GROUPE CONSULTATIF TECHNIQUE SUR LES DOCUMENTS DE VOYAGE LISIBLES À LA MACHINE

QUINZIÈME RÉUNION

Montréal, 17 – 21 mai 2004

Point 2 : Rapport du Groupe de travail sur le contenu et la forme des documents (DCFWG)
2.1 : Progrès réalisés dans la mise à jour du Doc 9303 et amendements proposés

INDICATEUR DE PASSEPORT ÉLECTRONIQUE — NUMÉRO DE VERSION ET NOUVEAU SYSTÈME À CARACTÈRES DE CONTRÔLE DANS LES DOCUMENTS DE VOYAGE LISIBLES À LA MACHINE

(Note présentée par le Groupe de travail sur le contenu et la forme des documents [DCFWG])

1. INTRODUCTION

1.1 La présente note donne suite à la demande du Groupe de travail des technologies nouvelles (NTWG) de trouver un moyen d'incorporer dans la zone de lecture automatique (ZLA) un indicateur signalant la présence d'un circuit intégré (CI) sans contact dans le document de voyage. Ce type de document de voyage à puce sans contact est appelé ci-après «passeport électronique», dont le passeport lisible à la machine (MRP) à CI sans contact est le premier exemple.

2. RÉSUMÉ

2.1 L'addition d'un indicateur de passeport électronique dans la ZLA soulève un grave problème de rétrocompatibilité avec l'équipement et les systèmes de lecture installés aux postes de contrôle frontalier. Quelle que soit la méthode adoptée, il y aura des difficultés. La présente note examine la question et propose une solution qui, sans permettre une rétrocompatibilité totale, conserve la structure fondamentale de la ZLA. La solution offre l'avantage supplémentaire d'améliorer considérablement l'utilité immédiate et à long terme de la ZLA. Les principes en cause ont été examinés à la réunion du DCFWG (Basingstoke, 8 – 10 mars 2004) et affinés dans le cadre d'un échange soutenu de courrier électronique.

3. PRINCIPES

3.1 Le passeport électronique est un MRP classique, décrit essentiellement dans le Doc 9303, qui offre une capacité accrue sous forme de puce sans contact pour le stockage de données facultatives.

3.2 La puce sans contact contient un ou plusieurs renseignements biométriques et une signature numérique (infrastructure à clés publiques [ICP]) encodés en fonction de la structure de données logiques (SDL). Les renseignements biométriques permettent de lier le passeport électronique à son titulaire, tandis que la signature numérique protège le document contre la falsification et l'altération. Il s'agit là de deux moyens effectifs qui rendent la falsification et la fraude beaucoup plus difficiles, voire impossibles.

3.3 Pour empêcher la lecture non autorisée, plusieurs pays émetteurs ont proposé une protection facultative de la puce par mot de passe. Le mot de passe doit être extrait de la ZLA au moyen d'une lecture par reconnaissance optique de caractère (ROC) classique. Il s'agit de la technique dite «à accès fermé» (par opposition aux puces non verrouillées, «à accès ouvert», sans mot de passe). La lisibilité ROC est un facteur critique à cet égard.

4. QUESTIONS POSÉES PAR LE DCFWG

4.1 Comment pourra-t-on confirmer la présence de la puce durant le processus de lecture automatique? On pourrait apposer un symbole lisible à l'œil nu sur la couverture et la page de données du passeport, mais il ne sera probablement pas reconnu par un lecteur automatique. Le NTWG a demandé au DCFWG d'étudier la possibilité de modifier la ZLA pour permettre cette fonction. Il est à noter que l'on ne pourra pas compter sur la puce pour une telle vérification, car elle risque d'être ineffective ou verrouillée («à accès fermé»).

4.2 Comment peut-on renforcer la précision et la fiabilité du processus de lecture de la ZLA? La technique de l'«accès fermé» est facultative, mais si un grand nombre de pays l'adoptaient, les pays récepteurs devraient utiliser un lecteur pour extraire de la ZLA du passeport électronique une clé permettant de déverrouiller la puce. Si, comme il a été signalé, le taux d'erreur de lecture automatique est élevé dans certains pays, c'est la facilitation qui en pâtira car il faudra alors revenir aux méthodes manuelles pour compenser le taux d'erreur.

