



Gouvernement  
du Canada

Government  
of Canada

Ombudsman  
des vétérans

Veterans  
Ombudsman

Rapport de l'ombudsman des vétérans

Octobre 2012

**Honorer les vétérans du Canada et favoriser  
l'établissement de liens avec eux :  
une carte d'identité nationale des vétérans**

Canada

**BUREAU DE L'OMBUDSMAN DES VÉTÉRANS**

360, rue Albert, bureau 1560

Ottawa (Ontario) K1R 7X7

Appels faits au Canada (numéro sans frais) : 1-877-330-4343

Appels à frais virés de l'étranger : 1-902-626-2919

Courriel : [info@ombudsman-veterans.gc.ca](mailto:info@ombudsman-veterans.gc.ca)

Cette publication est également disponible en format électronique à  
[www.ombudsman-veterans.gc.ca](http://www.ombudsman-veterans.gc.ca)

V104-3/2012F-PDF  
978-1-100-99813-8



Le 5 octobre 2012

L'honorable Steven Blaney, C.P., député  
Ministre des Anciens Combattants  
Chambre des communes  
Ottawa (Ontario)  
K1A 0A6

Monsieur le Ministre,

J'ai le plaisir de vous présenter le rapport intitulé *Honorer les vétérans du Canada et favoriser l'établissement de liens avec eux : une carte d'identité nationale des vétérans*.

Je pense de longue date qu'une carte d'identité serait un grand avantage pour les vétérans et pour Anciens Combattants Canada. Le rapport traite de questions telles que l'objet, les caractéristiques et les fonctionnalités de la carte, en plus de présenter des renseignements sur les coûts théoriques et le calendrier de délivrance à prévoir.

En outre, je suis de l'avis que le moment est venu de reconnaître officiellement les anciens membres de la Gendarmerie royale du Canada comme vétérans. Depuis fort longtemps, les membres de la GRC protègent, aux côtés de leurs homologues militaires, la population canadienne, tant au pays qu'à l'étranger, souvent dans des situations dangereuses. Pourtant, le gouvernement du Canada ne les a jamais reconnus officiellement en tant que vétérans.

J'espère pouvoir discuter de ces recommandations dès que cela vous conviendra.

Veillez agréer, Monsieur le Ministre, l'expression de mes sentiments les meilleurs.

L'ombudsman des vétérans,

Guy Parent



---

# TABLE DES MATIÈRES

---

4	<b>Mandat de l'ombudsman des vétérans</b>
5	<b>Sommaire du rapport</b>
6	<b>Le problème</b>
8	<b>Contexte</b>
8	Les vétérans du Canada
9	Taille de la population de vétérans
10	Cartes émises aux vétérans et aux membres actifs
12	<b>Discussion</b>
18	<b>Points saillants du rapport : <i>Cartes d'identité et Anciens Combattants Canada</i></b>
19	<b>Conclusion et recommandations</b>
21	<b>Annexe - <i>Cartes d'identité et Anciens Combattants Canada</i>, rapport préparé par la société E-CARD ID Products Ltd.</b>

---

# MANDAT DE L'OMBUDSMAN DES VÉTÉRANS

---

Le Bureau de l'ombudsman des vétérans, créé par décret<sup>1</sup>, veille à ce que les vétérans, les membres actifs des Forces canadiennes et de la Gendarmerie royale du Canada et les autres clients d'Anciens Combattants Canada soient traités avec respect, conformément à la *Déclaration des droits des anciens combattants*, et à ce qu'ils reçoivent les services et les avantages dont ils ont besoin de manière équitable, rapide et efficace.

Le Bureau traite les plaintes, les questions d'ordre systémique et les nouveaux enjeux relatifs aux programmes et aux services fournis ou administrés par Anciens Combattants Canada, en plus d'examiner les questions d'ordre systémique liées au Tribunal des anciens combattants (révision et appel).

L'ombudsman des vétérans est un agent indépendant et impartial qui veille à ce que les vétérans et les autres clients d'Anciens Combattants Canada soient traités de manière équitable. L'ombudsman évalue l'équité en termes de *pertinence* (Les programmes et les services répondent-ils aux besoins?), de *caractère suffisant* (Les bons programmes et les bons services sont-ils dotés de ressources suffisantes?) et d'*accessibilité* (Les critères d'admissibilité créent-ils des obstacles injustes et peut-on avoir accès rapidement et facilement aux avantages et aux services d'Anciens Combattants Canada?).

## DÉCLARATION DES DROITS DES ANCIENS COMBATTANTS

En vertu de la *Déclaration des droits des anciens combattants*, les vétérans et tous les autres clients d'Anciens Combattants Canada ont le droit :

- d'être traités avec respect, dignité, équité et courtoisie;
- de prendre part aux discussions les concernant;
- d'être accompagnés lors de leurs rencontres avec Anciens Combattants;
- d'obtenir de l'information claire sur les services, en français ou en anglais, conformément à la *Loi sur les langues officielles*;
- de savoir que leur vie privée sera protégée conformément à la *Loi sur la protection des renseignements personnels*;
- de recevoir des avantages et des services conformément aux normes de service et d'être informés de leurs droits d'appel.

S'ils croient que l'un ou l'autre de leurs droits n'a pas été respecté, ils ont le droit de déposer une plainte et d'être assurés qu'elle soit prise en considération.

---

<sup>1</sup> Décret du conseil C.P. 207-530 du 3 avril 2007.

---

## SOMMAIRE DU RAPPORT

---

Anciens Combattants Canada a la responsabilité globale des quelque 750 000 vétérans du Canada. Il doit notamment fournir des avantages pour soins de santé et des avantages financiers aux vétérans malades et blessés et leur assurer une aide à la transition vers la vie civile. Or, l'ombudsman des vétérans a des préoccupations de longue date concernant la capacité du Ministère d'établir et de maintenir des contacts avec le groupe élargi de vétérans, à part ceux qui figurent déjà parmi sa clientèle.

L'ombudsman des vétérans propose la délivrance d'une *carte d'identité nationale des vétérans* qui pourrait aider le Ministère à entrer en contact avec les vétérans et à communiquer de manière proactive avec eux. En exigeant le renouvellement périodique de la carte, Anciens Combattants Canada pourrait maintenir des liens avec les vétérans et les informer des changements aux programmes et aux services, d'autant plus que cela lui permettrait d'évaluer leurs nouveaux besoins de services et de planifier l'affectation future des ressources.

La *carte d'identité nationale des vétérans* répondrait aux exigences d'un document d'identification officiel délivré par l'État. En faisant appel à une technologie moderne<sup>2</sup>, il serait également possible de personnaliser la carte pour qu'elle précise les avantages auxquels le titulaire a droit, par exemple ceux offerts par le Ministère et par d'autres organismes et programmes, dont le Programme de reconnaissance des Forces canadiennes.

Selon l'ombudsman des vétérans, un avantage tout aussi important de la carte est qu'elle faciliterait la transition de l'appartenance aux Forces canadiennes ou à la Gendarmerie royale du Canada (GRC) à l'appartenance à la communauté des vétérans. En effet, la délivrance de la carte aux membres actifs des Forces canadiennes et de la GRC au moment de leur libération complèterait leur transition vers la vie civile de manière officielle et significative en leur fournissant un symbole concret de leur appartenance à un groupe et en les reconnaissant en tant que vétérans.

---

<sup>2</sup> Un expert-conseil, E-CARD ID Products Ltd., a été chargé de produire un rapport sur les systèmes de reconnaissance de l'identité ainsi que sur les aspects techniques et les usages possibles d'une carte d'identité pour les vétérans du Canada. L'analyse des méthodes de délivrance d'une telle carte d'identité et des coûts correspondants est exposée en détail dans le rapport de l'expert-conseil intitulé *Cartes d'identité et Anciens Combattants Canada* (voir l'annexe).

L'ombudsman des vétérans croit fermement en la nécessité d'avoir une *carte d'identité nationale des vétérans* :

*Il n'existe aucune carte officielle, délivrée par le gouvernement du Canada, qui identifie clairement les anciens membres admissibles en tant que vétérans, que ce soit pour des fins de commémoration ou des fins de prestation d'avantages et de services. Je crois qu'une carte d'identité nationale des vétérans comblerait cette lacune, tout en fournissant à nos vétérans un moyen concret nationalement reconnu de s'identifier comme vétérans. Ce serait une autre façon pour le gouvernement du Canada de les remercier pour leur service et de reconnaître non seulement qui ils étaient, mais aussi qui ils sont : **des vétérans!***

De plus, l'ombudsman des vétérans propose que la définition actuelle de *vétéran* utilisée à des fins de commémoration<sup>3</sup> soit modifiée de sorte à y inclure les anciens membres de la Gendarmerie royale du Canada. Depuis fort longtemps, les membres de la GRC protègent, aux côtés de leurs homologues militaires, la population canadienne, tant au pays qu'à l'étranger, souvent dans des situations dangereuses. Pourtant, le gouvernement du Canada ne les a jamais reconnus officiellement en tant que vétérans.

## RECOMMANDATIONS DE L'OMBUDSMAN DES VÉTÉRANS

**RECOMMANDATION 1** – Que le ministre des Anciens Combattants, en collaboration avec le ministre de la Défense nationale et le ministre de la Sécurité publique, modifie la définition actuelle de *vétéran* à des fins de commémoration afin qu'elle englobe les anciens membres de la Gendarmerie royale du Canada.

**RECOMMANDATION 2** – Qu'Anciens Combattants Canada diffuse à grande échelle et mette en évidence sur son site Web et dans les publications appropriées, la définition de *vétéran* à des fins de commémoration.

**RECOMMANDATION 3** – Que le ministre des Anciens Combattants, en collaboration avec le ministre de la Défense nationale et le ministre de la Sécurité publique, entreprenne en priorité les démarches nécessaires à la création d'une *carte d'identité nationale des vétérans* répondant aux normes qui régissent les documents d'identification délivrés par l'État.

**RECOMMANDATION 4** – Qu'Anciens Combattants Canada, en collaboration avec les Forces canadiennes et la Gendarmerie royale du Canada, élabore une stratégie pour la délivrance d'une *carte d'identité nationale des vétérans* aux membres en voie de libération et aux vétérans actuels.

---

<sup>3</sup> La définition actuelle du terme *vétéran* utilisée à des fins de commémoration inclut tous les anciens membres des Forces canadiennes qui ont suivi leur instruction de base et qui ont été libérés honorablement, y compris ceux qui ont servi dans la Force de réserve, dans une zone de service spécial et au Canada.

---

## LE PROBLÈME

---

En vertu de sa loi constitutive, Anciens Combattants Canada a la responsabilité globale des quelque 750 000 vétérans du Canada. Il doit fournir des avantages pour soins de santé et des avantages financiers aux vétérans malades et blessés et assurer une aide à la transition vers la vie civile. À l'heure actuelle, cependant, aucun des vétérans du pays n'a de moyens concrets et reconnus de s'identifier comme vétéran, de faire reconnaître ses états de service et d'attester son admissibilité aux avantages découlant de son statut. Par conséquent, il arrive que ces vétérans et leurs proches aient du mal à prouver leur admissibilité à ces avantages et à ces services, voire à se faire reconnaître officiellement comme vétérans par le pays qui a bénéficié de leur service. Comme l'a expliqué le sénateur Roméo A. Dallaire :

*... lorsque vous êtes libéré des forces et que vous remettez votre carte d'identité et votre uniforme, votre esprit n'est pas libéré des forces pour autant. [...] Vous avez besoin d'un pont pour passer de l'autre côté [...], pour continuer à ressentir cette loyauté, surtout si vous êtes un vétéran<sup>4</sup>.*

De manière encore plus succincte, Bruce Ferguson, président national de l'Association canadienne des anciens combattants de la marine marchande, a souligné la nécessité d'« [...] améliorer le système d'identification afin que les marins marchands, lorsqu'ils demandent de l'aide, ne soient pas rejetés au motif qu'ils ne sont pas des anciens combattants ». Il a précisé sa pensée en exigeant une «... pièce d'identité officielle qui montre clairement, avec photo à l'appui, que nous sommes des anciens combattants »<sup>5</sup>.

Alors qu'Anciens Combattants Canada est généralement très actif auprès des vétérans qui sont ses clients actuels, il a du mal à identifier, à établir et à maintenir des liens avec le groupe élargi de vétérans et leurs familles, qui représentent ses « clients éventuels ». Ainsi, le Ministère peut difficilement prévoir les tendances et l'évolution des besoins de cette clientèle éventuelle, l'informer des changements prévus aux régimes d'avantages, aux programmes et aux critères d'admissibilité et répartir les ressources nécessaires à la prestation de ses services.

---

<sup>4</sup> Comité permanent des anciens combattants de la Chambre des communes, témoignage n° 029, 3<sup>e</sup> session, 40<sup>e</sup> législature, page 5,

<http://www.parl.gc.ca/content/hoc/Committee/403/ACVA/Evidence/EV4795104/ACVAEV29-F.PDF> .

<sup>5</sup> Comité sénatorial permanent de la sécurité nationale et de la défense, Délibérations du Sous-comité des anciens combattants, fascicule 4, 2<sup>e</sup> session, 39<sup>e</sup> législature, page 21,

<http://www.parl.gc.ca/Content/SEN/Committee/392/vete/pdf/04issue.pdf>.

L'ombudsman des vétérans a signalé ses préoccupations quant à ces problèmes à maintes reprises et a encouragé le ministère à améliorer ses activités de communication et de sensibilisation dans le cadre de son programme de transformation. Il est d'avis qu'une campagne proactive et soutenue de sensibilisation accroîtrait la demande d'accès aux programmes du Ministère et se solderait en une clientèle plus importante que prévu.<sup>6</sup>

Dans son rapport intitulé *De meilleurs services pour une meilleure qualité de vie des vétérans et de leur famille*, le Comité permanent des anciens combattants de la Chambre des communes s'est également penché sur la question :

*Une fois qu'ils ont quitté les FC [Forces canadiennes] ou la GRC [Gendarmerie royale du Canada], les vétérans ne peuvent être ni identifiés, ni localisés, à moins d'entreprendre eux-mêmes une démarche volontaire pour demander des services auprès d'ACC [Anciens Combattants Canada]. Cela limite la capacité d'ACC à joindre les vétérans qui pourraient éventuellement avoir besoin de certains services, par exemple dans les cas où des problèmes de santé mentale apparaîtraient plusieurs mois, ou même des années, après que l'individu ait quitté les FC ou la GRC<sup>7</sup>.*

Le besoin d'Anciens Combattants Canada d'établir et de maintenir des contacts avec tous les vétérans canadiens par l'intermédiaire d'un programme de sensibilisation réussi est devenu un sujet de préoccupation récurrent pour les parlementaires<sup>8</sup>.

En réponse à ces préoccupations, l'ombudsman des vétérans a réclamé, lors de son témoignage devant le Comité permanent des anciens combattants de la Chambre des communes, la délivrance d'une carte d'identité à tous les vétérans, qui reconnaîtrait clairement leur statut et qui « permettrait de mettre en place un système de suivi servant à rejoindre tous les vétérans, y compris les réservistes »<sup>9</sup>.

À cette fin, le Bureau de l'ombudsman des vétérans a chargé la société E-CARD ID Products Ltd. de produire un rapport sur la technologie des cartes, les systèmes d'émission de cartes d'identité et les utilisations possibles d'une carte d'identité pour les vétérans du Canada (voir l'annexe).

---

<sup>6</sup> Bureau de l'ombudsman des vétérans, *Rapport annuel 2010-2011, Un seul groupe de vétérans : une question d'équité*.

<sup>7</sup> Rapport du Comité permanent des anciens combattants de la Chambre des communes, *De meilleurs services pour une meilleure qualité de vie des vétérans et de leur famille*, 1<sup>e</sup> session, 41<sup>e</sup> législature, mai 2012, page 60, <http://www.parl.gc.ca/content/hoc/Committee/411/ACVA/Reports/RP5506979/acvarp05/acvarp05-f.pdf>.

<sup>8</sup> Comité permanent des anciens combattants de la Chambre des communes, témoignage n<sup>o</sup> 029, 3<sup>e</sup> session, 40<sup>e</sup> législature, page 10, <http://www.parl.gc.ca/content/hoc/Committee/403/ACVA/Evidence/EV4795104/ACVAEV29-F.PDF>.

<sup>9</sup> Rapport du Comité permanent des anciens combattants de la Chambre des communes, *De meilleurs services pour une meilleure qualité de vie des vétérans et de leur famille*, 1<sup>e</sup> session, 41<sup>e</sup> législature, mai 2012, page 32, <http://www.parl.gc.ca/content/hoc/Committee/411/ACVA/Reports/RP5506979/acvarp05/acvarp05-f.pdf>.

## LES VÉTÉRANS DU CANADA

Avant d'envisager la délivrance de cartes d'identité aux vétérans du Canada, il faut de toute évidence s'entendre d'abord sur la définition du terme *vétéran* à des fins de commémoration, étant donné qu'il n'existe aucune définition totalement inclusive du terme<sup>10</sup>.

