

GRUPO TÉCNICO ASESOR SOBRE LOS DOCUMENTOS DE VIAJE DE LECTURA MECÁNICA

Decimoquinta reunión

(Montreal, 17 - 21 de mayo de 2004)

**Cuestión 2 del Informe del Grupo de trabajo sobre contenido y formato
orden del día: de documentos (DCFWG)
2.1: Progresos en la actualización del Doc 9303 y propuestas de enmienda**

INDICADOR “Pasaporte-e” — NÚMERO DE VERSIÓN Y NUEVO ESQUEMA DE CARACTERES DE VERIFICACIÓN EN LOS DOCUMENTOS DE VIAJE DE LECTURA MECÁNICA

[Nota presentada por el Grupo de trabajo sobre contenido y formato de documentos (DCFWG)]

1. INTRODUCCIÓN

1.1 La presente nota se preparó a pedido del Grupo de trabajo sobre nuevas tecnologías (NTWG) para encontrar una manera de incorporar en la zona de lectura mecánica (ZLM) un indicador de que el documento de viaje contiene un CI sin contacto. En la presente nota, este tipo de documento de viaje se denomina (“Pasaporte-e”) “Pasaporte electrónico”, puesto que el pasaporte de lectura mecánica (PLM) con CI sin contacto constituye el primer ejemplo de esta tecnología.

2. RESUMEN

2.1 La incorporación de un indicador de Pasaporte-e en la ZLM presenta un serio problema de compatibilidad con los equipos y sistemas de lectura mecánica instalados en los puestos de control fronterizos. Cualquiera sea el método que se adopte, habrá dificultades. En la presente nota se analiza ese problema. Se propone una solución que, si bien no es totalmente compatible con la tecnología anterior, conserva la estructura esencial de la ZLM. La solución tiene el mérito adicional de que mejora considerablemente la facilidad de uso inmediato y de largo plazo de la ZLM. Estos conceptos se analizaron en la reunión del DCFWG (Basingstoke, 8 al 10 de marzo de 2004) y se perfeccionaron luego mediante intensos intercambios por correo electrónico.

3. CONCEPTOS

3.1 El Pasaporte-e es el PLM tradicional, como se describe en el Doc 9303, con añadido de tecnología de ampliación de capacidad opcional en forma de microprocesador sin contacto.

3.2 El microprocesador sin contacto contiene uno o más datos de biometría y una firma digital (Infraestructura de clave pública – ICP), codificados mediante la estructura lógica de datos (LDS). El empleo de la biometría permite vincular al Pasaporte-e con su titular y la firma digital impide la

adulteración y falsificación del documento. Esos son dos conceptos importantes que hacen que la falsificación y el fraude sean considerablemente más difíciles, si no imposibles.

3.3 Para combatir la lectura no autorizada, varios países expedidores han propuesto la protección opcional del microprocesador mediante una contraseña. La contraseña se obtiene de la ZLM mediante la lectura tradicional por reconocimiento óptico de caracteres (OCR). Esto se conoce como “acceso cerrado” (a diferencia de los microprocesadores no bloqueados, que tendrían un “acceso abierto” y no requerirían el uso de una contraseña). La capacidad de lectura mediante OCR es una cuestión crítica en este sentido.

4. PREGUNTAS FORMULADAS POR EL DCFWG

4.1 ¿Cómo puede comprobarse la presencia del microprocesador durante el proceso de lectura mecánica? Si bien la cubierta y la página de datos del pasaporte pueden marcarse con un logo legible para el ojo humano, generalmente un dispositivo de lectura mecánica no puede reconocerlo. El NTWG encargó al DCFWG que considerara la posibilidad de efectuar un cambio apropiado en la ZLM para lograr esa función. Cabe señalar que no se puede confiar en que el microprocesador realice esa función por sí solo, ya que puede estar desactivado o bloqueado (con “acceso cerrado”).

4.2 ¿Cómo puede hacerse más preciso y confiable el proceso de lectura de la ZLM? Aunque sea opcional, si numerosos países adoptan el “acceso cerrado”, los países receptores tendrán que leer la ZLM del Pasaporte-e mediante dispositivos de lectura mecánica para obtener una clave que permita desbloquear el microprocesador cerrado. Si, como se ha informado, la tasa de error en la lectura mecánica es alta en algunos países, esto afectará la facilitación, ya que debe utilizarse el ingreso manual de datos para compensar esa tasa de error.