5. PROPOSITION DU DCFWG — NUMÉRO DE VERSION ET NOUVEAU SYSTÈME À CARACTÈRES DE CONTRÔLE

5.1 Le DCFWG propose l'adoption obligatoire d'un nouveau système à caractères de contrôle pour la ZLA et d'un numéro de version pour :

a) identifier le MRP comme étant un passeport électronique;

b) surmonter les limitations de l'actuel système à chiffre de contrôle;

c) accroître la sûreté de la lecture par ROC;

d) permettre des améliorations futures de la ZLA en numérotant les versions par un identificateur.

5.2 Il y aurait lieu de noter que toute modification de la ZLA, mineure (un caractère) ou majeure (plusieurs caractères), aura le même grave effet perturbateur sur tous les lecteurs automatiques et systèmes de traitement existant dans le monde. Par contre, pour les pays mettant en œuvre le passeport électronique, l'effort investi dans la modification des procédés d'impression et de lecture de la ZLA est minime par rapport à celui qu'exigent le cryptage et la lecture de la puce sans contact.

5.3 L'objectif est donc de causer le moins de perturbation possible et de conserver un certain degré de compatibilité amont, en particulier pour les pays qui projettent de conserver leurs installations de lecture automatique actuelles, et qui ne prévoient donc pas la lecture de passeports électroniques, sauf pour la ZLA, comme auparavant.

5.4 Le DCFWG a examiné et rejeté deux premières options :

a) utiliser la combinaison «PE» au début de la première ligne de lecture automatique (et d'autres combinaisons pour les visas et les documents de voyage officiels lisibles par machine, p. ex. «VE» et «IE», respectivement). Cette option offre l'avantage de préserver les systèmes d'impression, de lecture et de traitement en place. Par contre, elle présente les graves inconvénients suivants :

   1) elle élimine la possibilité d'utiliser la deuxième lettre pour indiquer le type de passeport (p. ex. «PD» pour «diplomatique»);

   2) elle serait une grande source de confusion, certains pays utilisant déjà la combinaison «PE» pour les MRP classiques;

b) remplacer le «P» initial figurant au début de la première ligne de lecture automatique par la lettre «E» (et les autres combinaisons de lettres utilisées pour les visas et les documents de voyage officiels lisibles par machine). La seconde lettre peut alors conserver sa signification actuelle; par exemple, «ED» pourrait servir à indiquer un passeport électronique diplomatique. Par contre, cette option présente les inconvénients suivants :

   1) tous les lecteurs et systèmes de traitement actuels devront être modifiés, et il n'y a aucune possibilité de rétrocompatibilité. Cette option causerait un maximum de perturbation sans autre avantage que d'identifier les passeports électroniques;

   2) l'utilisation d'un seul caractère pour signaler la présence de la puce est considéré comme peu sûre, car les falsificateurs, cherchant à empêcher la détection de la puce, vont s'attaquer à ce caractère et essayer de le modifier pour indiquer un passeport standard («P»).

5.5 Devant la possibilité d'une perturbation majeure des systèmes de lecture et de traitement à l'échelle du monde, d'autres solutions ont été étudiées qui :

   1) auraient un effet perturbateur moindre;

   2) permettraient une compatibilité en amont;

   3) amélioreraient les performances en matière de lisibilité ROC-B.

5.6 Il existe une troisième, et meilleure option, qui consiste à utiliser les cinq dernières positions du champ du nom pour un nouveau système à caractères de contrôle et un numéro de version. Cette solution prévoit de raccourcir le champ du nom de cinq caractères. Par ailleurs, il serait également souhaitable de raccourcir davantage ce champ de trois autres caractères et d'y insérer trois séparateurs («<<<»), pour établir clairement la démarcation entre le champ nominatif réduit et le nouveau champ des caractères de contrôle et du numéro de version.

5.7 Le numéro de version a pour objet :

1) d'identifier le MRP comme étant un passeport électronique;

2) de permettre des modifications ultérieures, s'il y a lieu.