En 2001, le ministre des Anciens Combattants de l'époque annonçait que tous les anciens membres des Forces canadiennes, y compris ceux qui avaient servi dans la Réserve, dans une zone de service spécial ou au Canada, seraient dorénavant reconnus comme des vétérans, à condition d'avoir satisfait aux exigences en matière d'instruction liées à leur classification professionnelle et d'avoir été libérés honorablement. La définition a été adoptée parce qu'elle tenait compte du « [...] risque potentiel auquel sont exposés tous les militaires des Forces canadiennes lorsqu'ils prêtent le serment d'allégeance et endossent l'uniforme canadien »<sup>11</sup>. Cette définition a été révisée en 2008. L'exigence relative à l'instruction professionnelle a été remplacée par celle de la simple instruction de base, et, à ce jour, cette définition constitue la définition officielle du terme *vétéran* utilisée par le gouvernement du Canada à des fins de commémoration<sup>12</sup>.

Dans la définition actuelle de *vétéran*, on perd un peu le contexte historique du terme, mais il est généralement reconnu que ceux qui ont participé à l'une ou l'autre des guerres mondiales et ceux qui ont pris part à la guerre de Corée sont des vétérans, y compris les membres de la marine marchande qui ont été reconnus officiellement comme des vétérans par le gouvernement du Canada en 1992.

---

<sup>10</sup> Quoique cela déborde du cadre du présent rapport, il importe de signaler que, pendant de nombreuses années, des conflits de la Première Guerre mondiale jusqu'aux conflits d'aujourd'hui, l'admissibilité aux programmes et aux avantages a souvent été décrite dans les lois ou les règlements applicables en fonction de la définition de *vétéran*. Le résultat? Il existe de nombreuses définitions du terme *vétéran* aux fins d'admissibilité aux avantages. L'établissement d'un lien entre l'admissibilité à des avantages et la catégorie de service est une question qui préoccupe l'ombudsman des vétérans, qui, conformément au thème d'un seul groupe de vétérans, demande que l'admissibilité aux nouveaux programmes et services soit définie en fonction des besoins plutôt que des catégories de service.

<sup>11</sup> Notes d'une allocution prononcée par le ministre des Anciens Combattants, l'honorable Ronald J. Duhamel, devant le Comité permanent de la défense nationale et des anciens combattants, le 29 mars 2001, <http://www.veterans.gc.ca/fra/ministere/presse/allocution/149>.

<sup>12</sup> La définition a été révisée après qu'on se soit rendu compte, pour deux raisons, que le fait d'avoir suivi une instruction professionnelle n'était pas le critère qui correspondait le mieux au nombre d'années de service requis pour avoir le droit de s'appeler *vétéran*. D'une part, la durée très variable des périodes d'instruction professionnelle créait des inégalités entre les professions. D'autre part, les membres des Forces canadiennes qui ont terminé leur instruction de base et qui attendent de suivre leur instruction professionnelle pourraient être mis dans des situations dangereuses lorsqu'ils sont affectés, au Canada, à des opérations de service spécial. Pour ces raisons, le fait d'avoir suivi une instruction de base était vu comme étant une exigence plus appropriée.

Le fait que la définition de *vétéran* adoptée par le gouvernement du Canada pour des fins de commémoration n'inclut pas les anciens membres de la Gendarmerie royale du Canada préoccupe l'ombudsman des vétérans.

Les activités militaires de la GRC remontent à la Rébellion du Nord-Ouest, à la guerre des Boers et aux guerres mondiales. Peu de gens savent que la GRC avait été envoyée en Sibérie en tant que force militaire en 1918-1919. La GRC a reçu officiellement des honneurs de guerre, qui ne sont attribués qu'à des unités militaires. Les membres de la GRC qui ont participé à la Seconde Guerre mondiale étaient admissibles à la Médaille canadienne du volontaire ainsi qu'à des avantages en tant que vétérans de ce conflit. Aujourd'hui, la GRC continue de servir aux côtés du personnel des Forces canadiennes dans presque tous les conflits où le Canada s'engage à donner du soutien, en participant, par exemple, à des opérations de maintien de la paix et à des patrouilles à risque élevé en Afghanistan. Les membres de la GRC sont admissibles à la Médaille canadienne du maintien de la paix<sup>13</sup>.

L'ombudsman des vétérans estime que le moment est venu de reconnaître officiellement les anciens membres de la GRC comme des vétérans.

**RECOMMANDATION 1** – Que le ministre des Anciens Combattants, en collaboration avec le ministre de la Défense nationale et le ministre de la Sécurité publique, modifie la définition actuelle de *vétéran* à des fins de commémoration afin qu'elle englobe les anciens membres de la Gendarmerie royale du Canada.

**RECOMMANDATION 2** – Qu'Anciens Combattants Canada diffuse à grande échelle et mette en évidence sur son site Web et dans les publications appropriées, la définition de *vétéran* à des fins de commémoration.

---

<sup>13</sup> En 1904, à la suite de la seconde guerre des Boers, le roi Édouard VII rendit hommage à la GRC (alors appelée Police à cheval du Nord-Ouest ou P.C.N.-O.) et à ses prouesses en lui confiant le titre de « royale ». Elle prit alors la désignation de Royale gendarmerie à cheval du Nord-Ouest (R.G.C.N.-O.). En 1920, la R.G.C.N.-O. changea son nom à la GRC. En 1921, par suite des exploits de la GRC lors de la Première Guerre mondiale (elle s'appelait la R.G.C.N.-O. à cette époque), le roi George V décerna à la Gendarmerie le statut officiel d'un régiment de dragons et, en 1935, le droit d'afficher ses honneurs de guerre sur un guidon (on accorde des drapeaux aux régiments d'infanterie tandis qu'on accorde des guidons aux régiments montés et aux régiments de dragons), ce qui distingue la GRC de toute autre force policière. Au fil des ans, la GRC a reçu les honneurs de guerre suivants : Nord-Ouest du Canada, 1885 (Rébellion); Afrique du Sud, 1900-1902; la Grande guerre (France et Flandres), 1918; Sibérie, 1918-1919 et la Seconde Guerre mondiale (Europe), 1939-1945 (en tant que 1er Corps de prévôté canadien). La GRC a reçu l'honneur, à deux reprises, de relever le Queen's Life Guard (cavalerie de la garde) à titre de régiment de dragons, la première fois en 1937, jusqu'au couronnement du roi George VI, et, plus récemment, en 2012, à l'occasion du jubilé de la Reine.

## TAILLE DE LA POPULATION DE VÉTÉRANS

Il est utile d'évaluer la taille de la population actuelle de vétérans à qui la carte d'identité serait émise et celle de la population de membres encore actifs des Forces canadiennes et de la Gendarmerie royale du Canada qui en seraient les futurs titulaires.

Il existe près de 750 000 vétérans de la GRC et des Forces canadiennes; 100 000 membres des Forces canadiennes (Force régulière et réservistes) et 23 000 membres de la GRC. Quelque 140 000 vétérans et membres actifs des Forces canadienne et de la GRC et plus de 78 000 survivants de vétérans décédés reçoivent des avantages et des services du ministère.

## CARTES ÉMISES AUX VÉTÉRANS ET MEMBRES ACTIFS

Avant de discuter de la question d'une *carte d'identité nationale des vétérans*, il importe de préciser qu'il n'existe aujourd'hui aucun document officiel (c.-à-d. délivré par l'État), tel qu'une carte, permettant d'identifier les anciens membres des Forces canadiennes et de la Gendarmerie royale du Canada comme vétérans. Certains vétérans n'ont aucun document attestant leur service (dans les forces armées, par exemple) alors que d'autres possèdent des documents (cartes) d'utilités variables. Par contre, aucun des ces documents ne renferme de mention confirmant que leur titulaire est un vétéran.

Il se peut que les vétérans de la Seconde Guerre mondiale et de la guerre de Corée aient en leur possession un document attestant leur libération honorable ou leur démobilisation à la suite de leur service, mais, pour autant qu'il soit possible d'en juger, aucun d'entre eux n'a reçu de carte d'identité de l'État qui leur accorde officiellement le statut de vétéran.

Voici une description des diverses cartes en circulation :

### **Certificat de service**

Au moment de leur libération, tous les membres des Forces canadiennes reçoivent un certificat de service, un document de grand format portant un sceau officiel qui atteste leurs états de service.

### **Registre de service (NDI 75)<sup>14</sup>**

Le registre de service (NDI 75) est une carte délivrée à la libération des membres de la Force régulière et des réservistes qui ont accumulé au moins 10 ans de service. La carte était autrefois délivrée exclusivement aux anciens membres de la Force régulière ayant accumulé au moins 25 ans de service.

La carte non-renouvelable porte le numéro matricule de l'ancien membre, la dernière photo d'identité utilisée par ce dernier ainsi que son nombre d'années de service et grade au moment de la libération. Il y manque la date de naissance et autres renseignements permettant l'identification (taille, poids, couleur des cheveux et des yeux, etc.). Elle porte un

---

<sup>14</sup> NDI est l'acronyme de *National Defence Identification*

numéro de série et un énoncé en caractères gras précisant qu'il ne s'agit *PAS* d'une carte d'identité. Il n'existe nulle part sur la carte une mention attestant que le titulaire est un vétéran.

La carte NDI 75 n'est rien de plus que ce que son titre indique : une attestation du service qui en précise la période et qui est utile pour prouver le statut antérieur de militaire.

### **Carte de membre retraité de la Gendarmerie royale du Canada**

Les anciens membres de la GRC reçoivent une carte non-renouvelable assortie d'une photo du titulaire. On y trouve également la date de naissance du titulaire et d'autres renseignements permettant de l'identifier (taille, poids, couleur des cheveux et des yeux), son grade et la date de son départ à la retraite, de même qu'un énoncé l'autorisant à porter son uniforme. La carte ne porte toutefois aucun numéro et n'indique pas que le titulaire est un vétéran.

### **Carte d'identité des soins de santé d'Anciens Combattants Canada**

Les clients d'Anciens Combattants Canada qui reçoivent des avantages médicaux du ministère reçoivent une carte d'identité des soins de santé qui porte le nom du titulaire et le numéro de client, de même qu'un code indiquant les avantages et les soins médicaux auxquels le titulaire a droit. Elle ne contient cependant ni photo ni renseignement d'identification. Abstraction faite du titre du Ministère, rien sur la carte n'indique que le titulaire est un vétéran.

### **Carte du Programme de reconnaissance des Forces canadiennes**

Les membres actifs et les anciens membres des Forces canadiennes, les employés civils actuels du ministère de la Défense nationale, les membres de la famille immédiate de ces groupes et d'autres personnes admissibles peuvent faire la demande d'une carte du Programme de reconnaissance des Forces canadiennes<sup>15</sup>.

Cette carte n'est pas renouvelable et ne contient ni renseignement d'identification ni photo. Chaque carte porte cependant un numéro distinct et précise le statut du titulaire, soit membre des Forces canadiennes, ancien membre, employé civil ou membre de la famille. Au verso se trouve une mention bien visible indiquant qu'il ne s'agit *PAS* d'une carte d'identité et que le document doit être utilisé avec une carte d'identité munie d'une photo valide. Il n'est précisé nulle part que le titulaire est un vétéran.

Les titulaires de cette carte s'en servent (avec une carte d'identité munie d'une photo) pour confirmer leur admissibilité aux avantages (rabais) offerts dans le cadre du Programme de reconnaissance des Forces canadiennes, une initiative financée grâce à des fonds non publics par les Services de soutien au personnel et aux familles des Forces canadiennes, qui relèvent du Chef du personnel militaire. Les renseignements recueillis sur le formulaire de demande et le numéro attribué sur la carte servent à faire un suivi des adhésions et à communiquer des détails aux participants sur les nouveaux avantages et les partenaires du Programme.

---

<sup>15</sup> Remarque : En l'occurrence, l'expression « autres personnes » englobe les employés et les anciens employés du Centre de la sécurité des télécommunications, les employés des fonds non publics, les employés des Centres de ressources pour les familles des militaires et les militaires étrangers participant à des échanges avec les Forces canadiennes.

En résumé, il n'existe pas de carte officielle délivrée par le gouvernement du Canada pour identifier clairement comme vétérans les anciens membres, que ce soit à des fins de commémoration ou de prestation de services et d'avantages.

---

## DISCUSSION

---

Pour s'acquitter de son mandat, Anciens Combattants Canada a le besoin clair d'établir et de maintenir des liens avec les vétérans du Canada. Les Forces canadiennes et la Gendarmerie royale du Canada n'ont aucune obligation de maintenir des contacts ou de communiquer avec leurs anciens membres. Les besoins de soins de santé découlant du service et l'aide à la transition vers la vie civile des anciens membres et de leurs proches relèvent du mandat d'Anciens Combattants Canada en vertu de lois du Parlement. Il en était de même pour les militaires qui ont servi pendant les deux guerres mondiales ou pendant la guerre de Corée, y compris les anciens membres de la marine marchande. Ils cessaient d'être la responsabilité de leur ancienne organisation dès leur libération et il revenait à Anciens Combattants Canada de répondre à leurs besoins.

De par leur nature même, les institutions militaires et policières sont des organisations très cohésives et paternalistes pour qui la bienveillance témoignée aux membres pendant leur service est à la mesure de la loyauté, du dévouement et de la prise de risques qui sont couramment exigés d'eux. L'identification claire des membres de ces organisations pendant leur service, par le port de l'uniforme et la possession d'une carte d'identité officielle, vise certes à assurer la sécurité et la bonne marche de la structure de commandement, mais il s'agit aussi d'un moyen essentiel de leur garantir une identité en tant que membres d'une équipe respectée – d'un moyen de ne pas être seul.

Mais, une fois que les membres remettent leur uniforme et leur carte d'identité au moment de la retraite ou la libération, cette garantie disparaît, ayant, bien souvent, des répercussions sur leur identité et leur sentiment de valorisation. Les membres doivent alors surmonter les défis de la réinsertion dans la société civile sans le bénéfice de liens d'appartenance, en souffrant parfois des effets de leurs années de service. Dans de telles circonstances, il leur faut, comme l'a si éloquemment exprimé le sénateur Roméo A. Dallaire, « ...un pont pour passer de l'autre côté [...], surtout si vous êtes un vétéran... »<sup>16</sup>. C'est là l'environnement opérationnel d'Anciens Combattants Canada, qui a pour mandat de voir « ...aux soins, au traitement ou à la réinsertion dans la vie civile... » d'anciens membres : les vétérans.

Il s'agit aussi de l'environnement opérationnel du Chef d'état-major de la Défense, à qui la *Loi sur la défense nationale* confère le mandat d'utiliser des biens non publics (y compris des fonds) « au profit de l'ensemble ou d'une partie des officiers et militaires du rang, anciens ou

---

<sup>16</sup> Comité permanent des anciens combattants de la Chambre des communes, témoignage n° 029, 3<sup>e</sup> session, 40<sup>e</sup> législature, page 5, <http://www.parl.gc.ca/content/hoc/Committee/403/ACVA/Evidence/EV4795104/ACVAEV29-F.PDF>.

en poste, ou des personnes à leur charge »<sup>17</sup>. Le Programme de reconnaissance des Forces canadiennes vise à établir et à entretenir des rapports avec les membres et les anciens membres (vétérans) des Forces canadiennes ainsi qu'avec leurs familles, afin de leur faire profiter d'un ensemble sans cesse changeant de rabais offerts par des entreprises et des organismes partenaires. Si les cartes délivrées jusqu'à présent dans le cadre du programme ne comprennent ni photo, ni renseignement d'identification, ni le mot *vétéran*, elles ont néanmoins fait naître un sentiment d'engagement et d'appartenance renouvelé chez certains titulaires qui avaient peut-être l'impression d'avoir été abandonnés au fil des ans. C'est loin d'être insignifiant.

Dans une certaine mesure, c'est cette fonction de commémoration et de reconnaissance que remplirait la *carte d'identité nationale des vétérans*, du fait qu'elle représenterait un élément concret et substantiel de ce « pont » que décrit le sénateur Roméo A. Dallaire, entre l'appartenance à un service en uniforme et l'appartenance à la communauté élargie des vétérans, reconnus et estimés (*appréciés*) par le pays pour ce qu'ils ont accompli au nom du Canada et de ses citoyens. Elle permettrait aussi au Ministère d'établir et de maintenir les contacts avec les vétérans qui ne sont pas ses clients, ce qui lui pose tant de difficultés, pour les informer et aux fins de planifications.

L'importance pour Anciens Combattants Canada d'établir et de maintenir des rapports avec *tous* les vétérans, clients et autres, a été soulignée à maintes reprises dans des témoignages présentés devant les comités du Sénat et de la Chambre des communes ainsi que dans un rapport du Comité permanent des anciens combattants de la Chambre des communes :

*[...] Les témoignages entendus par le Comité [...] font ressortir un même point : le Ministère [Anciens Combattants Canada] doit atteindre tous les anciens combattants qui ont besoin de services, et non seulement ceux qui sont déjà bénéficiaires de ses programmes*<sup>18</sup>.

Anciens Combattants Canada a reçu à peu près le même message de la part de vétérans qui participaient à des groupes de réflexion dans le cadre de l'*Évaluation de la nouvelle Charte des anciens combattants* de 2010. Ils ont établi un parallèle entre « la reconnaissance des anciens combattants » et « une entière proactivité [...], prendre de leurs nouvelles avant qu'ils ne s'adressent au Ministère [...], assurer un suivi auprès d'eux afin de vérifier comment ils vivent leur transition »<sup>19</sup>. Ce « suivi », que certains appellent aussi « surveillance », est considéré

---

<sup>17</sup> *Loi sur la défense nationale*, L.R.C. (1985), ch. N-5, paragraphe 39. (1);

<http://laws-lois.justice.gc.ca/fra/lois/N-5/page-15.html#docCont>.