5. PROPUESTA DEL DCFWG — NÚMERO DE VERSIÓN Y NUEVO ESQUEMA DE CARACTERES DE VERIFICACIÓN

5.1 El DCGWG propone la adopción obligatoria de un nuevo esquema de caracteres de verificación para la ZLM y un nuevo número de versión, que permitan:

- a) identificar al PLM como Pasaporte-e;
- b) superar las limitaciones del esquema actual de dígitos de verificación;
- c) hacer que la lectura mediante OCR sea más segura; y
- d) sentar las bases para mejoras futuras de la ZLM mediante la introducción de un identificador de versión.

5.2 Cabe señalar que toda modificación de la ZLM, ya sea menor (un carácter) o sustancial (numerosos caracteres), tendrá el mismo efecto, es decir una grave perturbación para los actuales dispositivos de lectura mecánica y sistemas de procesamiento en todo el mundo. No obstante, para los países que introduzcan el uso de Pasaportes-e, el esfuerzo de modificar la impresión y lectura de la ZLM es ínfimo comparado con el esfuerzo que requiere la codificación y lectura del microprocesador sin contacto.

5.3 El objetivo es entonces causar la menor perturbación posible y mantener cierta compatibilidad con la tecnología anterior, especialmente para aquellos países que prevén conservar su capacidad actual de lectura mecánica, es decir que no tienen previsto leer Pasaportes-e, excepto la lectura de la ZLM como se efectuaba antes.

5.4 El DCFWG consideró y descartó dos opciones iniciales:

- a) utilizar la combinación “PE” al comienzo de la primera línea de lectura mecánica (y otras combinaciones para visados y documentos oficiales de viaje de lectura mecánica, por ejemplo “VE” e “IE”, respectivamente). Esa opción tiene la ventaja de que se conservan los sistemas actuales de impresión, lectura y procesamiento. No obstante, existen desventajas importantes:
 - 1) se perderá el uso de la segunda letra para indicar tipos de pasaportes (p. ej, “PD” para “diplomáticos”); y
 - 2) algunos países ya están utilizando la combinación “PE” para los PLM tradicionales. Ello causará una gran confusión si se adopta esta opción.
- b) reemplazar la inicial “P” que se encuentra al principio de la primera línea de lectura mecánica por la letra “E” (y otras combinaciones de letras para visados y documentos oficiales de viaje de lectura mecánica). La segunda letra puede conservar el significado que tenía; por ejemplo, “ED” podría designar a un Pasaporte-e diplomático. No obstante, esta opción implica que:
 - 1) todos los dispositivos de lectura y sistemas de procesamiento actuales deberán modificarse, y no hay compatibilidad con la tecnología anterior. Esta opción causaría una gran perturbación y no tendría otro beneficio que el de indicar que se trata de Pasaportes-e; y
 - 2) también se considera inseguro utilizar sólo un carácter para indicar la presencia del microprocesador, dado que los falsificadores, deseosos de ocultar la presencia del microprocesador, atacarán ese carácter y tratarán de modificarlo, reemplazándolo por el de un pasaporte normal (“P”).

5.5 Al considerar la gran perturbación que esto ocasionaría a los sistemas de lectura y procesamiento de todo el mundo, se analizó la posibilidad de aplicar otras soluciones que:

- 1) no serían tan perturbadoras;
- 2) serían potencialmente compatibles con la tecnología anterior; y
- 3) ofrecerían un mejor rendimiento en cuanto a la legibilidad de los OCR-B.

5.6 Por consiguiente, una tercera y mejor opción consiste en reemplazar las últimas cinco posiciones del campo “Nombre” por un nuevo sistema de caracteres de verificación y un número de versión. Esto implica acortar el campo “Nombre” en cinco caracteres. Quizá también sea conveniente acortar en otras tres posiciones el campo “Nombre” e insertar tres separadores (“<<<”) para delimitar claramente el campo acortado “Nombre” del nuevo campo “Carácter de verificación y número de versión”.

