAO 9303 (chapitre 6).

En effet, l'ouverture du canal sécurisé permet de s'assurer que l'individu a bien en main un support de document d'identité avec une puce qui contient les données attendues, mais il pourrait être falsifié. On appelle en effet le « clonage » l'action frauduleuse consistant à dupliquer un document d'identité en fabriquant un faux support (et de manière générale en utilisant un support non autorisé) comprenant une puce électronique sur laquelle on vient copier les données lues depuis la puce originale.

Pour prévenir cela, les puces originales/autorisées stockent une paire d'une clé privée et d'une clé publique, la clé privée étant inaccessible en lecture et la clé publique étant accessible (par exemple référencée DG14 pour la chip authentication et référencée DG15 pour l'active authentication). A noter que cette clé publique peut être récupérée en utilisant le canal sécurisé (elle est bien plus légère que la donnée biométrique par exemple), voire avoir été directement récupérée lors de la création du DTC (étape d'enrôlement (a0)), ce qui est préféré pour éviter tout besoin de lecture de données sur la puce électronique. Ainsi, il est possible de copier la clé publique si l'on tente de cloner la puce, mais pas la clé privée.

La chip authentication est bien connue de l'homme du métier, et se base sur un protocole d'agrément de clés Diffie-Hellman et consiste en un échange de clés publiques avec la puce électronique (la puce électronique fournit sa clé publique dit statique, et le dispositif de contrôle 30 fournit une clé publique dite éphémère), puis la génération d'un secret commun (la puce électronique utilise sa clé privée correspondant à la clé publique statique et le dispositif de contrôle 30 utilise sa clé privée correspondant à la clé publique éphémère), et enfin le changement de la clé de chiffrement du canal sécurisé à partir de ce secret commun (la nouvelle clé de session est dérivée du secret commun). Si le dispositif de contrôle 30 « comprend » le document d'identité après ce changement de clé (i.e. chaque partie a bien obtenu la même clé de session), alors la puce électronique du document d'identité est correctement authentifiée.

Dans l'autre cas plus récent de l'active authentication, cette authentification est dite active car elle implique un mécanisme de challenge/response : ladite authentification active de ladite puce électronique comprend la vérification (par le dispositif de contrôle 30) en utilisant ladite clé publique d'une signature électronique reçue depuis la puce électronique en réponse à l'envoi d'un nonce (le challenge).

De manière plus détaillée, le dispositif de contrôle 30 génère un nonce, l'envoi via le canal à la puce sécurisée. Celle-ci calcule sa signature en utilisant sa clé privée : la puce hache le nonce (avec une fonction de hachage cryptographique), puis chiffre (entre autres) le haché en utilisant la clé privée, avec une fonction
5 cryptographique telle que RSA, et renvoie la signature en réponse au dispositif de contrôle 30 qui la déchiffre avec la clé publique et vérifie qu'on retrouve bien le haché du nonce.

A noter que la clé publique de l'un ou l'autre des mécanismes peut elle-même être signée avec une clé privée d'un organisme gouvernemental ou émetteur du
10 document d'identité pour s'assurer qu'on n'a pas mis un faux couple clé privée/clé publique sur la puce électronique.

On comprendra que de manière particulièrement préférée, aucune donnée autre que les données nécessaires à ladite authentification de la puce électronique n'est transmise via ledit canal de communication sécurisé, de sorte à conserver le
15 bénéfice d'une absence de récupération des données contenues sur la puce.

En fonction du résultat de l'étape (c) (et en particulier de l'authentification active ou matérielle), l'accès à la zone est autorisé ou refusé pour l'individu.

A noter que l'étape (c) peut comprendre une authentification biométrique
20 supplémentaire de l'individu. Cette étape comprend la comparaison de la donnée biométrique de référence correspondant à la puce du document formellement authentifié avec une nouvelle donnée biométrique candidate acquise sur le même trait. Cette autre donnée peut être une deuxième donnée biométrique acquise par le dispositif de contrôle 30 (ou bien un autre dispositif de contrôle) exclusivement aux
25 fins de l'authentification. Ceci est notamment le cas si le trait biométrique correspond à une autre donnée biométrique de référence que la donnée biométrique de référence correspondant à la première donnée candidate, ou bien si l'on a plusieurs dispositifs de contrôle, par exemple dans un aéroport un premier dispositif au franchissement de frontière et un deuxième à l'embarquement.

30

Ainsi le procédé proposé supprime complètement toute lecture de la zone de lecture automatique dans le processus récurrent de contrôle (l'utilisateur peut aller de l'entrée à l'aéroport de départ jusqu'à la sortie de l'aéroport d'arrivée sans jamais devoir présenter la zone de lecture automatique) et simplifie encore la manipulation

du support du document d'identité puisque la communication sans contact peut être bien plus brève, tout en s'assurant de la présence du document d'identité lors dudit contrôle et en permettant le contrôle de l'individu à l'aide des données dudit documents d'identité.