<sup>18</sup> Rapport du Comité permanent des anciens combattants de la Chambre des communes : *Relever la barre plus haut – Les soins de santé pour les anciens combattants : Le Programme pour l'autonomie des anciens combattants et l'examen des soins de santé pour anciens combattants*, 2<sup>e</sup> session, 39<sup>e</sup> législature, mai 2008, page 11, <http://www.parl.gc.ca/content/hoc/Committee/392/ACVA/Reports/RP3517720/acvarp01/acvarp01-f.pdf>.

<sup>19</sup> Anciens Combattants Canada, Rapport : *Évaluation de la nouvelle Charte des anciens combattants – Phase II*, Annexe G, août 2010, page 68.

[http://www.veterans.gc.ca/pdf/deptReports/2010-08-nvce-p2\\_f.pdf](http://www.veterans.gc.ca/pdf/deptReports/2010-08-nvce-p2_f.pdf).

comme particulièrement important pour les vétérans, chez qui l'apparition des symptômes de traumatismes liés au stress opérationnel peut être différée<sup>20</sup>. En fait, les membres des groupes de réflexion ayant participé à l'*Évaluation de la nouvelle Charte des anciens combattants* se sont entendus sur le fait que «... certains anciens combattants sont susceptibles d'être déprimés ou d'être soumis à des stress et, par conséquent, d'être moins susceptibles de se charger de communiquer avec ACC (Anciens Combattants Canada) [...]. Le Ministère devrait prendre l'initiative et communiquer avec eux »<sup>21</sup>.

Les réservistes font face à des obstacles particuliers sur le plan du soutien et de l'accès aux soins après la libération. Bien souvent, ceux-ci retournent chez-eux dans des localités très éloignées de la base de l'unité à laquelle ils étaient affectés pendant leur déploiement. Ces personnes peuvent avoir un accès limité au réseau de soutien créé pour leurs homologues de la Force régulière<sup>22</sup>. En fait, le sénateur Roméo A. Dallaire décrit de la façon suivante la situation des réservistes :

*Quand un réserviste se retrouve dans différents villages du pays et décide d'abandonner l'armée, on se soucie très peu de savoir quels soins il reçoit. Voilà pourquoi il y a davantage de soldats devant les tribunaux. Vous verrez là de nombreux réservistes parce qu'on les a pratiquement laissés tomber*<sup>23</sup>.

Il prédit également que la diminution de l'envergure de la mission en Afghanistan se traduira par une augmentation du nombre de cas de traumatismes liés au stress opérationnel chez les vétérans et les familles qui sont parvenus jusqu'ici à supporter le stress de missions multiples<sup>24</sup>. Cette situation soulève une question importante : la capacité pour Anciens Combattants Canada de prévoir les services dont les vétérans auront besoin dans l'avenir, le nombre de vétérans qui en auront besoin et leur répartition géographique, afin de pouvoir répartir les ressources nécessaires. La question touche aux mandats et aux responsabilités d'Anciens Combattants Canada, des Forces canadiennes et du ministère de la Défense nationale lorsque les membres font la transition à la vie civile de vétéran<sup>25</sup>.

---

<sup>20</sup> Rapport du Comité permanent des anciens combattants de la Chambre des communes : *De meilleurs services pour une meilleure qualité de vie des vétérans et de leur famille*, 1<sup>e</sup> session, 41<sup>e</sup> législature, mai 2012, page 30, <http://www.parl.gc.ca/content/hoc/Committee/411/ACVA/Reports/RP5506979/acvarp05/acvarp05-f.pdf>.

<sup>21</sup> Anciens Combattants Canada, Rapport : *Évaluation de la nouvelle Charte des anciens combattants – Phase II*, Annexe G, août 2010, page 48, [http://www.veterans.gc.ca/pdf/deptReports/2010-08-nvce-p2\\_f.pdf](http://www.veterans.gc.ca/pdf/deptReports/2010-08-nvce-p2_f.pdf).

<sup>22</sup> Rapport du Comité permanent des anciens combattants de la Chambre des communes : *Relever la barre plus haut – Les soins de santé pour les anciens combattants : Le Programme pour l'autonomie des anciens combattants et l'examen des soins de santé pour anciens combattants*, 2<sup>e</sup> session, 39<sup>e</sup> législature, mai 2008, page 19, <http://www.parl.gc.ca/content/hoc/Committee/392/ACVA/Reports/RP3517720/acvarp01/acvarp01-f.pdf>.

<sup>23</sup> Comité permanent des anciens combattants de la Chambre des communes, témoignage n° 029, 3<sup>e</sup> session, 40<sup>e</sup> législature, page 3, <http://www.parl.gc.ca/content/hoc/Committee/403/ACVA/Evidence/EV4795104/ACVAEV29-F.PDF>.

<sup>24</sup> Id., *ibid.*, page 2.

<sup>25</sup> Rapport du Comité permanent des anciens combattants de la Chambre des communes : *Relever la barre plus haut – Les soins de santé pour les anciens combattants : Le Programme pour l'autonomie des anciens combattants*

À cet égard, il a été recommandé qu'Anciens Combattants Canada travaille de concert avec le ministère de la Défense nationale à normaliser les systèmes de dossiers des deux organisations et qu'il utilise le numéro matricule des militaires au lieu d'attribuer un numéro de client distinct, de manière à faciliter le transfert des dossiers au moment de la libération et à assurer une transition aussi harmonieuse que possible<sup>26</sup>. La même pratique pourrait être étendue aux vétérans de la Gendarmerie royale du Canada.

La délivrance d'une *carte d'identité nationale des vétérans* au moment de la libération serait un moyen concret et significatif pour les membres touchés d'assurer la transition. Elle confirmerait sans équivoque le statut de vétéran et donnerait accès rapidement aux coordonnées à employer pour obtenir de l'aide. La carte agirait à titre de preuve d'états de service, tout en répondant aux exigences d'un document d'identification délivré par l'État.

En faisant appel aux technologies décrites dans le rapport *Cartes d'identité et Anciens Combattants Canada*, il serait possible de « personnaliser » la carte pour tenir compte de l'admissibilité du titulaire à divers avantages et services fournis par Anciens Combattants Canada, ainsi qu'à des rabais et à d'autres offres de partenaires de l'industrie, comme dans le cadre du Programme de reconnaissance des Forces canadiennes. Cette fonctionnalité multiple éliminerait la nécessité pour les vétérans de détenir plus d'une carte pour attester de leur statut, ce qu'ils ont dit souhaiter ne pas avoir à faire<sup>27</sup>.

En exigeant le renouvellement de la carte et la mise à jour périodique de la photo, éventuellement par l'intermédiaire de points de service locaux, Anciens Combattants Canada pourrait avoir des contacts récurrents avec les vétérans, pour les informer des nouveaux programmes, évaluer leurs nouveaux besoins et planifier l'affectation future des ressources.

Les questions liées aux méthodes de délivrance et aux coûts correspondants sont abordées dans le rapport de l'expert-conseil intitulé *Cartes d'identité et Anciens Combattants Canada* (voir l'annexe). L'expert-conseil, la société E-CARD ID Products Ltd., prévoit que le coût de délivrance d'un million de cartes (chiffre théorique) à puce<sup>28</sup> par un système centralisé s'élèverait à 5,20 \$ la carte, ou à 5,2 millions de dollars, somme à laquelle s'ajoutent les coûts rattachés à l'inscription (c.-à-d. les demandeurs se rendraient à l'un des points de service disséminés d'un bout à l'autre du pays pour se faire photographier et se faire inscrire), soit 1,5 million de dollars. Ces chiffres sont très généreux et basés sur l'hypothèse d'une stratégie d'inscription audacieuse qui engloberait *tous* les vétérans actuels (quelque 750 000 vétérans, un chiffre bien moindre que le chiffre théorique d'un million utilisé) et qui se ferait au cours d'une seule année civile.

---

*et l'examen des soins de santé pour anciens combattants, 2<sup>e</sup> session, 39<sup>e</sup> législature, mai 2008, page 10, <http://www.parl.gc.ca/content/hoc/Committee/392/ACVA/Reports/RP3517720/acvarp01/acvarp01-f.pdf>.*

<sup>26</sup> *Id.*, *ibid.*, page 17.

<sup>27</sup> Rapport du Comité permanent des anciens combattants de la Chambre des communes : *De meilleurs services pour une meilleure qualité de vie des vétérans et de leur famille*, page 23, <http://www.parl.gc.ca/content/hoc/Committee/411/ACVA/Reports/RP5506979/acvarp05/acvarp05-f.pdf>.

<sup>28</sup> Remarque : Le recours à la carte à puce (qui coûterait 0,70 \$ de plus la pièce) prolonge la période de validité de la photo par rapport à la carte à bande magnétique, ce qui réduit la fréquence des renouvellements et les coûts globaux.

En fait, comme le révèle l'expérience acquise lors de la délivrance de la carte du Programme de reconnaissance des Forces canadiennes, le simple repérage des vétérans actuels, en particulier des anciens réservistes et du grand nombre d'anciens membres de la Force régulière qui ne reçoivent pas de prestations d'invalidité, représente une tâche difficile qui exige du temps, mesuré en *années*. Plusieurs moyens devront être utilisés pour joindre la population de vétérans actuels, notamment : envois postaux; annonce de la création du programme par l'intermédiaire de divers médias, tels que des revues et d'autres publications destinées aux organismes de vétérans; et aide directe de certains de ces organismes. La délivrance de la *carte d'identité nationale des vétérans* dès la libération éliminerait le besoin de les repérer plus tard et mettrait un terme à l'accroissement annuel du nombre de vétérans sans carte (il y a environ 6 000 libérations et départs à la retraite chaque année).

Les organismes de vétérans, qui sont disséminés d'un océan à l'autre, pourraient également faciliter l'inscription et en réduire les coûts en mettant à contribution leurs bénévoles et leurs installations locales. Ces possibilités, qui dépassent largement la portée du présent rapport, méritent néanmoins d'être prises en considération pendant l'élaboration du plan de mise en œuvre. Qu'il suffise pour l'instant de préciser que, une fois que le plus grand nombre possible de vétérans se seront vu offrir ou délivrer une carte, les coûts de délivrance chuteront probablement à moins de 300 000 \$ par année.

Ainsi, la *carte d'identité nationale des vétérans* pourrait remplacer les quatre cartes décrites précédemment : le registre de service (NDI 75) de la Défense nationale, la carte de membre retraité de la Gendarmerie royale du Canada, la carte d'identité des soins de santé d'Anciens Combattants Canada et la carte du Programme de reconnaissance des Forces canadiennes. Elle procurerait également une carte à d'autres vétérans, tels que les anciens membres de la marine marchande.

De par sa qualité et son utilité, cette carte viendrait renforcer la valeur que l'État accorde au *service*. En outre, elle répondrait aux besoins commémoratifs des vétérans, qui veulent être *identifiés et reconnus*, et elle permettrait l'établissement de liens entre les divers groupes, qui disposeraient d'un statut commun, celui de vétéran. Comme souligné dans le rapport *Cartes d'identité et Anciens Combattants Canada*, c'est « ce qu'offre réellement une carte d'identité – relier un groupe de personnes différentes à une appartenance commune »<sup>29</sup>.

**RECOMMANDATION 3** – Que le ministre des Anciens Combattants, en collaboration avec le ministre de la Défense nationale et le ministre de la Sécurité publique, entreprenne en priorité les démarches nécessaires à la création d'une *carte d'identité nationale des vétérans* répondant aux normes qui régissent les documents d'identification délivrés par l'État.

**RECOMMANDATION 4** – Qu'Anciens Combattants Canada, en collaboration avec les Forces canadiennes et la Gendarmerie royale du Canada, élabore une stratégie pour la délivrance d'une *carte d'identité nationale des vétérans* aux membres en voie de libération et aux vétérans actuels.

---

<sup>29</sup> Annexe : E-Card ID Products Ltd, *Cartes d'identité et Anciens Combattants Canada*, 2012, page 21.

---

# POINTS SAILLANTS DU RAPPORT : CARTES D'IDENTITÉ ET ANCIENS COMBATTANS CANADA

---

Le Bureau de l'ombudsman des vétérans a retenu les services de la société E-CARD ID Products Ltd. pour obtenir des renseignements sur la technologie des cartes, les systèmes d'émission de cartes d'identité et les utilités possibles d'une carte d'identité pour les vétérans du Canada. Voici les points saillants du rapport :

- Il est important de déterminer d'entrée de jeu les raisons d'être de la carte d'identité.
- Du point de vue de la sécurité et de la protection des renseignements personnels, il importe d'adhérer aux politiques et aux règlements fédéraux et provinciaux et de n'inclure sur la carte que les renseignements essentiels.
- Les documents d'identification doivent contenir plusieurs caractéristiques électroniques et physiques de sécurité; il est déconseillé de ne recourir qu'à une seule méthode d'authentification.
- Les moyens d'identification électroniques qui n'exigent aucune carte évoluent rapidement, mais ils reposent sur une infrastructure vaste et coûteuse. La carte d'identité traditionnelle, en revanche, même lorsqu'elle est pourvue d'une puce, est relativement peu dispendieuse.
- Les cartes à bande magnétique sont moins sécuritaires que les cartes à puce, qui peuvent intégrer des caractéristiques d'authentification pour prolonger la période de validité de la photo figurant sur la carte.
- La délivrance des cartes peut se faire depuis un endroit centralisé ou depuis des points de service disséminés un peu partout au pays. La délivrance répartie est plus rapide et évite les problèmes engendrés par le courrier ou les services de messagerie, mais elle est beaucoup plus coûteuse (37 % de plus) que la délivrance centralisée, qui offre une sécurité accrue.
- Le renouvellement des cartes peut se faire à un endroit centralisé ou par l'intermédiaire de points de service répartis à l'échelle du pays.

- Le rapport fourni quelques détails sur les coûts et les calendriers de délivrance potentiels à prévoir pour un million (chiffre théorique) de cartes intelligentes (c.-à-d. à puce) dans le cadre d'un programme centralisé, en supposant que les données sur les titulaires sont accessibles.
- Il est très difficile de faire l'analyse des coûts et avantages d'une carte d'identité. Bien souvent, il n'est pas possible d'attribuer une valeur financière à sa raison d'être véritable : relier un groupe de personnes différentes à une appartenance commune.

---

## CONCLUSION ET RECOMMANDATIONS

---

Anciens Combattants Canada a la responsabilité globale des près de 750 000 vétérans du Canada. Il doit notamment fournir des avantages financiers et des avantages pour soins de santé aux vétérans malades et blessés et leur assurer une aide à la transition vers la vie civile.

Bien que le Ministère soit généralement actif auprès des quelque 140 000 vétérans et membres en service qu'il sert, il a du mal à établir des contacts avec le groupe élargi de vétérans et de membres de leur famille qui ne sont pas ses clients, mais qui constituent sa clientèle éventuelle. Or, les parlementaires, l'ombudsman des vétérans et les vétérans eux-mêmes ont maintes fois insisté sur l'importance cruciale d'établir et de maintenir des contacts avec les vétérans pour assurer une intervention et des soins efficaces.

De plus, les vétérans du Canada ne disposent actuellement d'aucun moyen concret nationalement reconnu de s'identifier comme vétérans.

L'ombudsman des vétérans a proposé la délivrance d'une *carte d'identité nationale des vétérans* pour aider le Ministère à établir des liens avec les vétérans et qui servirait aussi à identifier les vétérans comme tels et à reconnaître officiellement leurs états de service.

La *carte d'identité nationale des vétérans* pourrait remplacer plusieurs cartes qui sont actuellement délivrées à d'anciens membres par les Forces canadiennes, la Gendarmerie royale du Canada et Anciens Combattants Canada, mais qui n'accordent pas à leur titulaire le statut de vétéran. La carte répondrait aux exigences d'un document d'identification délivré par l'État et ferait appel à une technologie moderne. Il serait possible de personnaliser la carte pour qu'elle précise les services et les avantages particuliers auxquels le titulaire a droit, par exemple ceux offerts par Anciens Combattants Canada et par le Programme de reconnaissance des Forces canadiennes.

La délivrance d'une *carte d'identité nationale des vétérans* à tous les vétérans nécessitera du temps et des efforts, puisqu'il n'y a aucune façon simple de communiquer avec bon nombre d'entre eux. La délivrance d'une carte aux membres actifs au moment de leur libération éliminerait le besoin de communiquer avec eux ultérieurement pour cette même fin, tout en mettant un terme à l'accroissement annuel du nombre de vétérans sans carte (il y a environ 6 000 libérations et départs à la retraite chaque année). Par ailleurs, la délivrance de la carte aux membres en voie de libération compléterait leur transition vers la vie civile de manière officielle et significative en leur fournissant un symbole concret de leur appartenance à un groupe reconnu en les reconnaissant en tant que vétérans.

Enfin, l'ombudsman des vétérans propose que la définition actuelle de *vétéran* utilisée à des fins de commémoration soit modifiée de sorte à y inclure les anciens membres de la Gendarmerie royale du Canada. Depuis fort longtemps, les membres de la GRC protègent, aux côtés de leurs homologues militaires, la population canadienne, tant au pays qu'à l'étranger, souvent dans des situations dangereuses. Pourtant, le gouvernement du Canada ne les a jamais reconnus officiellement en tant que vétérans.

L'ombudsman des vétérans fait les quatre recommandations suivantes :

**RECOMMANDATION 1** – Que le ministre des Anciens Combattants, en collaboration avec le ministre de la Défense nationale et le ministre de la Sécurité publique, modifie la définition actuelle de *vétéran* à des fins de commémoration afin qu'elle englobe les anciens membres de la Gendarmerie royale du Canada.