Le premier numéro de version de tous les passeports électroniques serait le numéro 1, figurant à la position 42 de la ligne supérieure de lecture automatique.

5.8 Les caractères de contrôle ont pour objet :

1) d'améliorer la lisibilité ROC;

2) de contribuer à l'identification du MRP comme un passeport électronique, ce qui supprime le recours à un seul caractère pour ce processus.

Il existe d'autres méthodes possibles de contrôle simples mais efficaces du point de vue numérique, qui utilisent quatre caractères de contrôle (A à Z, 0 à 9 et <) et offrent une capacité maximale de détection et de redressement d'erreur pour 88 caractères. Le nouveau système à caractères de contrôle améliore la précision de la lecture de la ZLA car il porte sur toutes les données figurant dans cette zone et non pas seulement sur celles qui figurent dans certains champs, comme c'est le cas actuellement.

5.9 L'algorithme proposé fonctionne comme suit :

a) chaque caractère est mis en correspondance avec un nombre (p. ex. 0 à 9 = 0 à 9; A = 10, B = 11, etc., jusqu'à Z = 35; et < = 36);

b) tous les champs de données sont disposés selon la séquence définie (p. ex. type, pays émetteur, nom, numéro de version, numéro du document, etc.), y compris les chiffres de contrôle avec pondération 7-3-1 actuels. On obtient ainsi une rangée de 84 caractères dans le cas du MRP (étant donné qu'il faut enlever les quatre nouveaux caractères de contrôle du total de 88 caractères présents sur les deux lignes);

c) le caractère de contrôle n° 1 (CC1) est alors calculé en additionnant toutes les valeurs numériques correspondant aux 85 caractères particuliers. Le résultat est divisé itérativement par 37 tant que le reste issu de la division est supérieur à 37; le reste final constitue le CC1;

d) le CC2 est calculé de la même manière; pour l'addition, la valeur de chaque caractère est multipliée par le chiffre correspondant à sa position dans la rangée;

e) le CC3 est calculé de la même manière; pour l'addition, les valeurs des 37 premiers caractères de la rangée sont multipliées par 1, celles des 37 caractères suivants, par 2, et celles des caractères restants, par 3;

f) le CC4 est calculé comme suit [à annoncer];

g) les caractères de contrôle (CC1, CC2, CC3 et CC4) correspondront à un nombre compris entre 0 et 36, et chacun pourra à son tour être représenté par un caractère unique qui figurera à leur position respective dans la ZLA (positions 40, 41, 43 et 44 de la ligne supérieure de lecture automatique);

h) le numéro de version est placé à la position 42 de la ligne supérieure de lecture automatique pour séparer les caractères de contrôle en deux paires de caractères, ce qui permet d'éviter la formation d'un mot «grossier» dans quelque langue que ce soit.

5.10 Le nouveau système à caractères de contrôle couvre l'ensemble de la ZLA et non pas seulement des champs particuliers, comme c'est le cas avec le système actuel à chiffres de contrôle avec pondération 7-3-1. Le champ du nom et les autres champs de données qui ne sont actuellement pas contrôlés le seront avec le nouveau système. Grâce à la fonction mathématique, ces caractères de contrôle peuvent identifier jusqu'à trois erreurs si les positions de ces erreurs ne sont pas connues, et corriger l'erreur si une seule position de caractère est corrompue. Si les positions des erreurs sont connues, deux erreurs peuvent être corrigées. Il est à noter que les chiffres de contrôle utilisés auparavant ne concernent que leurs champs respectifs (numéro de document, date de naissance, date d'expiration et champ de données facultatives) et qu'ils permettent normalement de détecter des erreurs, encore que parfois, deux ou plusieurs erreurs peuvent s'annuler l'une l'autre et ne pas être détectées. La correction d'erreur n'est possible que dans certaines circonstances. D'une façon générale, le système actuel à chiffres de contrôle avec pondération 7-3-1 est inefficace, mais il a été adopté en partie parce qu'il peut être calculé manuellement. Le nouveau système à caractères de contrôle est plus puissant et peut lui aussi se prêter à un calcul manuel, mais l'opération sera plutôt longue.