REVENDEICATIONS

1. Procédé de contrôle d'un individu disposant d'un document d'identité sur un support comprenant une puce électronique dans laquelle est stockée une donnée biométrique de référence de l'individu et apte à afficher une zone de lecture automatique représentant une donnée de lecture optique du document d'identité, le
5 procédé comprenant la mise en œuvre par un dispositif de contrôle (30) d'étapes de :
 - (a) acquisition d'une donnée biométrique candidate sur un trait biométrique de l'individu ;
 - 10 (b) à partir de la donnée biométrique candidate, récupération, dans une mémoire (20), d'une donnée de lecture optique associée à la donnée biométrique de référence correspondant au trait biométrique de l'individu ;
 - (c) ouverture d'un canal de communication sécurisé avec la puce
15 électronique du support du document d'identité de l'individu en utilisant ladite donnée de lecture optique récupérée.
2. Procédé selon la revendication 1, dans lequel l'étape (c) ne comprend ni la récupération de la donnée biométrique de référence de l'individu depuis ladite puce
20 électronique via ledit canal de communication sécurisé ni la lecture de ladite zone de lecture automatique du support du document d'identité.
3. Procédé selon l'une des revendications 1 et 2, dans lequel l'étape (c) comprend la mise en œuvre d'une authentification de ladite puce électronique via ledit canal de
25 communication sécurisé.
4. Procédé selon la revendication 3, dans lequel ladite puce électronique stocke une paire d'une clé privée et d'une clé publique, ladite authentification de ladite puce électronique étant choisie parmi une authentification active et une authentification
30 matérielle.
5. Procédé selon la revendication 4, dans laquelle ladite authentification de ladite puce électronique est une authentification active comprenant la vérification en

utilisant ladite clé publique d'une signature électronique reçue depuis la puce électronique en réponse à l'envoi d'un nonce.

6. Procédé selon l'une des revendications 3 à 5, dans lequel aucune donnée autre
5 que les données nécessaires à ladite authentification de la puce électronique n'est transmise via ledit canal de communication sécurisé.

7. Procédé selon l'une des revendication 1 à 6, dans lequel ledit canal sécurisé est
ouvert conformément à un protocole choisi parmi Basic Access Control, BAC, et
10 Password Authenticated Connection Establishment, PACE, en utilisant une clé dérivée de ladite donnée de lecture optique récupérée.

8. Procédé selon l'une des revendications 1 à 7, dans lequel l'étape (b) comprend :
- une comparaison des données biométriques de référence stockées dans la
15 mémoire avec la donnée biométrique candidate, et
- la sélection d'au moins une donnée de lecture optique de document d'identité correspondant à au moins une donnée biométrique de référence présentant un taux de similarité avec la donnée biométrique candidate supérieure à un seuil prédéterminé.

20 9. Procédé selon la revendication 8, dans lequel, si plus d'une donnée de lecture optique de document d'identité a été sélectionnée, l'étape (c) est tentée pour chaque donnée de lecture optique sélectionnée jusqu'à l'ouverture du canal de communication sécurisée.

25 10. Procédé selon l'une des revendications 1 à 9, dans lequel le dispositif de contrôle (30) comprend des moyens de communication sans contact, l'étape (c) étant mise en œuvre en approchant ledit support du dispositif de contrôle (30) dans une orientation quelconque.

30 11. Procédé selon la revendication 1 à 10, comprenant une étape (a0) préalable mise en œuvre par un dispositif d'enrôlement (10), de récupération de la donnée biométrique de référence de l'individu depuis ladite puce électronique ; d'acquisition de la donnée de lecture optique du document d'identité par lecture de la zone de

lecture automatique ; et d'enregistrement, dans ladite mémoire (20) distante, de la donnée de lecture optique du document d'identité en lien avec la donnée biométrique de référence de l'individu.

5 12. Procédé selon la revendication 11, dans lequel le document d'identité est un passeport, et :

- 10 - lors de l'étape (a0), le passeport est présenté ouvert à la page de la zone de lecture automatique auprès dispositif du d'enrôlement (10) pour la mise en œuvre de l'acquisition de la donnée de lecture optique du document d'identité, et
- lors de l'étape (c), le passeport est présenté fermé auprès du dispositif de contrôle (30).

15 13. Dispositif de contrôle (30) d'un individu disposant d'un document d'identité sur un support comprenant une puce électronique dans laquelle est stockée une donnée biométrique de référence de l'individu et apte à afficher une zone de lecture automatique représentant une donnée de lecture optique du document d'identité, configuré pour la mise en œuvre d'étapes de :

- 20 (a) acquisition d'une donnée biométrique candidate sur un trait biométrique de l'individu ;
- (b) à partir de la donnée biométrique candidate, récupération, dans une mémoire (20), d'une donnée de lecture optique associée à une donnée biométrique de référence correspondant au trait biométrique de l'individu ;
- 25 (c) ouverture d'un canal de communication sécurisé avec la puce électronique du support du document d'identité de l'individu en utilisant ladite donnée de lecture optique récupérée.

14. Système (1) de contrôle d'individus, comprenant :

- 30 - une mémoire (20),
- un dispositif de contrôle (30) selon la revendication 13, et
- un dispositif d'enrôlement (10), configuré pour la mise en œuvre d'étapes de récupération de la donnée biométrique de référence de l'individu depuis ladite puce électronique ; d'acquisition de la donnée de lecture optique du document

d'identité par lecture de la zone de lecture automatique ; et d'enregistrement, dans ladite mémoire (20) distante, de la donnée de lecture optique du document d'identité en lien avec la donnée biométrique de référence de l'individu.

5

15. Produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon l'une des revendications 1 à 12 de contrôle d'un individu, lorsque ledit procédé est exécuté sur un ordinateur.

10 16. Moyen de stockage lisible par un équipement informatique sur lequel un produit programme d'ordinateur comprend des instructions de code pour l'exécution d'un procédé selon l'une des revendications 1 à 12 de contrôle d'un individu.