**RECOMMANDATION 2** – Qu'Anciens Combattants Canada diffuse à grande échelle et mette en évidence sur son site Web et dans les publications appropriées, la définition de *vétéran* à des fins de commémoration.

**RECOMMANDATION 3** – Que le ministre des Anciens Combattants, en collaboration avec le ministre de la Défense nationale et le ministre de la Sécurité publique, entreprenne en priorité les démarches nécessaires à la création d'une *carte d'identité nationale des vétérans* répondant aux normes qui régissent les documents d'identification délivrés par l'État.

**RECOMMANDATION 4** – Qu'Anciens Combattants Canada, en collaboration avec les Forces canadiennes et la Gendarmerie royale du Canada, élabore une stratégie pour la délivrance d'une *carte d'identité nationale des vétérans* aux membres en voie de libération et aux vétérans actuels.

# **CARTES D'IDENTITÉ ET ANCIENS COMBATTANTS CANADA**

---

*Rapport sur la technologie des cartes, les systèmes d'émission de cartes d'identité et les utilisations possibles des cartes d'identité par les vétérans du Canada.*

**KYLE FAIRFIELD, B.A., B.ED., CPP  
E-CARD ID PRODUCTS LTD.**

© 2012

**VERSION 1.10**

## Table des matières

<b>Qu'est-ce qu'une carte d'identité? .....</b>	<b>24</b>
<b>Types de cartes et applications possibles.....</b>	<b>25</b>
<b>Matériaux de composition des cartes .....</b>	<b>25</b>
Cartes de plastique standards .....	25
Cartes en composite .....	25
Polycarbonate .....	25
<b>Technologie des cartes .....</b>	<b>27</b>
Code à barres .....	27
Estampage en relief.....	27
Bande magnétique .....	27
Carte à puce .....	29
<b>Sécurité des cartes .....</b>	<b>31</b>
Dispositifs de sécurité physiques .....	31
Dispositifs de sécurité électroniques.....	35
<b>Diverses applications des cartes .....</b>	<b>36</b>
Identité .....	36
Finances .....	36
Sécurité physique.....	36
Protection des renseignements ou sécurité logique.....	36
Santé/médecine .....	37
Adhésion/fidélité.....	37
Chiffrement et échange de documents.....	37
Convergence .....	37
<b>Approche fondée sur les normes -- un aperçu de la PIV .....</b>	<b>38</b>
Historique .....	38
Incidences de la norme FIPS 201.....	39
Importance de la PIV .....	40
<b>Choisir la bonne technologie pour son organisme.....</b>	<b>43</b>
1. Comprendre son organisme .....	43
2. Déterminer les pertes et les risques.....	43
3. Déterminer les conséquences associées à une perte.....	43
4. Effectuer une analyse des coûts et des avantages .....	44
<b>Fonctions, sécurité et stockage des cartes à puce.....</b>	<b>45</b>
<b>Sécurité des cartes à puce – cryptographie, ICP et AC .....</b>	<b>45</b>
<b>L'avenir de la technologie des cartes et pratiques exemplaires .....</b>	<b>47</b>
<b>Pratiques exemplaires .....</b>	<b>47</b>
<b>L'avenir de la technologie des cartes .....</b>	<b>48</b>
<b>Émission des cartes.....</b>	<b>50</b>
<b>Émission répartie des cartes.....</b>	<b>50</b>
Avantages d'une émission répartie .....	51
Inconvénients d'une émission répartie.....	51
<b>Émission centralisée des cartes .....</b>	<b>52</b>
Inconvénients d'une émission centralisée.....	53
Avantages d'une émission centralisée .....	53
<b>Exigences relatives à l'émission des cartes .....</b>	<b>55</b>
<b>Matériel et logiciel .....</b>	<b>55</b>
<b>Personnel.....</b>	<b>56</b>

<b>Options de renouvellement de la carte .....</b>	<b>59</b>
<b>Aspects liés à la sécurité et à la protection des renseignements personnels .....</b>	<b>60</b>
<b>Incidences d'une falsification de la carte .....</b>	<b>60</b>
Carte d'identité ordinaire .....	60
Carte à puce .....	61
<b>Effet d'une intrusion dans le système .....</b>	<b>61</b>
<b>Établissement des coûts.....</b>	<b>62</b>
<b>Hypothèses liées au projet .....</b>	<b>62</b>
<b>Éléments livrables du projet .....</b>	<b>63</b>
<b>Calendrier de mise en œuvre du projet .....</b>	<b>64</b>

## Qu'est-ce qu'une carte d'identité?

Une carte est considérée comme étant une carte d'identité si elle permet d'établir correctement l'identité d'une personne au degré de certitude exigé dans le cadre de fonctionnement pour lequel elle est conçue. Ce cadre général est parfois appelé « l'écosystème » d'une carte.

Il n'existe aucune norme nationale canadienne publiée relative aux cartes d'identité. Chaque ministère fédéral, provincial et municipal possède généralement ses propres normes (p. ex. Transports Canada compte divers modèles de cartes pour les inspecteurs, les policiers à bord d'aéronefs, le personnel civil, les cartes d'identité de zones réglementées ACSTA, etc.) conçues pour répondre aux besoins de son écosystème. Certaines cartes ne servent qu'à une vérification visuelle (c.-à-d. qu'elles fonctionnent comme une carte éclair aux fins de vérification visuelle uniquement) alors que d'autres comportent des dispositifs électroniques intégrés aux fins d'authentification automatisée.

La principale question à se poser avant de choisir un type particulier de technologie de carte ou de méthode d'impression est « à quoi servira la carte »? À partir de cet énoncé de l'utilisation ou du but de la carte, on ne peut choisir le type de technologie approprié et le mettre en application.

Si la carte est utilisée uniquement aux fins de vérification visuelle, il est recommandé d'y intégrer les éléments variables suivants :

- Photographie
- Nom et prénom (s)
- Numéro de carte
- Autorité émettrice
- Date d'émission
- Date d'expiration

Si la carte sert aux fins d'authentification électronique, il n'y aura alors aucune restriction ni exigence relatives à l'impression de quoi que ce soit sur la carte. Certains organismes chargés de l'application de la loi possèdent des laissez-passer de sécurité qui sont souvent entièrement vierges, à l'exception d'une petite photographie de 3 cm<sup>2</sup> du détenteur de la carte. Advenant qu'une personne autre que le détenteur de la carte trouve un de ces laissez-passer, elle ne saura pas avec certitude à quel bâtiment ou à quelle porte la carte donne accès.

## **Types de cartes et applications possibles**

### **Matériaux de composition des cartes**

#### ***Cartes de plastique standards***

Les cartes de plastique se composent généralement de polychlorure de vinyle (PVC) à 100 %, mais peuvent être combinées à un type de polyester (PET) pour prolonger la durée de vie de la carte. Le PVC se fragilise au fil du temps et est susceptible de se casser s'il est exposé aux intempéries. Afin d'augmenter la durée de vie de la carte, d'autres composants, comme le PET doit être ajouté à la structure de la carte. On appelle les cartes fabriquées à partir d'une combinaison de matériaux des cartes en composite.

#### ***Cartes en composite***

Les cartes en composite peuvent contenir 40 % de PET et 60 % de PVC et peuvent atteindre une durée de vie de trois à cinq ans lorsqu'elles sont utilisées dans de bonnes conditions environnementales. Les cartes en PVC et les cartes en composite sont personnalisées au moyen d'imprimantes de cartes d'identité par procédé de sublimation. Il est possible d'appliquer une couche plastifiée supplémentaire sur la carte pendant le processus de personnalisation pour éviter d'endommager la couche imprimée et prolonger la durée de vie de la carte.

#### ***Polycarbonate***

Les cartes en polycarbonate (PC) sont largement utilisées dans le cadre de programmes relatifs aux permis de conduire. Les cartes en PC peuvent être gravées au laser pour assurer une image beaucoup plus durable; les matériaux utilisés les rendent presque indestructibles. Les cartes en PC ont une durée de vie pouvant atteindre jusqu'à 10 ans.

En plus du matériau utilisé (voir ci-dessus), il est possible d'avoir recours à un autre type de technologie soit sur la carte même, soit dans la structure interne de celle-ci. Les éléments lisibles à la machine permettent d'éliminer toute possibilité d'erreur humaine pendant le processus de collecte des données.

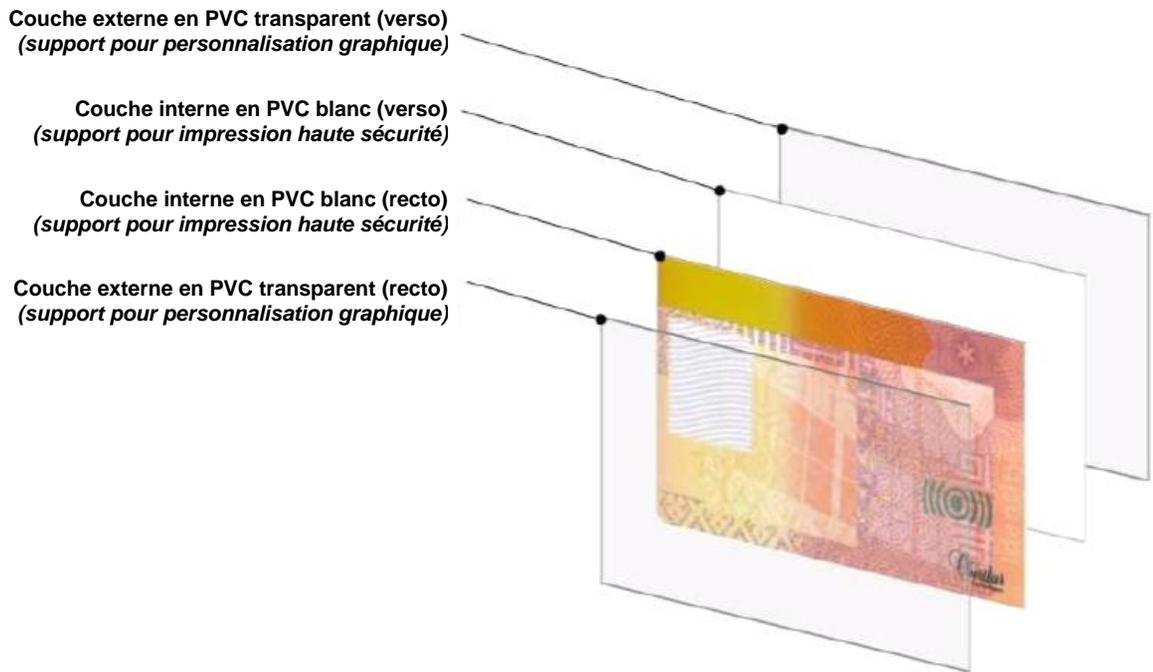


Figure 1 : Couches multiples d'une carte en PVC avant personnalisation

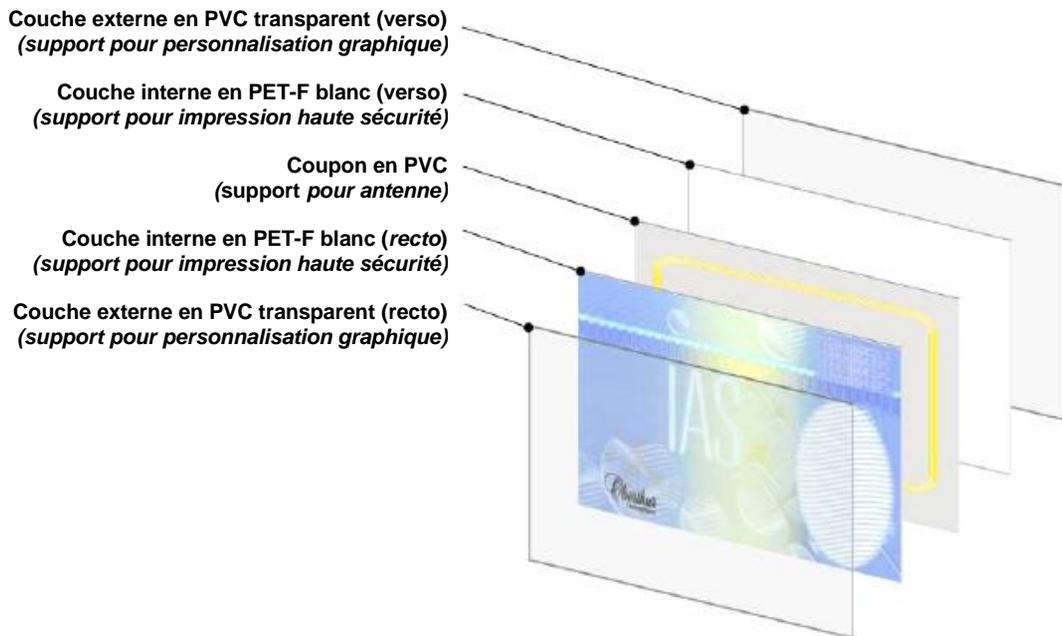


Figure 2 : Couches multiples d'une carte en PET avant personnalisation

## Technologie des cartes

### **Code à barres**

Un code à barres (ou code-barres) est la représentation de données lisibles à la machine par lecture optique. À l'origine, les codes à barres représentaient des données sous forme de lignes parallèles d'épaisseurs variées; on les désigne sous l'appellation symbologie ou codes-barres linéaires ou unidimensionnels (1D). Il existe également des codes à barres qui utilisent une variété de motifs, comme des carrés, des points, des hexagones et d'autres formes géométriques enregistrés sous forme de codes ou de symbologies matriciels ou bidimensionnels (2D). Malgré le fait qu'ils ne contiennent pas de lignes, ces systèmes bidimensionnels sont généralement désignés comme des codes à barres.

Les codes à barres ne peuvent stocker qu'une quantité limitée d'information (par exemple, un numéro à 14 chiffres) et ne peuvent être modifiés une fois qu'ils ont été imprimés, sinon ils ne fonctionneront pas. Ils servent habituellement d'identificateurs de produits dans des commerces de détail et sont souvent utilisés sur les cartes d'identité. On les utilise le plus souvent pour les systèmes de pointage des présences et de prêts dans les bibliothèques.

Les codes à barres n'offrent que très peu de protection, voire aucune et peuvent être reproduits sans difficulté.

### **Estampage en relief**

L'estampage en relief renvoie aux lettres ou aux chiffres qui sont en relief au recto de la carte. Par exemple, les cartes émises par les institutions financières comportent deux formats de caractères : un pour les chiffres inscrits sur la carte et un autre pour le nom du détenteur de la carte. Au dos de la carte, figure un autre numéro (composé de 3 ou 4 chiffres) gravé par l'estampeuse, mais qui ne sont pas en relief. Ce procédé s'appelle « estampage en creux ».

Les cartes estampées en relief sont facilement reproduisibles et n'offrent donc aucune sécurité. Leur utilisation actuelle se limite uniquement lorsque des formulaires de papier carbone sont requis.

### **Bande magnétique**

Les cartes à bande magnétique peuvent stocker des données en modifiant le magnétisme de minuscules particules magnétiques à base de fer qui se trouvent sur une bande fabriquée à partir de matières magnétiques posées sur une carte.

La bande magnétique peut être lue par contact physique et par glissement dans une fente de lecture magnétique. On utilise couramment les cartes à bande magnétique pour les cartes de crédit (aux États-Unis), les cartes d'identité et les titres de transport.

Un certain nombre de normes publiées par l'Organisation internationale de normalisation (ISO), soit les normes ISO 7810, ISO 7811, ISO 7812, ISO 7813, et ISO 4909, décrivent les propriétés physiques d'une carte, y compris les dimensions, la souplesse, l'emplacement de la bande magnétique et les caractéristiques magnétiques. Ces normes visent également les cartes émises par les institutions financières, y compris l'attribution d'une série de numéros de carte à différentes institutions émettrices.

Les bandes magnétiques font partie de deux catégories principales : les bandes à haute coercitivité (HiCo) de 4000 Oe et à basse coercitivité (LoCo) de 300 Oe. Les bandes magnétiques à haute coercitivité sont habituellement offertes à une coercitivité de 2750 Oe. Il est d'ailleurs très difficile de les effacer; par conséquent, ces bandes sont appropriées pour des cartes d'usage fréquent ou pour des cartes qui doivent avoir une longue durée de vie. Les bandes magnétiques à basse coercitivité nécessitent une plus petite quantité d'énergie magnétique pour le stockage de données, et ainsi, les encodeurs de cartes à basse coercitivité coûtent beaucoup moins cher que les encodeurs de cartes à bandes magnétiques à haute coercitivité. Un lecteur de carte peut lire les deux types de bandes magnétiques et un encodeur de carte à bande magnétique à haute coercitivité peut encoder des cartes à bandes magnétiques à haute et à basse coercitivités (la plupart des appareils comportent les deux options, mais l'encodage d'une bande à LoCo en bande à HiCo peut parfois fonctionner), alors qu'un encodeur de cartes à bandes magnétiques à basse coercitivité ne peut encoder que des cartes magnétiques à basse coercitivité.

Les bandes magnétiques à haute coercitivité résistent aux dommages causés par la plupart des aimants susceptibles d'appartenir à des clients. Les bandes magnétiques à basse coercitivité sont facilement endommageables, même par un bref contact avec, par exemple, une courroie ou une attache magnétique de sac à main.