5.11 L'essentiel de cette troisième option est que la présence du numéro de version et la vérification par des caractères de contrôle indiqueront que le MRP est un passeport électronique. Les chiffres de contrôle avec pondération 7-3-1 aux positions 10, 20, 28, 43 et 44 de la ligne inférieure de lecture automatique sont conservés pour assurer un maximum de compatibilité amont.

5.12 Le nouveau système à caractères de contrôle améliorera considérablement la lecture par ROC-B. Cette caractéristique est vitale pour une lecture fiable de la ZLA afin d'obtenir une «clé» ou un «mot de passe» permettant de déverrouiller une puce sans contact «à accès fermé».

5.13 La troisième option est considérée comme offrant la plus grande rétrocompatibilité parmi toutes les options étudiées. Les pays récepteurs équipés de lecteurs automatiques et de systèmes de traitement traditionnels pourront encore lire la ZLA des passeports électroniques. Par contre, les nouveaux caractères figurant à la fin du champ nominatif risquent d'être considérés comme faisant partie du nom, ce qui empêchera une vérification auprès des bases de données. L'emploi de trois séparateurs («<<<») entre le champ nominatif et le nouveau champ permettra, dans la plupart des cas, de contourner ce problème. Il faudrait inviter instamment les pays à mettre à niveau leurs dispositifs et systèmes de lecture automatique traditionnels en les reprogrammant ou en les remplaçant pour pouvoir tirer parti du nouveau système.

5.14 Les pays qui mettent à niveau leurs dispositifs ou systèmes de lecture automatique ou qui en installent de nouveaux pourront lire les deux types de documents de voyage (à savoir le MRP traditionnel et le passeport électronique). L'adoption du nouveau système à caractères de contrôle et du champ nominatif réduit correspond essentiellement à une reprogrammation. Une telle mesure ne représente qu'une faible part des efforts nécessaires à la mise en œuvre de la lecture des CI sans contact.

5.15 À l'issue des délibérations de la réunion du DCFWG, une solution de rechange similaire a été proposée et rejetée. Elle consistait à utiliser le numéro de version et le nouveau système à caractères de contrôle en remplacement de l'actuel système à chiffres de contrôle avec pondération 7-3-1. Le numéro de version serait une lettre (initialement, la lettre «A») qui remplacerait le chiffre de contrôle global à la position 44 de la ligne inférieure de lecture automatique. Les nouveaux caractères de contrôle remplaceraient les chiffres de contrôle actuels aux positions 10, 20, 28 et 43 de la ligne inférieure de lecture automatique. Cette solution a été rejetée pour les raisons suivantes :

a) risque accru d'erreur de lecture avec les lecteurs actuels, le système à chiffres de contrôle n'étant plus effectif, et les passeports électroniques seraient probablement signalés comme étant des faux;

b) disparition d'un outil précieux pour la détection des passeports falsifiés, les agents d'inspection ne pouvant plus calculer manuellement les chiffres de contrôle. Dans les passeports falsifiés, ces chiffres sont souvent erronés. Les nouveaux caractères de contrôle offrent le même moyen de détection, mais le nouvel algorithme est beaucoup plus difficile à calculer manuellement.

5.16 Il y a lieu de noter que le champ de données facultatives de la ZLA (positions 29 à 43 de la ligne inférieure de lecture automatique) ne peut être utilisé pour les caractères de contrôle et le numéro de version, car de nombreux États émetteurs utilisent ce champ à d'autres fins.

6. SUITE À DONNER PAR LE TAG-MRTD

6.1 Le DCFWG invite le TAG-MRTD :

a) à prendre note des travaux et de l'approche du DCFWG concernant l'identification des passeports électroniques au moyen de la ZLA, ainsi que du nouveau système à caractères de contrôle proposé pour la ZLA;

b) à recommander l'approbation de l'approche et des travaux effectués jusqu'ici par le DCFWG et à approuver l'élaboration de spécifications techniques plus précises, aux fins d'inclusion dans le Doc 9303.

— FIN —