5.7 El número de versión tiene como propósito:

- 1) identificar al PLM como Pasaporte-e; y
- 2) permitir futuras revisiones, de ser necesario.

El primer número de versión en todos los Pasaportes-e sería el número “1”, en la posición 42 de la línea superior de lectura mecánica.

5.8 Los caracteres de verificación tienen por propósito:

- 1) mejorar la legibilidad de los OCR; y
- 2) identificar al PLM como Pasaporte-e, es decir no depender sólo de un carácter de identificación.

Se han identificado posibles esquemas de caracteres de verificación simples pero eficientes numéricamente, que utilizan cuatro caracteres de verificación (A-Z, 0-9 y <) y que proporcionan un máximo de detección de errores y recuperación para 88 caracteres. El nuevo esquema de caracteres de verificación permite una lectura más precisa de la ZLM, puesto que incluye todos los datos que figuran en la ZLM, no solamente los campos seleccionados, como ocurre en el esquema actual.

5.9 El algoritmo propuesto funciona de la siguiente manera:

- a) todo carácter existente se representa con un número correspondiente (p. ej., 0..9 = 0..9; A = 10, B = 11, etc., hasta Z = 35; y < = 36);
- b) todos los campos de datos se disponen en la secuencia definida (p. ej., Clase, País expedidor, Nombre, Número de versión, Número del documento, etc), incluidos los dígitos de verificación ponderados 7-3-1 actuales. Esto genera una fila de 84 caracteres para el caso de PLM (puesto que deben sustraerse los cuatro caracteres de verificación nuevos de los 88 caracteres totales que figuran en las dos líneas);
- c) se calcula entonces el carácter de verificación núm. 1 (CV1) sumando todos los valores numéricos correspondientes a los 85 caracteres específicos. El resultado se divide por 37 tantas veces como sea necesario mientras el entero resultante sea mayor que 37, y el residuo final es el CV1;
- d) se calcula el CV2 mediante el mismo procedimiento; al efectuar la suma, el valor de cada carácter se multiplica por su posición en la fila;
- e) se calcula el CV3 mediante el mismo procedimiento; al efectuar la suma, los valores de los primeros 37 caracteres en la fila se multiplican por 1, los segundos 37 valores se multiplican por 2 y el resto de los valores se multiplican por 3;
- f) se calcula el CV4 mediante un procedimiento [tba];
- g) los caracteres de verificación (CV1, CV2, CV3 y CV4) oscilarán entre cero 0 y 36, y cada uno de ellos puede representarse mediante un único carácter, que luego se inserta en la posición respectiva en la ZLM (posiciones 40, 41, 43 y 44 de la línea superior de lectura mecánica); y
- h) el número de versión utiliza la posición 42 de la línea superior de lectura mecánica para “separar” los caracteres de verificación en dos grupos de dos caracteres cada uno, evitando así que resulte escrita una “mala” palabra en cualquier idioma.

5.10 El nuevo esquema de caracteres de verificación remite a toda la ZLM y no a campos individuales, como ocurría con el esquema anterior de dígitos de verificación con factores de

ponderación 7-3-1. Los campos que actualmente no están verificados, como “nombre” y otros, se incluyen en el nuevo esquema. Por medio de la función matemática, esos caracteres de verificación pueden detectar de manera fiable hasta tres errores, si las ubicaciones de los errores son desconocidas, y corregir el error, si sólo se ha corrompido una posición de carácter. Si se conocen las ubicaciones de los errores, se pueden corregir dos errores. Cabe señalar que los dígitos de verificación utilizados hasta ahora sólo remiten a sus respectivos campos (número del documento, fecha de nacimiento, fecha de caducidad y el campo de datos opcionales) y generalmente pueden detectar errores, aunque a veces dos o más errores pueden cancelarse entre sí y no ser detectados. La corrección de errores es posible sólo en determinadas circunstancias. En general, el esquema actual de dígitos de verificación con factores de ponderación 7-3-1 es ineficiente y, en parte, se adoptó porque puede calcularlo un ser humano. El nuevo esquema de caracteres de verificación es más eficaz y también podría ser calculado por un ser humano, aunque llevaría mucho tiempo hacerlo.