Un numéro exclusif est encodé sur chaque bande magnétique et permet la lecture de la bande par l'appareil (contrairement à une lecture humaine qui comporte des risques d'erreurs inhérentes à ce processus). Les bandes magnétiques protègent mal contre la falsification puisqu'elles peuvent être lues et reproduites par un équipement simple. Toutefois, dans le cadre d'un écosystème qui nécessite l'entrée d'un NIP ou de renseignements

supplémentaires, la bande magnétique s'avère être une technologie très économique pour identifier le détenteur d'une carte et autoriser ses transactions.

### **Carte à puce**

Il s'agit d'une expression générique qui indique que la carte comporte une puce ou une « intelligence ». On l'appelle également carte à circuit intégré ou « carte CI ». Les cartes à puce offrent une très grande protection puisqu'elles permettent le chiffrement de la transaction et l'authentification mutuelle avec leur écosystème (c.-à-d. que la carte et l'écosystème sont compatibles).

Les deux principaux types de cartes CI sont des cartes mémoires et des cartes à processeur.

- Les cartes mémoires ne stockent que des données et protègent peu contre la falsification.
- Les cartes à processeur comportent des microcontrôleurs de sécurité qui authentifient la transaction et effectuent plusieurs lectures et écritures, en plus d'exécuter la logique et des calculs.

Il existe deux types « d'interfaces » de cartes à puce : à contact et sans contact.

- Les cartes à puce à contact comportent une puce visible qui entre en contact avec le lecteur.
- Les cartes sans contact comportent une puce intégrée qui se trouve sous la surface de la carte et une antenne dont les spires sont moulées dans l'épaisseur de plastique de la carte. La puce et l'antenne ne sont pas visibles sur ce type de carte. Les cartes à puce sans contact sont parfois désignées cartes d'identité par radiofréquence.

Il est également possible qu'une carte soit dotée de deux types de technologies.

- Technologie hybride – deux puces intégrées sur la carte, une pour l'interface de contact et l'autre pour l'interface sans contact.
- Technologie à interface double – une seule puce comportant une interface à contact et une interface sans contact interconnectées.

Bon nombre de renseignements techniques et de spécifications relatives aux cartes sont disponibles dans des sites Web comme Wikipédia. Les normes ISO qui suivent portent principalement sur les cartes et leur utilisation.

- ISO 7610 - norme relative aux dimensions et au format de la carte
- ISO 7611 - norme relative à l'estampage en relief et à l'encodage de la bande magnétique
- ISO 7618 - norme relative aux puces intégrées et aux surfaces de contact
- ISO 14443 et 15693 – normes relatives à la transmission sans contact
- ISO 18092 – norme relative à la communication de champ proche (NFC)

Même si les cartes à puce constituent la solution à bien des problèmes d'authentification liés à l'identification, leur utilisation dépend d'un système de terminaux répartis qui peuvent traiter correctement les données stockées dans les cartes. L'achat et la personnalisation de cartes à puce représentent une partie du coût total de l'écosystème de la carte.

## **Sécurité des cartes**

On compte deux catégories principales de dispositifs de sécurité installés sur une pièce d'identité, soit des dispositifs physiques et électroniques.

### ***Dispositifs de sécurité physiques***

Chaque carte devrait comprendre plusieurs dispositifs de sécurité visant à prévenir la falsification. Il existe quatre niveaux principaux de dispositifs de sécurité physiques :

- Niveau 1 – dispositifs facilement reconnaissables (à l'œil nu). Exemples : photographie, hologramme ou guillochis.
- Niveau 2 – dispositifs reconnaissables à l'aide d'un outil de vérification, comme une lampe UV ou une loupe.
- Niveau 3 – dispositifs détectables avec un outil d'investigation informatique légale, ce qui entraîne généralement la destruction du document.
- Niveau 4 – dispositifs de sécurité dont l'existence n'est connue que par le fabricant.

Voici des exemples de dispositifs de sécurité physiques installés sur une carte.

- Hologramme intégré – Hologramme appliqué sous la surface de la carte en PVC, difficile à reproduire et permettant l'impression directe sur toute la surface de la carte, y compris l'hologramme.
- Couches de plastique holographiques de recouvrement – Pellicules plastiques directement appliquées sur la surface des cartes imprimées. En plus d'avoir les avantages anti-falsification des hologrammes, elles contribuent également à augmenter la protection de la surface imprimée de la carte en PVC. Elles protègent également contre l'abrasion causé par le lecteur ainsi que contre l'usure et la détérioration normales. Les dessins holographiques peuvent être imprimés sur la pellicule de transfert.
- Encres irisées et estampage personnalisé sur feuilles métalliques – Feuilles métalliques et encres irisées ayant des propriétés diffractives et

offrant les mêmes avantages anti-falsification que les hologrammes. Elles ne peuvent être reproduites avec précision. On les trouve dans diverses couleurs et modèles et on peut les utiliser pour imprimer des images personnalisées sur des cartes en PVC, du papier Teslin, des pellicules plastiques et des feuilles de papier. Les encres peuvent s'appliquer sur la forme d'un logo ou de toute autre image exclusive à l'organisme.

- Encres thermochromatiques – Encres préimprimées sensibles à la température et changeant de couleur lorsqu'elles sont exposées à une source de chaleur, comme une empreinte digitale.
- Impression irisée – Technique qui consiste à imprimer de deux à quatre couleurs d'encres simultanément sur toute la surface de la carte pour créer une fusion progressive des couleurs semblable à ce qu'on observe dans un arc-en-ciel.
- Impression de microtexte – Impression de très petits caractères. La plupart des photocopieurs ne peuvent reproduire la résolution serrée des microcaractères sans défauts visibles. On trouve souvent une erreur volontaire glissée dans le texte pour en faciliter la détection avec une loupe.
- Guillochis – Motif formé d'un entrecroisement de lignes très fines qui représente une image unique en son genre ne pouvant être reproduite qu'avec l'équipement, le logiciel et les paramètres utilisés pendant la création de la conception initiale.
- Impression UV et impression infrarouge - Image obtenue par impression UV ou infrarouge ne pouvant être visualisée qu'avec un appareil spécial. Si l'on intègre une image personnalisée imprimée de cette façon, on élimine ainsi tout risque de reproduction frauduleuse d'insignes.
- Image dissimulée – Photographie secondaire du détenteur de la carte, obtenue par perforation au laser, visible à la lumière transmise.
- Gravure avec dispositif tactile – Texte gravé au laser sur la surface d'une carte de manière à créer un effet tactile.
- Motif antinumérisation – Zone délimitée par un arrière-plan particulier composé de fines lignes et d'une fusion de couleurs, rendant ainsi la photocopie impossible.

- Code de couleur – Différentes couleurs utilisées pour illustrer divers niveaux d'accès constitue une méthode facile et efficace d'accroître la sécurité. Les couleurs sont des identificateurs visuels évidents qui peuvent être rapidement confirmées à une certaine distance.
- Numérotation séquentielle – Numéro séquentiel incorporé qui renvoie à des renseignements dans une base de données. Cela permet aussi de vérifier que la personne portant l'insigne est autorisée à le faire.
- Filigranes – Procédé anti-falsification qui consiste à intégrer une image (ressemble à la façon dont le papier-monnaie est filigrané) à l'intérieur de cartes en plastique. Il est possible de voir les filigranes si l'on tient la carte devant une source lumineuse.
- Masque de sécurité pour code à barres – Couverture de protection visant à cacher le code à barres.

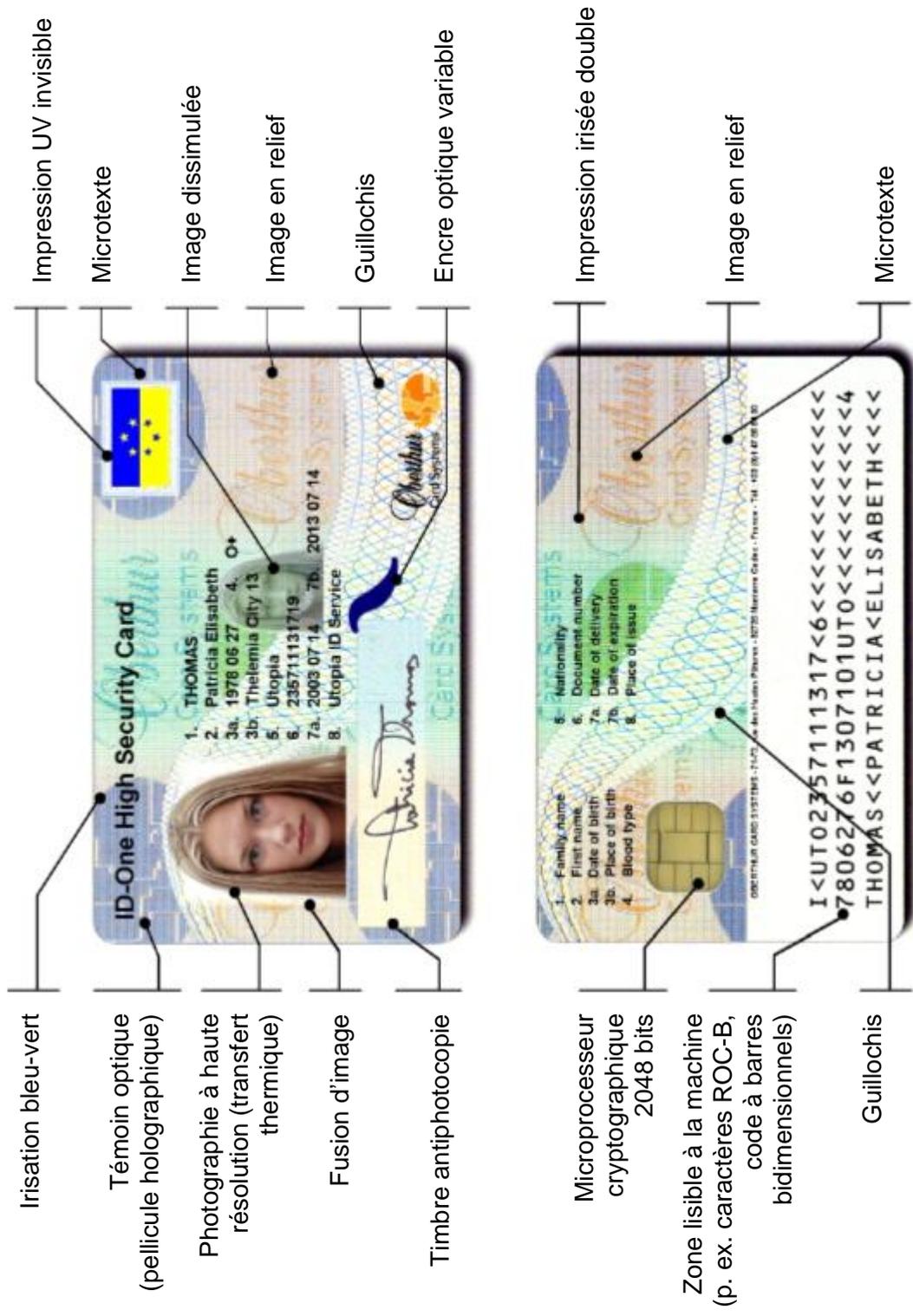


Figure 3 : Exemples de dispositifs de sécurité des cartes

Avec l'arrivée de nombreux moyens d'authentification électroniques qui fonctionnent avec des cartes à puce et des réseaux, l'utilisation de dispositifs de détection visuelle d'éléments falsifiés est très souvent négligée. Cependant, dans les cas où l'authentification électronique du document d'identité ne peut être effectuée (puce endommagée, etc.), des normes reconnues à l'échelle internationale requièrent d'intégrer au document d'autres dispositifs d'authentification. L'Organisation de l'aviation civile internationale (OACI), dont le siège social est à Montréal (Québec), précise que toute pièce d'identité émise est toujours valide, MÊME SI la puce ne fonctionne pas. La puce d'une carte ne constitue qu'UN des nombreux dispositifs de sécurité. Étant donné que les organisations criminelles chercheront toujours le maillon faible pour mener leurs activités frauduleuses, il est essentiel d'intégrer des dispositifs d'identification physiques qui réduisent considérablement les risques de falsification.

### ***Dispositifs de sécurité électroniques***

Dans la plupart des systèmes actuels, l'information est stockée dans un réseau accessible à partir de plusieurs points. Le stockage de données en un seul endroit et l'accès sécurisé en provenance de plusieurs points contribuent à assurer l'intégrité des données et la non-reproduction des ressources ou des renseignements.

Dans le milieu de la protection de l'identité, la carte sert généralement à donner un accès et non à stocker de l'information.

Les cartes à bande magnétique et les cartes à puce contiennent un identifiant exclusif intégré. Pendant une transaction, l'identifiant exclusif est transmis au système aux fins d'authentification, et, une fois l'autorisation obtenue, les renseignements sont partagés avec le lecteur ou l'appareil de requête.

La principale différence entre une bande magnétique et une puce est le niveau de SÉCURITÉ.

Pour moins de 200 \$, il est possible de lire et de reproduire une carte à bande magnétique. Aucune authentification de la carte n'est requise par le système. Ce dernier n'a besoin que de la présentation d'un numéro valide; aucune vérification de la carte n'est effectuée. Le système ne peut différencier une carte originale d'une carte reproduite.

En ce qui concerne les cartes à puce, l'authentification de la carte est au centre de toutes les transactions. Le système peut fournir un degré élevé de certitude qu'aucune reproduction ni falsification de la carte n'ont été tentées. Ce degré de

certitude lie la carte à la transaction avec le degré requis de certitude. Le système peut ensuite partager l'information avec le lecteur ou l'appareil puisque la carte est autorisée à partager ou à recevoir cette information.

On appelle ce processus l'authentification mutuelle (AM).

## **Diverses applications des cartes**

Les pièces d'identité peuvent servir à diverses applications.

### ***Identité***

Déterminer l'identité du détenteur de la carte constitue la fonction principale d'une carte. Un document fiable et précis confirme le lien entre le détenteur de la carte et l'organisme qui utilise la carte.

### ***Finances***

Toutes les banques d'importance et les marchands qui font le traitement de cartes au Canada sont passés à la carte EMV, fondée sur la technologie des cartes à puce à contact et sans contact. La capacité de la carte à puce de résister à la falsification et à la reproduction constitue un facteur essentiel à la diminution des fraudes.

### ***Sécurité physique***

Beaucoup d'entreprises ont déjà fait la transition vers les cartes à puce sans contact pour accroître la sécurité dans les bâtiments. Les cartes à puce permettent d'authentifier la personne par un lecteur de porte à accès contrôlé avant d'échanger les renseignements essentiels secrets qui lancent le déverrouillage des numéros de la carte aux fins de vérification.

### ***Protection des renseignements ou sécurité logique***

De nos jours, les cartes à puce peuvent servir à sécuriser l'accès logique qui gère l'utilisation d'un ordinateur et d'un réseau. Les cartes peuvent également servir à chiffrer des courriels, des transmissions, des transactions et des demandes de connexion. Les cartes à puce servent aussi à appuyer une infrastructure à clés publiques (ICP) lorsqu'il faut assurer un degré de certitude très élevé.

### ***Santé/médecine***

Les cartes peuvent contenir les renseignements qui permettent d'identifier le détenteur de la carte et d'accéder aux services réservés aux personnes autorisées. De plus, on peut sauvegarder dans la mémoire de la carte à puce des registres médicaux portatifs aux fins d'utilisation et d'authentification. Aux États-Unis, les vétérans se servent de leur carte d'identité pour obtenir des soins de santé dans le réseau d'hôpitaux pour vétérans partout au pays.

### ***Adhésion/fidélité***

Les cartes peuvent servir de « carte éclair » ou de carte à solde dégressif. L'expression carte éclair signifie que le détenteur de la carte présente cette dernière pour obtenir un rabais, alors que la carte à solde dégressif indique que la carte accède à une base de données dans laquelle la valeur de la carte est stockée. La transaction permet de déduire un certain montant du compte du détenteur de la carte ou d'enregistrer les achats pour obtenir d'éventuels rabais.

### ***Chiffrement et échange de documents***

Grâce à des certificats de sécurité stockés sur les cartes à puces, les courriels et autres documents électroniques peuvent être signés pour vérifier :

- l'authenticité de l'expéditeur;
- la non-falsification du document transmis;
- le non-reniement (l'expéditeur ne peut pas nier avoir envoyé le document).

### ***Convergence***

Il s'agit d'un terme utilisé pour décrire la combinaison continue des applications sur une seule pièce d'identité (c.-à-d. une seule carte à puce peut franchir la « porte », se connecter à un ordinateur, authentifier des demandes d'accès au réseau et payer un repas à la caisse de la cafétéria). Plusieurs applications peuvent utiliser plusieurs technologies sur la carte.

## **Approche fondée sur les normes -- un aperçu de la PIV**

*\* Basé sur les renseignements obtenus dans le document IC-08002 de la Smart Card Alliance*

La « Personal Identity Verification » (PIV) est une norme du gouvernement fédéral américain élaborée à la suite des événements du 11 septembre dans le but de créer un cadre de référence stricte pour la gestion de l'identité. Les gouvernements américains et les industries établies aux États-Unis ont travaillé pendant plus de dix ans à l'élaboration d'un processus normalisé d'identification visant à vérifier l'identité des personnes et à fournir des pièces d'identité sécurisées.

### ***Historique***

Le 27 août 2004, la Maison Blanche publiait la Directive présidentielle sur la sécurité intérieure 12 (HSPD-12), qui vise à accroître la sécurité et l'efficacité du gouvernement, à réduire les vols d'identité et à protéger la vie privée en établissant une norme obligatoire gouvernementale relative à une identification fiable et sûre. La directive HSPD -12 prescrit l'utilisation d'une pièce d'identité commune.

À la suite de la publication de cette directive, le National Institute of Standards and Technology (NIST) publiait à son tour, au début de l'année 2005, une norme de la série Federal Information Processing Standards (FIPS) portant le numéro 201 et intitulée « Personal Identity Verification (PIV) of Federal Employees and Contractors ». La norme FIPS 201 fournit un cadre de gestion de l'identité auquel les entreprises devraient se reporter pour concevoir et mettre en œuvre leur propre programme de gestion de l'identité.

La norme FIPS 201 définit les exigences en matière de validation de l'identité, d'inscription et d'émission d'une pièce d'identité commune ainsi que les spécifications techniques visant les cartes d'identité utilisées par les gouvernements et les entrepreneurs, ou cartes PIV.

Les cartes PIV ne peuvent être émises que par des agences fédérales. Il existe deux autres types de cartes PIV :

- la carte PIV-I (interopérable) est une carte construite selon les mêmes spécifications techniques que la carte PIV standard, mais elle est émise par d'autres agences fédérales et nécessite un accès aux ressources

fédérales. D'autres organismes gouvernementaux non fédéraux et de grands entrepreneurs employés par le gouvernement fédéral, comme Lockheed Martin ou Boeing, utilisent aussi la carte PIV-I;

- la carte CIV (anciennement PIV-C) pour « Commercial Identity Verification » est destinée à un usage commercial. Les cartes CIV peuvent être émises par n'importe quelle entité commerciale selon les politiques et procédures de celle-ci, toutefois, la puce doit être conforme à la même norme technique.

### ***Incidences de la norme FIPS 201***

Les cartes d'identité et les insignes ont évolué, passant de jetons imprimés à des documents sécurisés qui incorporent une technologie lisible à la machine. Les anciennes pièces d'identité validaient un privilège et, afin de lier la pièce d'identité à son détenteur, les renseignements sur l'identité pouvaient avoir été imprimés ou écrits sur la surface de la carte ou de l'insigne.

Pour valider rapidement la pièce d'identité, les émetteurs devaient fournir une infrastructure en mesure de vérifier le statut en cours du détenteur de la pièce d'identité. Les pièces d'identité lisibles à la machine sont devenues la norme pour faciliter la vérification rapide. Ainsi, les pièces d'identité vérifiées visuellement jouent un rôle différent de celui des pièces d'identité vérifiées électroniquement. Un insigne imprimé peut valider une identité et un privilège. Une pièce d'identité lue par un système électronique ne valide que l'identité. Le système détermine les privilèges autorisés pour le détenteur de la pièce d'identité.

Un nombre croissant d'organismes gouvernementaux et de grandes sociétés utilisent maintenant les cartes à puce comme moyen d'identification pour leurs employés. La technologie des cartes à puce permet de stocker les renseignements d'identité de l'employé en toute sécurité pour que ceux-ci soient accessibles aux fins de vérification rapide et automatisée. Ces renseignements serviront aussi à déterminer si l'employé est autorisé à accéder aux ressources ministérielles ou aux ressources de l'entreprise.

L'utilisation de cartes à puce permet à l'émetteur de confirmer que la personne qui recevra la carte peut accorder un degré élevé de confiance à l'information qui se trouve sur la carte. Cette information comprend, entre autres, des renseignements personnels (par exemple, des données biométriques ou une photographie numérique signée) ou des privilèges (comme un porte-monnaie électronique ou un certificat numérique permettant de se connecter à un

ordinateur). De plus, puisqu'une carte à puce possède une puissance de calcul, il peut s'avérer nécessaire que l'utilisateur s'authentifie en entrant un NIP ou, dans certains cas, des données biométriques avant que la carte ne communique avec le système de requête. Finalement, les cartes à puce peuvent comporter une technologie utilisant des méthodes cryptographiques visant à établir une voie de communication sécurisée entre le lecteur et la carte (par exemple, au moyen d'une méthode d'appel-réponse qui nécessite que le système de requête s'authentifie auprès de la carte à puce avant d'établir la communication).

Dans n'importe quel système de validation de l'identité sécurisé, le processus d'émission est aussi important que la protection de la pièce d'identité. Le processus d'émission doit relier la personne aux vérifications des antécédents et aux essais réalisés avant l'émission de la pièce d'identité. Une fois la pièce d'identité émise, le processus de gestion de la durée de vie de la pièce doit comprendre les processus d'authentification, de révocation et de réémission. Les parties utilisatrices n'auront confiance en une pièce d'identité que si elles jugent que les processus d'émission et de gestion de la durée de vie sont sûrs.

### ***Importance de la PIV***

Pour la première fois, les organismes sont en mesure d'utiliser une approche axée sur les normes pour les cartes d'identité et d'appliquer les pratiques exemplaires à leurs programmes de cartes d'identité respectifs. La norme FIPS 201 et le processus de vérification de l'identité personnelle définissent un certain nombre d'étapes importantes.

**Parrainage.** Un parrain doit se porter garant de la demande d'une personne concernant une pièce d'identité pour une entreprise et doit autoriser l'inscription du demandeur. Le parrain peut également autoriser les coûts engagés dans le cadre du processus de validation de l'identité.

**Inscription.** Le processus d'inscription est conçu pour vérifier l'identité d'un demandeur et pour recueillir les renseignements personnels de ce dernier. Les demandeurs doivent apporter deux formulaires d'identification. Au moment de l'inscription, on prendra leurs empreintes digitales et une photographie. L'information ainsi recueillie servira à effectuer les vérifications de conformité et à créer la pièce d'identité.

**Attribution.** Un arbitre de confiance détermine si un demandeur devrait se voir attribuer une pièce d'identité en fonction des résultats obtenus à la suite de la vérification de conformité. Les procédures de validation de l'identité (p. ex. la vérification des casiers judiciaires, la scolarité, l'expérience professionnelle, les

antécédents en matière de crédit et la vérification des compétences déclarées) font partie du processus d'attribution dont les facteurs d'exclusion sont définis dans les procédures de validation. La réussite du processus d'attribution entraîne la production de la pièce d'identité. Le niveau d'attribution varie d'un organisme à un autre en fonction du niveau de sécurité ou d'accès requis. L'attribution peut être structurée de manière que les personnes devant accéder, par exemple, à un centre d'exploitation du réseau ou à un centre des opérations de sécurité soient soumises à un processus d'évaluation plus long.

**Fabrication de pièces d'identité.** Les pièces d'identité peuvent être personnalisées dans une installation centralisée ou à un bureau local d'émission. Des renseignements pertinents sont imprimés conformément aux normes, des dispositifs de sécurité sont incorporés et une puce électronique (carte à puce) est encodée avec des renseignements personnels.

**Émission et activation.** Lorsqu'un demandeur se présente pour obtenir sa pièce d'identité personnalisée, l'émetteur confirme l'identité du demandeur en revérifiant les documents d'identité soumis au moment de l'inscription et en faisant correspondre l'empreinte digitale du demandeur avec celle utilisée pour l'inscription. Par la suite, on « déverrouille » la pièce d'identité, on charge des certificats numériques et un NIP sur la puce et on remet la pièce d'identité au demandeur pour qu'il l'utilise.

**Utilisation des pièces d'identité.** Les pièces d'identité activées peuvent servir à valider l'identité d'une personne de façon électronique et à accéder à des secteurs et à des réseaux informatiques sécurisés.

Toutes ces étapes doivent être appuyées non seulement par la technologie, mais aussi par des politiques et des procédures. L'intégrité globale du système ne peut être assurée que par l'exécution et l'application uniformes de politiques et de procédures. La norme FIPS 201 constitue un cadre de pratiques exemplaires pour le processus complet de vérification de l'identité et de l'émission des pièces d'identité que les entreprises peuvent utiliser pour mettre en œuvre un système très efficace de gestion de l'identité de leurs employés.

La carte PIV figurant dans la norme FIPS 201 offre les avantages suivants par rapport aux autres types de carte à puce :

- Elle est utilisée par un grand éventail de fabricants et d'intégrateurs.

- Elle ne contraint pas un organisme à faire appel aux services d'un seul fournisseur de composants principales.
- Elle offre des fonctions souples d'authentification, de signature et de chiffrement.
- Elle est en mesure de s'adapter aux nouvelles technologies, comme la biométrie.
- En tant que norme consultée par des organismes fédéraux pour l'émission de pièces d'identité à des millions d'employés et d'entrepreneurs fédéraux américains, la norme bénéficie du nombre d'utilisateurs.
- Elle fournit un cadre de référence en appui à l'interopérabilité des pièces d'identité parmi les divers organismes.

En raison de ces facteurs, la mise en place d'une méthode axée sur des pièces d'identité conçues selon le principe des cartes PIV fondé sur la norme FIPS 201 peut s'avérer extrêmement avantageuse pour les organismes à l'extérieur du gouvernement fédéral américain. Un organisme qui utilise le modèle et la norme FIPS 201 peut profiter d'un degré de fonctionnalité élevé à des prix de volume avantageux. La technologie de vérification de l'identité a fait l'objet d'un examen approfondi et est reconnue par les plus hautes instances. Le processus de validation de l'identité est souple et a été minutieusement examiné pour constituer la meilleure pratique.

## **Choisir la bonne technologie pour son organisme**

Effectuer une évaluation des risques standard peut aider à choisir le type de technologie de carte.

1. Comprendre son organisme, ses procédés, ses employés et ses biens à risque.
2. Déterminer les pertes, les risques et les vulnérabilités.
3. Déterminer les conséquences et le coût possibles associés à une perte.
4. Effectuer une analyse des coûts et des avantages.

### ***1. Comprendre son organisme***

Il importe de bien comprendre le but de la carte d'identité nationale des vétérans. Plus précisément, quels sont les privilèges associés à la carte et quels avantages peut-on tirer lorsqu'on présente sa carte et confirme son identité? Les éléments suivants devraient être considérés :

- la quantité de cartes en circulation;
- le délai requis pour la distribution initiale;
- la distribution des cartes (à l'échelle nationale ou mondiale);
- la distribution des services offerts ou les endroits où la carte doit être présentée;
- les types de services offerts par la carte;
- le type de renseignements personnels partagés;
- la valeur des services offerts grâce à la carte.

### ***2. Déterminer les pertes et les risques***

La carte peut-elle être reproduite ou falsifiée?

La carte est-elle associée au détenteur de la carte par une photographie, un NIP ou par des renseignements biométriques?

La carte peut-elle être utilisée par une autre personne que le détenteur de la carte?

L'identité du détenteur de la carte peut-elle être volée, modifiée ou compromise?

### ***3. Déterminer les conséquences associées à une perte***

En cas de perte ou de vol d'une carte, à quels avantages peut-on avoir accès avec la carte?

Quel type d'information peut être compromise?  
Quel est le coût associé à la perte d'une carte?  
Est-il possible d'estimer à quelle fréquence on peut perdre sa carte?

#### ***4. Effectuer une analyse des coûts et des avantages***

Il est habituellement très difficile de définir les avantages associés à l'utilisation d'une carte d'identité. Bien souvent, il n'est pas possible de quantifier la valeur monétaire de ce qu'offre réellement une carte d'identité, comme relier un groupe de personnes différentes à une appartenance commune qui éprouvent ainsi un plus grand sentiment de bien-être qui ne se définit pas en termes monétaires.

Il importe de comparer le coût associé à l'émission des cartes d'identité actuellement en utilisation avec le coût d'un nouveau système et des avantages qu'il pourrait offrir. Si l'on ne définit pas clairement les avantages liés à une nouvelle carte, il ne sera pas possible d'évaluer parfaitement le rendement du capital investi (RCI).

#### **Formule de base pour le calcul du RCI :**

Coût du programme existant - Coût du nouveau programme = Coût réel du programme

Coût réel du programme = Rendement du capital investi  
Avantages offerts

## **Fonctions, sécurité et stockage des cartes à puce**

Les cartes à puce peuvent stocker et extraire des données grâce à leur mémoire interne. Les données sont stockées dans des dossiers. Chaque dossier doit être nommé et répertorié pour que la carte sache dans quel dossier sont stockées les données. Les cartes à puce peuvent contenir 1 K, 4 K, 64 K et jusqu'à 128 K ou plus d'information. Dans les nombreux cas où le détenteur de la carte doit être authentifié comme étant l'utilisateur autorisé de la carte, les renseignements biométriques (empreintes digitales ou image de l'iris de l'utilisateur) sont stockés sur la carte aux fins de comparaison.

Le principal avantage d'utiliser une carte à puce est que l'authentification de celle-ci et du détenteur peut être incorporée dans un nouveau programme global de vérification d'identité. Les cartes à puce contribuent à réduire les risques de falsification, d'ajout ou de suppression d'information. Elles assurent également un degré de certitude élevé en ce qui concerne l'intégrité du programme de vérification d'identité en plus de permettre un échange de renseignements ou d'avantages de plus hauts niveaux.

### **Sécurité des cartes à puce – cryptographie, ICP et AC**

L'Internet contient une foule de renseignements sur la cryptographie et les infrastructures à clés publiques (ICP).

On trouve, au cœur des cartes à puce, des renseignements stockés sur la puce dans un milieu sécurisé. Chaque carte à puce comporte un algorithme sécurisé qui sert à chiffrer et à déchiffrer l'information. Cette cryptographie est protégée contre les attaques physiques et virtuelles grâce à diverses contre-mesures.

Une infrastructure à clés publiques consiste en un ensemble de matériel, de logiciel, de personnes, de politiques et de procédures qui visent à créer, gérer, distribuer, utiliser, stocker et révoquer des certificats numériques. Un certificat numérique est un document électronique qui relie une clé à une identité. Une ICP comprend une clé publique et une clé privée.

Les clés privées et publiques peuvent être produites par la carte. La clé privée est stockée sur la carte (elle ne quitte jamais la carte) alors que la clé publique est partagée avec l'autorité de certification (AC). L'AC approuve ensuite la validité des clés publiques et privées, et délivre un certificat. Ce certificat peut être stocké sur la carte puis comparé au certificat initial lorsqu'une transaction doit être effectuée. Grâce à la gestion de la liste des certificats révoqués (LCR)

par l'AC, la transaction peut être validée comme étant authentique et autorisée. Si l'autorité de certification retire le certificat, la demande de transaction effectuée par la carte sera rejetée. Ce milieu, qui comprend des clés, de la cryptographie et des autorités de certification s'appelle une infrastructure à clés publiques. Il s'agit, en ce moment, de la méthode d'authentification la plus sûre qui existe.

## **L'avenir de la technologie des cartes et pratiques exemplaires**

Au fur et à mesure que les demandes relatives à la sécurité augmentent, l'industrie utilise de plus en plus les cartes à puce pour garantir l'authenticité et la sécurité des transactions et des appareils. Grâce à leur logique intégrée, à leurs calculs et à leurs processus d'authentification, les cartes à puce servent entre autres à appliquer correctement les politiques en matière de protection des renseignements personnels et de sécurité qu'exigent la plupart des programmes d'identification. Les cartes à puce peuvent fonctionner dans un grand éventail de milieux, mais doivent être commandées à partir d'un lieu central.

### **Pratiques exemplaires**

La liste des pratiques exemplaires qui s'appliquent au présent projet s'applique également à n'importe quel projet de gestion de l'identité.

1. Prioriser les facteurs opérationnels dès le début du projet et se concentrer sur les éléments livrables les plus urgents.
2. Embaucher des intervenants tôt dans le projet et exposer clairement les éléments livrables et l'échéancier du projet. Encourager les intervenants à participer à la création du projet plutôt que de reporter à plus tard des conversations avec certains d'entre eux. Tout projet d'identification comporte des enjeux complexes en matière de protection des renseignements personnels qui doivent être pris en compte à l'étape de la planification.
3. Embaucher un parrain au niveau de la direction. Celui-ci contribuera à résoudre les conflits entre les intervenants et à accélérer les processus décisionnels.
4. Faire appel aux experts en technologies de l'information (TI). On ne saurait trop insister sur l'importance de ces ressources. Une fois le projet livré et mis en place, ces experts en TI constituent le premier niveau de soutien. Leur implication est essentielle au succès du programme.
5. Embaucher un expert technique (similaire à l'article 3) qui deviendra l'administrateur permanent du système de l'infrastructure du projet d'identification et le faire participer au choix des produits.
6. Mesurer le succès. Établir des paramètres pour appuyer chaque facteur opérationnel, puis mesurer les résultats avant et après la mise en œuvre.
7. Commencer à travailler à des éléments livrables de moindre envergure et simples, puis à des intégrations et des fonctions plus complexes.

Répartir la mise en œuvre des fonctionnalités dans le temps et améliorer continuellement le produit.

8. Planifier l'acceptation par l'utilisateur, les essais et surtout, les programmes de sensibilisation destinés aux utilisateurs. Informer les utilisateurs sur le produit pour les encourager à choisir votre produit plutôt que d'autres options.

Plus particulièrement, dans le milieu des cartes d'identité et de la vérification de l'identité, un élément essentiel domine. Dans la plupart des cas, ce sont les plus récentes technologies disponibles qui suscitent le plus d'intérêt. Dans le monde des organismes émetteurs de documents d'identité, il y a eu un empressement à utiliser une méthode d'authentification électronique. Fait intéressant : perdue dans la forte poussée vers l'utilisation des cartes à puce et des ICP, l'utilisation de dispositifs de sécurité physiques sur les cartes a aussi augmenté considérablement.