5.11 Lo fundamental de esta tercera opción es que la presencia del número de versión y el esquema revisado de caracteres de verificación indicarán que el PLM es un Pasaporte-e. Los dígitos de verificación ponderados 7-3-1 tradicionales en las posiciones 10, 20, 28, 43 y 44 de la línea inferior de lectura mecánica se dejan como antes para maximizar la compatibilidad.

5.12 El nuevo esquema de caracteres de verificación se traducirá en una lectura de OCR-B considerablemente mejorada. Esto es fundamental para que la ZLM pueda leerse en forma fiable para obtener una “clave” o “contraseña” que permita desbloquear un microprocesador sin contacto “cerrado”.

5.13 De todas las opciones examinadas, se considera que esta tercera opción es la más compatible con la tecnología anterior. Los países receptores que cuenten con dispositivos de lectura mecánica y sistemas de procesamiento tradicionales también podrán leer la ZLM de los Pasaportes-e. No obstante, los nuevos caracteres que figurarán al final del campo correspondiente al nombre pueden identificarse como parte del nombre, lo que ocasionará una falta de correspondencia en la base de datos. El uso de tres separadores (“<<<”) para separar el campo del nombre del nuevo campo puede evitar ese problema en la mayoría de los casos. Se debería instar a los países a que actualicen sus dispositivos de lectura mecánica y sistemas tradicionales mediante reprogramación o reemplazo para adaptarlos al nuevo esquema.

5.14 Los países que actualicen o instalen nuevos equipos de lectura y sistemas podrán leer ambos tipos de documentos de viaje (es decir, PLM tradicionales o Pasaportes-e). La adaptación al nuevo esquema de caracteres de verificación y la longitud reducida del campo correspondiente al nombre es esencialmente un ejercicio de programación. Ese ejercicio representa una pequeña fracción del esfuerzo para introducir la lectura de los CI sin contacto.

5.15 A raíz de las deliberaciones que tuvieron lugar en la reunión del DCFWG, se propuso como alternativa un sistema similar, que finalmente fue rechazado. Ese sistema de alternativa iba a utilizar el número de versión y el nuevo esquema de caracteres de verificación e iba a reemplazar al actual sistema de dígitos de verificación ponderados 7-3-1. El número de versión sería una “letra” (inicialmente, “A”) y reemplazaría al dígito de verificación general ubicado en la posición 44 de la línea inferior de lectura mecánica. Los nuevos caracteres de verificación reemplazarían a los dígitos de verificación que actualmente ocupan las posiciones 10, 20, 28 y 43 de la línea inferior de lectura mecánica. Ese esquema de alternativa se descartó por las razones siguientes:

- a) existiría una alta probabilidad de que los dispositivos actuales efectuaran una lectura defectuosa, puesto que el actual esquema de dígitos de verificación ya no se computaría, y lo más probable es que el Pasaporte-e se considerara falsificado; y

- b) los inspectores perderían un instrumento valioso para detectar pasaportes falsificados puesto que no podrían calcular manualmente los dígitos de verificación. Los falsificadores suelen colocar dígitos de verificación incorrectos. Con el nuevo esquema de caracteres de verificación, también se dispone de los mismos medios de detección, por cierto, pero el nuevo algoritmo es mucho más difícil de calcular manualmente.

5.16 Cabe señalar que no es posible utilizar el campo de datos opcionales de la ZLM (posiciones 29 a 43 de la línea inferior de lectura mecánica) para los caracteres de verificación y número de versión, puesto que numerosos Estados expedidores utilizan ese campo para otros propósitos.

6. **MEDIDAS PROPUESTAS AL TAG/MRTD**

6.1 El DCFWG invita al TAG/MRTD a que:

- a) tome nota de la labor y del enfoque adoptado por el DCFWG para la identificación de Pasaportes-e mediante el uso de la ZLM, y del nuevo esquema de caracteres de verificación para la ZLM; y
- b) recomiende la aprobación del enfoque y de la labor realizada hasta la fecha por el DCFWG, y apruebe la elaboración de especificaciones técnicas más precisas para su inclusión en el Doc 9303.

— FIN —