Il est primordial que les documents d'identité contiennent divers dispositifs de sécurité physiques et électroniques pour permettre une authentification à plusieurs niveaux. Aucune méthode d'authentification ne devrait être considérée comme fiable à 100 %.

## **L'avenir de la technologie des cartes**

La durée de vie des cartes d'identité est au cœur de débats depuis une dizaine d'années. On remarque une hausse de la demande pour des dispositifs d'authentification électroniques, comme des cartes à puce et des jetons, ainsi qu'un engouement récent pour la technologie de communication en champ proche (NFC).

Avec la technologie NFC, la puce qui se trouvait habituellement sur la carte de crédit est passée au téléphone mobile dont la puce comprend un élément sécurisé (ES) à plusieurs composants, comme un objet d'identité sécurisé (SIO) et des certificats. Ces composants sont stockés sur la puce, tout comme l'information est stockée sur une carte à puce, et peuvent être utilisés dans le cadre d'une ICP pour des transactions financières et des transactions d'identification. Certains experts proposent que l'utilisation des cartes puisse être éliminée grâce à cette nouvelle technologie.

Cependant, il importe de tenir compte des conditions dans lesquelles la transaction d'identification a lieu et s'il y a, ou non, une infrastructure connexe pouvant l'appuyer.

À moins d'avoir recours à une infrastructure d'envergure (et coûteuse) pour appuyer l'utilisation de pièces d'identité électroniques, la carte d'identité traditionnelle demeure le moyen idéal pour valider une identité. Si l'on incorpore un dispositif de sécurité physique qui réduit les risques de falsification, la carte d'identité est relativement peu coûteuse et constitue la seule solution de rechange pour vérifier une identité en cas de panne de courant.

Si l'on jette un coup d'œil à nos porte-monnaie d'aujourd'hui, nous y trouverons une grosse quantité de cartes de crédit et de documents d'identité, conçus pour valider notre identité dans différents systèmes. Les entreprises qui émettent ces cartes et ces documents ont des intérêts financiers importants pour maintenir leur statut « supérieur » en offrant une variété d'avantages et de services. La surface occupée sur la carte est un élément de marketing important pour ces entreprises, et jusqu'à maintenant, on ne sait pas exactement comment cette guerre de territoire pour obtenir les dollars des consommateurs se terminera. Par exemple, si la puce de NFC intégrée dans un téléphone mobile contient les renseignements de la carte de crédit d'un consommateur, l'image de marque du fournisseur de crédit a complètement disparue. Pour cette raison, les entreprises ayant des intérêts financiers à connaître l'identité des consommateurs utilisent toujours la carte comme moyen de choix.

Nous croyons que l'utilisation de la carte d'identité comme document d'identité demeurera pendant dix ans encore un élément essentiel de tout programme d'identification.

## **Émission des cartes**

Il existe deux méthodes principales d'émission de cartes d'identité : méthode d'émission centralisée et méthode d'émission répartie.

### **Émission répartie des cartes**

On utilise l'émission répartie des cartes lorsqu'il y a des problèmes de livraison importants pour envoyer les documents d'identité au détenteur de la carte. En Indonésie, un programme d'émission de permis de conduire s'est terminé il y a quelques années à l'aide des options fournies par Digital Identification Solutions, fonctionnait selon une stratégie d'émission répartie des permis de conduire. La communication entre les centaines de petites îles s'est avérée difficile et l'organisation d'une livraison sécurisée des cartes par courrier a été difficile. Le problème a été résolu grâce à la mise en place de bureaux locaux où les résidents ont pu faire leur demande pour une carte d'identité et la recevoir. Les permis de conduire ont été imprimés à l'aide d'imprimantes de cartes.

L'encodage des cartes à code-barres, à bande magnétique et à puce peut être effectué en même temps que la personnalisation. Il est maintenant possible de graver au laser avec des appareils de bureau.

En moyenne, le processus d'impression répartie des cartes est 37 % plus cher que le processus d'émission centralisée. Les coûts explicites d'une émission répartie comprennent, sans toutefois s'y limiter, les dispositifs de protection des cartes, les coûts associés au personnel, la surface utile, les postes de saisie des données, les imprimantes, les serveurs, l'hébergement et la mise en réseau des serveurs et les coûts d'entretien et d'installation.

### ***Avantages d'une émission répartie***

<b>Rapidité</b>	Service à la clientèle très rapide. Cela ne prend habituellement que quelques minutes avant que le client reçoive sa carte d'identité.
<b>Distribution</b>	Réduction ou élimination des problèmes liés au courrier ou aux services de messagerie.

### ***Inconvénients d'une émission répartie***

<b>Protection des cartes</b>	<p>Il est difficile de gérer un gros stock réparti partout au pays.</p> <p>Il arrive souvent que des articles manquants ne soient pas immédiatement signalés.</p> <p>Les articles perdus ou volés menacent l'intégrité de l'ensemble du programme d'identification.</p>
<b>Vol d'imprimante</b>	<p>Le vol d'imprimantes de cartes d'identité entraîne un temps d'arrêt catastrophique au centre d'exploitation.</p> <p>L'imprimante volée peut servir à créer des documents non autorisés qui semblent identiques aux documents originaux.</p>
<b>Entretien</b>	<p>Les imprimantes de cartes doivent être entretenues et utilisées avec soin.</p>
<b>Coût associé au personnel</b>	<p>Le personnel formé doit faire fonctionner une imprimante de cartes.</p> <p>Le roulement de personnel fait en sorte que des personnes non qualifiées exploitent les appareils.</p> <p>Les coûts associés à une nouvelle formation sont élevés.</p> <p>Il faut des spécialistes en soutien de composants particuliers.</p>
<b>Coût global du projet</b>	<p>Le coût moyen est d'environ 37 % supérieur au coût d'une émission centralisée. (Source : Oberthur Technologies)</p>

## **Émission centralisée des cartes**

On utilise un processus d'émission centralisée lorsqu'il faut imprimer une grande quantité de cartes et qu'il existe déjà un système de distribution par courrier sécurisé. Une émission centralisée permet de gérer les millions de demandes initiales de cartes plus les demandes de cartes de remplacement et de nouvelles demandes de cartes.

Dans le cadre du processus d'émission centralisée, les données peuvent être consignées en ligne ou saisies à des bureaux éloignés. Les données sont stockées sur un serveur central aux fins de traitement à un seul site. On entrepose le matériel d'impression et le papier cartonné dans un local sécurisé et seul le personnel formé et autorisé utilise le matériel.

Ce processus d'émission centralisée peut être simplifié pour y inclure l'impression de papier et de papier à en-tête, le collage des cartes sur le papier, le pliage, l'insertion dans une enveloppe et les envois postaux. À l'installation finale, les données sont normalement envoyées par voie électronique au centre de traitement et les boîtes de courrier trié sont livrées à Postes Canada à la fin de la journée. Une installation de traitement à émission centralisée peut généralement produire plusieurs milliers de documents d'identité par jour, selon la complexité des documents.

Les centres de traitement à émission centralisée peuvent être installés par un client dans ses locaux ou encore, l'ensemble du programme de traitement des documents d'identité peut être confié à une tierce partie digne de confiance.

### ***Inconvénients d'une émission centralisée***

<b>Rapidité</b>	Les clients doivent patienter de une à deux semaines environ pour recevoir leurs documents d'identité.
-----------------	--

### ***Avantages d'une émission centralisée***

<b>Volume</b>	On peut fabriquer un grand nombre de cartes par année (des milliers à des millions).
<b>Protection du matériel</b>	Les imprimantes sont entreposées dans une installation sécurisée où seules les personnes autorisées peuvent y accéder.
<b>Détenteurs de cartes</b>	Les détenteurs de carte sont répartis sur une vaste zone géographique.
<b>Continuité des activités</b>	Une fonction de reprise après sinistre, des procédures et un système de sauvegarde entièrement automatisés sont en place.
<b>Sécurité des documents d'identité</b>	Les cartes et les impressions sont protégées.
<b>Protection des documents d'identité</b>	Une seule méthode de protection contre la falsification peut être employée. Cette méthode n'est pas disponible sur les imprimantes de cartes.
<b>Durée de vie des documents d'identité</b>	Les cartes ont une durée de vie supérieure en raison des méthodes de fabrication et de personnalisation utilisées.
<b>Souplesse</b>	On peut gérer de très gros volumes de demandes initiales (millions de cartes) en plus des demandes courantes soumises chaque année.
<b>Expansion éventuelle</b>	Il est possible d'incorporer des puces et des fonctions d'authentification avancées sans devoir racheter du nouveau matériel (imprimante) et modifier les postes de saisie existants au pays.

<b>Coût</b>	En moyenne, le processus d'impression centralisée des cartes est 37 % plus économique que le processus d'émission répartie, calculé sur la durée de vie du programme d'émission de cartes.
-------------	--

## Exigences relatives à l'émission des cartes

Les exigences relatives à l'émission des cartes diffèrent selon le choix de la méthode d'impression qui peut être répartie ou centralisée.

### Matériel et logiciel

Dans un modèle d'émission répartie, le matériel suivant est nécessaire à chaque emplacement :

- PC
- Caméra
- Appareils sécurisés d'accès réseau (RPV, pare-feux, etc.)
- Imprimante de cartes et machine à plastifier
- \*\* Facultatif : encodeurs de cartes à puce
- Délivrance d'une licence pour le logiciel

Dans un modèle d'émission centralisée, le matériel suivant peut être nécessaire à chaque endroit :

- tout ce qui précède, SAUF l'imprimante de cartes et la machine à plastifier.

L'imprimante de cartes et la machine à plastifier sont des pièces d'équipement les plus chères dans un poste d'émission répartie et peuvent coûter plus de 12 000 \$ selon les fonctionnalités nécessaires. Des encodeurs de cartes à puce peuvent être intégrés à l'imprimante afin que l'impression et l'encodage se fassent en une seule étape. Ces encodeurs seraient nécessaires SEULEMENT si une technologie de cartes à puce est utilisée.

Tant pour l'impression répartie que centralisée, il est nécessaire d'avoir un accès réseau sécurisé à un serveur central. Les données sont toujours stockées dans une mémoire centralisée peu importe la méthode d'impression choisie.

Dans un modèle d'émission centralisée, il faut disposer d'un local dans une installation sécurisée pour y placer l'imprimante et le papier. De manière générale, ces installations sont beaucoup mieux protégées que les bureaux locaux et ils offrent un plus haut niveau de sécurité. La surveillance par télévision en circuit fermé (TVCF), le contrôle de l'accès et des employés qui sont habilités et autorisés, permettent de garantir un milieu opérationnel sécurisé.

## **Personnel**

Dans le cas de postes d'impression et de prise de photos répartis, un employé affecté à chaque poste peut produire des cartes, selon un rapport de un sur un. Dans le cas d'une méthode d'impression centralisé, un seul employé peut exploiter plusieurs postes d'impression de cartes ou deux employés peuvent exploiter une grosse imprimante conçue pour traiter des centaines ou des milliers de cartes à l'heure.

Voici, à titre informatif seulement, une liste de pièces d'équipement démontrant ce qu'il faut réellement se procurer pour un déploiement à grande échelle du modèle d'émission centralisée. Dans ce cas-ci, nous supposons qu'il y a trois PC par emplacement (33 emplacements en tout) pour émettre 1 000 000 cartes la première année du projet.

#### NOMENCLATURE

Fonction	Type d'équipements	Description technique	Qté	Pièces de rechange / total	Dév. et maint.	Qté totale
Pièce d'identité	Cartes plastifiées	Cartes PETF avec préimpression de sécurité avancée	1000000	10000		1010000
<b>Cartes</b>	<b>SOUS-TOTAL</b>					
Inscription	Ordinateur	Dell Optiplex 380 avec Windows XP édition Professionnel ou équivalent	99			99
Inscription	Antivirus	F-Secure	99			99
Inscription	Scanneur à plat	Canon CanoScan LiDE 100 ou équivalent	66			66
Inscription	Lecteur de codes à barres	Lecteur de codes à barres numérique USB Motorola PDF417 ou équivalent	99			99
Inscription	APN	À déterminer	66			66
Inscription	Câble	Câble RJ45 de catégorie 6 (3 m de longueur pour PC)	99			99
Inscription	Logiciels	Logiciels du fournisseur	99			99
<b>Inscription</b>	<b>SOUS-TOTAL</b>					
Personnalisation	Ordinateur	Dell Optiplex 380 avec Windows XP édition Professionnel ou équivalent	1	1		2
Personnalisation	Antivirus	F-Secure	1	1		2
Personnalisation	Imprimante de cartes	Datacard MX1000 ou équivalent	1	1		2
Personnalisation	Câble	Câble RJ45 de catégorie 6 (3 m de longueur pour PC)	1	1		2
Personnalisation	Machine à plastifier	Fasver 6041P	1	1		2
<b>Personnalisation</b>	<b>SOUS-TOTAL</b>					
Emballage	Ordinateur	Dell Optiplex 380 avec Windows XP édition Professionnel ou équivalent	3	1		4
Emballage	Antivirus	F-Secure	3	1		4
Emballage	Alimentation sans coupure	ASC Dell, format tour, 500 W, 230 V avec cordon d'alimentation C13 à C14 de 2 m – kit	3	1		4
Emballage	Câble réseau	Câble RJ45 de catégorie 6 (3 m de longueur pour PC)	3	1		4
Emballage	Lecteur de codes à barres numérique	Lecteur de codes à barres numérique USB Motorola PDF417 ou équivalent	3	1		4
Emballage	Machine à emballer	Flexiwrap ou équivalent	3	1		4
Emballage	Imprimante de bordereaux d'expédition	Imprimantes laser HP : modèle 1505 ou équivalent	3	1		4
<b>Emballage</b>	<b>SOUS-TOTAL</b>					
Gestion des stocks / Administration du système	Ordinateur	Dell Optiplex 380 avec Windows XP édition Professionnel ou équivalent	1	1		2
Gestion des stocks / Administration du système	Antivirus	F-Secure	1	1		2
Gestion des stocks / Administration du système	Câble réseau	Câble RJ45 de catégorie 6 (3 m de longueur pour PC)	1	1		2
Gestion des stocks / Administration du système	Lecteur de codes à barres numérique	Lecteur de codes à barres numérique USB Motorola PDF417 ou équivalent	1	1		2
Gestion des stocks / Administration du système	Imprimante de bordereaux	Imprimantes laser HP : modèle 1505 ou équivalent	1	1		2
<b>Gestion des stocks / Administration du système</b>	<b>SOUS-TOTAL</b>					
Expédition	Ordinateur	Dell Optiplex 380 avec Windows XP édition Professionnel ou équivalent	33	1		34
Expédition	Antivirus	F-Secure	33	1		34

Expédition	Lecteur de codes à barres	Lecteur de codes à barres numérique USB Motorola PDF417 ou équivalent	33	1		34
Expédition	SOUS-TOTAL					
Serveur de personnalisation	Administration des bases de données du serveur	Cartes à processeur	1			1
Serveur de personnalisation	Bâti	Boîtier sur bâti 42U pour serveurs Dell PowerEdge 4220 avec portes et panneaux latéraux, configuration standard	1			1
Serveur de personnalisation	Serveur FTP et serveurs d'émission et de collecte	Serveur Dell PowerEdge à quatre cœurs R200 avec processeur Xeon X3330 (2,66 GHz, 2 x 3 Mo, bus frontal cadencé à 1333 MHz, TDP de 96 W) ou équivalent	1			1
Serveur de personnalisation	Serveur de domaine	Active Directory des cartes à processeur - Surveillance - Serveur de mise à jour de l'antivirus	1			1
Serveur de personnalisation	Système de stockage LTO	Dell PowerVault 124T LTO4	1			1
Serveur de personnalisation	Bandes LTO	Bandes de type LTO4	24			24
Serveur de personnalisation	Sauvegarde	Logiciel Symantec Backup Exec et contrôleur matériel pour la gestion du système de sauvegarde sur bandes	1			1
Serveur de personnalisation	ASC sur bâti	ASC sur bâti 4U Dell pour serveurs PowerEdge 4220 avec contrôleur de gestion de réseau, 5600 W, 230 V, matériel et électricien requis, autonomie de 93 à 134 min	1			1
Serveur de personnalisation	Clavier du serveur	Clavier Dell QWERTY sur bâti	1			1
Serveur de personnalisation	Écran sur bâti	Écran ACL Dell de 17 po avec fixation	1			1
Serveur de personnalisation	Unité de distribution de l'alimentation	Unité d'alimentation Dell	1			1
Serveur de personnalisation	Câble réseau	Câble d'alimentation APC	28			28
Serveur de personnalisation	Câble réseau	Câble réseau Belkin RJ-45 de catégorie 5	28			28
Serveur de personnalisation	Câble réseau	Câble réseau Belkin RJ-45 de catégorie 6	28			28
Serveur de personnalisation	Licence CPS (Continuous Protection Server)	Configuration, documentation incluse	1			1
Serveur de personnalisation	SOUS-TOTAL					
Serveur central	Administration des bases de données du serveur - Production	Cartes à processeur	1			1
Serveur central	Bâti	Boîtier sur bâti 42U pour serveurs Dell PowerEdge 4220 avec portes et panneaux latéraux, configuration standard	1			1
Serveur central	Serveur FTP et serveurs d'émission et de collecte	Serveur Dell PowerEdge à quatre cœurs R200 avec processeur Xeon X3330 (2,66 GHz, 2 x 3 Mo, bus frontal cadencé à 1333 MHz, TDP de 96 W) ou équivalent	1			1
Serveur central	Serveur de domaine	Active Directory des cartes à processeur - Surveillance - Serveur de mise à jour de l'antivirus	1			1
Serveur central	Système de stockage LTO	Dell PowerVault 124T LTO4	1			1
Serveur central	Bandes LTO	Bandes de type LTO4	24			24
Serveur central	Sauvegarde	Logiciel Symantec Backup Exec et contrôleur matériel pour la gestion du système de sauvegarde sur bandes	1			1
Serveur central	ASC sur bâti	ASC sur bâti 4U Dell pour serveurs PowerEdge 4220 avec contrôleur de gestion de réseau, 5600 W, 230 V, matériel et électricien requis, autonomie de 93 à 134 min	1			1
Serveur central	Clavier du serveur	Clavier Dell QWERTY sur bâti	1			1
Serveur central	Écran sur bâti	Écran ACL Dell de 17 po avec fixation	1			1
Serveur central	Unité de distribution de l'alimentation	Unité d'alimentation Dell	1			1
Serveur central	Câble réseau	Câble d'alimentation APC	28			28
Serveur central	Câble réseau	Câble réseau Belkin RJ-45 de catégorie 5	28			28
Serveur central	Câble réseau	Câble réseau Belkin RJ-45 de catégorie 6	28			28
Serveur central	SOUS-TOTAL					
Serveur d'inscription et de livraison	Entièrement centralisé / matériel	Serveur DELL R610, processeur Intel XEON, 12 Go de mémoire vive, logiciel Win Server 2008 R2, contrôleurs RAID, DD 250	1	1		2
Serveur d'inscription et de livraison	Entièrement centralisé / matériel	Dell PowerVault MD1220, capacité de stockage de 9 To	1	1		2
Serveur d'inscription et de livraison	Entièrement centralisé / matériel	Unité de sauvegarde sur bandes Dell PowerVault 124T LTO4, demi-hauteur	1	1		2
Serveur d'inscription et de livraison	Entièrement centralisé / matériel	Routeur et pare-feu	1	1		2
Serveur d'inscription et de livraison	Entièrement centralisé / matériel	Bâti du serveur	1			1
Serveur d'inscription et de livraison						
TOTAL GÉNÉRAL						

## Options de renouvellement de la carte

Des cartes d'identité imprimées ordinaires, dotées d'une date d'expiration, ne peuvent être renouvelées à moins de les réimprimer au complet. Il est courant de conserver les données dans un fichier pour une utilisation future afin que, à l'expiration, une nouvelle carte puisse être imprimée et postée au détenteur. Différentes politiques visant la durée des photos existent, mais habituellement une photo datant de plus de cinq ans n'est pas jugée valable pour une photo d'identité. Avec la technologie de la puce, il existe d'autres façons d'authentifier la carte dans cet écosystème (pas exclusivement avec la photo), on peut donc considérer une durée de vie plus longue pour la photo.

Le processus de renouvellement de la carte dépendra des politiques du programme :

- Devons-nous renouveler la photo tous les cinq ans?
- Avons-nous besoin d'information provenant d'autres sources ou bases de données pour vérifier la prolongation de la validité de la carte?
- Allons-nous émettre une carte à vie et puis, la remplacer si elle est perdue ou endommagée?
- Quels autres systèmes ou services utilisent cette carte et comment un renouvellement de carte aura-t-il des incidences sur ces systèmes?

Dans le modèle d'émission répartie, les détenteurs de cartes se rendraient au bureau le plus près et soumettraient une nouvelle photo, après quoi ils recevraient leur nouvelle carte sur place.

Dans le modèle d'émission centralisée, le détenteur de la carte pourrait faire une demande en téléchargeant une photo vers un site Web centralisé et une nouvelle carte pourrait lui être envoyée par la poste une fois que la demande serait terminée.

## **Aspects liés à la sécurité et à la protection des renseignements personnels**

Les aspects liés à la protection des renseignements personnels sont régis par les politiques en vigueur et les futures politiques de l'organisme et ils peuvent dépendre de la province de résidence du détenteur. Il existe une politique fédérale sur la protection des renseignements personnels, mais les politiques provinciales ont préséance sur les politiques fédérales si la province s'est dotée de telles politiques.

Habituellement, pourvu que le détenteur soit informé de l'utilisation prévue des renseignements personnels, il est possible de recueillir presque n'importe quel type de renseignements. Le détenteur de la carte doit être informé et être un partenaire consentant de l'échange d'information. On recommande que le ministère des Anciens Combattants obtienne des avis juridiques à cet égard.

En règle générale, il faut seulement recueillir et stocker l'information qui sera utilisée. S'il n'est pas nécessaire de prendre les empreintes digitales, nous recommandons de ne pas le faire. De même, si la photo n'est pas utile, il n'est pas nécessaire de la prendre. (Les coûts sont ainsi considérablement réduits, car les postes de prise de photos peuvent être éliminés.)

### **Incidences d'une falsification de la carte**

Plusieurs aspects doivent être examinés selon les deux principaux types de cartes examinés précédemment (la carte d'identité ordinaire et la carte à puce électronique) :

#### ***Carte d'identité ordinaire***

Même si la carte d'identité contient des renseignements personnels sur sa surface, elle demeure la propriété du détenteur. Il incombe donc au détenteur de protéger sa carte contre une perte. La perte d'une seule carte ne touche qu'un seul détenteur de carte. Il est important d'incorporer dans les cartes imprimées une technologie anti-falsification qui permet de détecter toute tentative de reproduction.

**Carte à puce**

La carte à puce contient des données électroniques et souvent, de l'information imprimée à la surface. Cependant, les données sont stockées de façon à empêcher leur extraction et leur destruction. Les données ne peuvent être récupérées, copiées, reproduites ni modifiées. Dans le cas extrêmement improbable que cela se produise, seules les données stockées dans la carte falsifiée ont été compromises et l'intégrité de l'ensemble du programme d'identification n'a pas été touchée.

**Effet d'une intrusion dans le système**

Une intrusion dans le système est beaucoup plus grave. La totalité de la base de données des détenteurs de cartes peut être compromise. Il est donc important que les politiques applicables et les protocoles connus en matière de TI soient respectés.

## Établissement des coûts

### Hypothèses liées au projet

<b>Généralités</b>	
Durée du projet	3 ans
Nombre de jours ouvrables/an	250 jours
Nombre de jours ouvrables/mois	20 jours
Nombre d'heures ouvrables/jour	8 heures
<b>Inscription</b>	
Nombre de personnes à inscrire	1 000 000
Durée de l'inscription	12 mois
Durée de l'inscription	240 jours
<b>Collecte des données</b>	
Nombre de sites de collecte des données	33
Nombre d'équipes au site de collecte des données	1
Site de collecte – quantité traitée par année (moyenne)	30 303 cartes
Site de collecte – quantité traitée par jour (moyenne)	121
<b>Personnalisation</b>	
Nombre de sites de personnalisation (Ottawa)	1
Nombre d'équipes au site de personnalisation	2
Site de personnalisation, quantité de cartes produites par année	1 000 000
Site de personnalisation, quantité de cartes produites par jour	4 000

## Éléments livrables du projet

<b>Sommaire</b>	
Nombre de détenteurs : 1 000 000	
Cartes en PET-F (polyester) avec caractéristiques de sécurité perfectionnées	
Personnalisation (vérification, contrôle de la qualité, gestion des stocks)	
Système centralisé (serveur et matériel pour l'administration)	
Articles consommables (rubans, matériaux d'emballage, etc.)	
Frais de mise en œuvre (gestion de projet et logiciel)	
Maintenance (frais annuels)	
Coûts de transport et de livraison	
<b>Cartes et prix du système de personnalisation par carte</b>	<b>Est. 4,50 \$ CAN</b>
<b>Cartes à puce, prix du système de personnalisation par carte</b>	<b>Est. 5,20 \$ CAN</b>

Nota : Les cartes à puce sont des cartes en polycarbonate intégrant une puce à contact avec une fonctionnalité d'authentification très efficace. Cette fonctionnalité n'exige pas d'infrastructure complexe (lecteurs, réseau, serveurs, ICP et politiques) pour le processus d'authentification. Le coût de production de la carte sera le seul coût dont il faut tenir compte.

<b>Coût des postes d'inscription, 33 emplacements</b>	
Matériel et logiciels nécessaires pour l'inscription, acheminement des données au site centralisé	
Déploiement, gestion de projet et développement	
Maintenance, transport et livraison	
<b>Sous-total pour les postes d'inscription</b>	<b>1 488 000 \$</b>

## **Calendrier de mise en œuvre du projet**

Pour émettre un million de cartes dans le cadre d'un programme d'émission centralisée, il faudrait environ 237 jours ouvrables selon notre estimation. La production des cartes selon un modèle d'émission répartie prendrait un peu plus de temps, car il faudrait doter chaque poste d'une imprimante de cartes et former le personnel pour l'utiliser. De plus, ce serait plus long de produire ce grand volume de cartes initiales.

Par exemple, si nous supposons de faire appel à la solution d'émission centralisée à compter du 6 août 2012, les dernières cartes du million de cartes initiales à imprimer seraient livrées au début de juillet 2013.

À titre d'information, voici un exemple de plan de projet ventilé dans ses moindres détails avec des dates d'échéance et des délais.

<b>CAN --- Projet de cartes d'identité pour les AC</b>	<b>JOURS</b>	<b>DATE DU DÉBUT</b>	<b>DATE DE FIN</b>	<b>INTERVENANTS</b>
<b>LANCEMENT</b>	<b>29 jours</b>	<b>6-août-12</b>	<b>13-sept-12</b>	
Commande d'achat	1 jour	6-août-12	6-août-12	Gouvernement CAN (CAN)
Réunion interne de lancement	1 jour	7-août-12	7-août-12 4	OTC YML; OT LTS/GTS/PD/PROC/PM
Signature du contrat + versement initial	20 jours	7-août-12	3-sept-12 4	CAN; OT Ventas
Commande des logiciels	1 jour	13-sept-12	13-sept-12 12	OT PD
Préparation du plan du projet	10 jours	8-août-12	21-août-12 5	CAN; Fourn. inscriptions (Inscr); DTC, OT
Atelier pour faire la liste exhaustive des besoins	5 jours	22-août-12	28-août-12 8	CAN; Inscrip; OT GTS/LTS/PM
Achèvement du plan du projet	6,67 jours	29-août-12	6-sept-12 9	CAN; Inscrip, OT,DTC
Réunion de lancement	3,33 jours	6-sept-12	11-sept-12 10	CAN; Inscrip, OT,DTC
Signature du plan du projet	1 jour	12-sept-12	12-sept-12 11	CAN; Inscrip, OT
<b>PLANIFICATION</b>	<b>46 jours</b>	<b>13-sept-12</b>	<b>15-nov-12</b>	
<b>SPÉCIFICATIONS TECHNIQUES ET FONCTIONNELLES</b>	<b>46 jours</b>	<b>13-sept-12</b>	<b>15-nov-12</b>	
Livraison des matières premières pour l'épreuve en bon à tirer	25 jours	13-sept-12	17-oct-12 12	OT PD
Épreuve en bon à tirer/fabrication de la MTE	20 jours	18-oct-12	14-nov-12 17	OT R et D
Épreuve en bon à tirer/approbation de la MTE	1 jour	15-nov-12	15-nov-12 18	CAN, OTLTS/PM
Rédaction des spécifications techniques et fonctionnelles	30 jours	13-sept-12	24-oct-12 12	Inscrip; OT GTS/LTS,DTC
Approbation	5 jours	25-oct-12	31-oct-12 20	CAN; OT LTS/PM
Environnement de développement et qualification	2 jours	1-nov-12	2-nov-12 21	OT GTS/ R et D, Inscrip, DTC
<b>EXÉCUTION</b>	<b>162 jours</b>	<b>1-nov-12</b>	<b>14-juin-13</b>	
<b>ÉLABORATION D'UN DOC. D'ACHAT POUR LOGICIELS ET MATÉRIEL</b>	<b>68 jours</b>	<b>1-nov-12</b>	<b>4-févr-13</b>	
Commande du matériel	3 jours	1-nov-12	5-nov-12 21	Inscrip, OT PD
Fabrication du matériel	65 jours	6-nov-12	4-févr-13 27	Inscrip, OT PD, DTC
Développement de la solution logicielle	66 jours	5-nov-12	4-févr-13 22	OT GTS/ R et D, Inscrip
<b>FABRICATION DES CARTES</b>	<b>130 jours</b>	<b>16-nov-12</b>	<b>16-mai-13</b>	
Commandes et livraison des matières premières	45 jours	16-nov-12	17-janv-13 19	OT PROC et PD
Fabrication et livraison des échantillons à des fins de développement et qualification	15 jours	18-janv-13	7-févr-13 32	OT Prod
Fabrication de 500 000 cartes	35 jours	8-févr-13	28-mars-13 33	Inscrip,OT PD,DTC
Fabrication de 500 000 cartes	35 jours	29-mars-13	16-mai-13 34	OT GTS/ R et D, Inscrip
<b>ESSAIS D'ACCEPTATION</b>	<b>15 jours</b>	<b>5-févr-13</b>	<b>25-févr-13</b>	
Mise en œuvre de la plate-forme EAF aux USA ou en FR	2 jours	5-févr-13	6-févr-13 29	Inscrip; DTC; OT GTS/LTS
Essais d'acceptation fonctionnelle (EAF) interne	1 jour	8-févr-13	8-févr-13 38,33	Inscrip; OT LTS/GTS
Modifications	10 jours	11-févr-13	22-févr-13 39	Inscrip, OT GTS
EAF avec client final	1 jour	25-févr-13	25-févr-13 40	CAN; Inscrip; OT LTS/PM
<b>ENVOI</b>	<b>79 jours</b>	<b>26-févr-13</b>	<b>14-juin-13</b>	
Confirmation que le local d'entreposage du matériel est prêt	1 jour	26-févr-13	26-févr-13 41	CAN
Envoi du matériel	15 jours	27-févr-13	19-mars-13 44	Inscrip, OT PD/Logistique
Dédouanement	5 jours	20-mars-13	26-mars-13 45	CAN
Transport depuis les douanes jusqu'à la chambre forte du client	1 jour	27-mars-13	27-mars-13 46	CAN
Confirmation de la réception du matériel	0 jours	27-mars-13	27-mars-13 47	CAN
Envoi des cartes	15 jours	29-mars-13	18-avr-13 34	OT Logistique / CS
Dédouanement	5 jours	19-avr-13	25-avr-13 49	CAN
Transport depuis les douanes jusqu'à la chambre forte du client	1 jour	26-avr-13	26-avr-13 50	CAN
Confirmation de la réception	0 jours	26-avr-13	26-avr-13 51	CAN
Envois des cartes	15 jours	17-May-13	6-juin-13 35	OT Logistique /CS
Dédouanement	5 jours	7-juin-13	13-juin-13 53	CAN
Transport depuis les douanes jusqu'à la chambre forte du client	1 jour	14-juin-13	14-juin-13 54	CAN
Confirmation de la réception	0 jours	14-juin-13	14-juin-13 55	CAN
<b>MISE EN ŒUVRE SUR PLACE</b>	<b>49 jours</b>	<b>28-mars-13</b>	<b>4-juin-13</b>	

<b>SITE CENTRALISÉ</b>	<b>16 jours</b>	<b>28-mars-13</b>	<b>18-avr-13</b>	
Mise en œuvre sur place --- serveurs	5 jours	28-mars-13	3-avr-13 48	Inscrip; OT GTS/LTS
Mise en œuvre sur place --- ligne personnelle	5 jours	4-avr-13	10-avr-13 61	OT GTS/LTS
Mise en œuvre sur place --- serveurs centr d'inscrip	5 jours	28-mars-13	3-avr-13 48	Inscrip; OT GTS
Formation des utilisateurs	3 jours	11-avr-13	15-avr-13 62	Inscrip; OT LTS
Formation des administrateurs	2 jours	16-avr-13	17-avr-13 64	Inscrip; OT GTS
Transfert automatique protégé (TAP)	1 jour	18-avr-13	18-avr-13 65	CAN; Inscrip; OT LTS/PM
<b>SITES DÉCENTRALISÉS</b>	<b>33 jours</b>	<b>19-avr-13</b>	<b>4-juin-13</b>	
Mise en œuvre sur place de 99 postes d'inscription	33 jours	19-avr-13	4-juin-13 66	Inscrip; OT GTS/LTS
Formation des utilisateurs	33 jours	19-avr-13	4-juin-13 66	Inscrip; OT LTS
Sites de saisie TAP	33 jours	19-avr-13	4-juin-13 66	Inscrip; OT LTS/PM
Aide au démarrage	33 jours	19-avr-13	4-juin-13 66	Inscrip; OT LTS
<b>CLÔTURE DU PROJET</b>	<b>20 jours</b>	<b>5-juin-13</b>	<b>2-juil-13</b>	
Collecte des rapports d'analyse et des rapports de fin de projet auprès des principaux membres de l'équipe	10 jours	5-juin-13	18-juin-13 72	OT, OT PM, Inscrip, DTC
Rapports de fin de projet	5 jours	19-juin-13	25-juin-13 75	OT PM
Archivage et leçons apprises ABD	5 jours	26-juin-13	2-juil-13 76	OT PM



