**ТЕХНИЧЕСКАЯ КОНСУЛЬТАТИВНАЯ ГРУППА
ПО МАШИНОСЧИТЫВАЕМЫМ ПРОЕЗДНЫМ ДОКУМЕНТАМ**

Пятнадцатое совещание

(Монреаль, 17–21 мая 2004 года)

Пункт 2 повестки дня. **Доклад Рабочей группы по содержанию и формату документов**
Пункт 2.1 повестки дня. **Ход обновления документа Doc 9303 и предлагаемые поправки**

ИНДИКАТОР "ЭЛЕКТРОННОГО ПАСПОРТА". НОМЕР ВЕРСИИ И СХЕМА ПРОВЕРКИ ЗНАКОВ МАШИНОСЧИТЫВАЕМЫХ ПРОЕЗДНЫХ ДОКУМЕНТОВ

(Представлено Рабочей группой по содержанию и формату (DCFWG))

1. ВВЕДЕНИЕ

1.1 Настоящий рабочий документ был подготовлен по просьбе Рабочей группы по новым технологиям (NTWG) с целью найти способ включения в машиносчитываемую зону (МСЗ) указателя на то, что проездной документ содержит бесконтактную интегральную схему. Такой тип проездного документа называется "электронный паспорт", поскольку машиносчитываемый паспорт (МСП) с бесконтактной интегральной схемой является первым образцом этой технологии.

2. АННОТАЦИЯ

2.1 Введение индикатора электронного паспорта в МСЗ вызывает серьезную проблему обратной совместимости установленного считывающего оборудования и систем пограничного контроля. Трудности возникают независимо от принятого метода. Эта проблема рассматривается в настоящем рабочем документе. В нем предлагается решение по сохранению основной структуры машиносчитываемой зоны, хотя этот метод не совсем соответствует принципам обратной совместимости. Решение имеет дополнительные преимущества в плане значительного повышения использования машиносчитываемой зоны, как в настоящее время, так и в долгосрочной перспективе. Концепция была обсуждена на совещании Группы DCFWG (Базингсток, 8–10 марта 2004 года), а затем более подробно разработана в ходе продолжительной переписки по электронной почте.

3. КОНЦЕПЦИЯ

3.1 Электронный паспорт является традиционным МСП, описание которого приводится в Doc 9303, но обладающим дополнительными характеристиками факультативной информации в виде включенной в него бесконтактной микросхемы.

3.2 Бесконтактная микросхема содержит одну или более биометрических характеристик и цифровую подпись (Инфраструктура открытого ключа – PKI), зашифрованных с использованием структуры логических данных (LDS). Посредством биометрических характеристик электронный паспорт связан с владельцем, а цифровая подпись может защитить документ от подделки и самовольных изменений. Эти две основные концепции в значительной степени затрудняют подлог и фальсификацию, а то и полностью исключают их.

3.3 С целью борьбы с несанкционированным чтением документов несколько выпускающих такие паспорта стран предложили факультативно защитить микросхему паролем. Этот пароль извлекается из машиносчитываемой зоны с помощью традиционного оптического распознавания знаков (OCR). Эта операция известна как "закрытый доступ" (в отличие от незакрытых микросхем, которые имеют "открытый доступ" и поэтому не требуют пароля). Возможность считывания с помощью OCR здесь является критическим вопросом.

4. ЗАТРОНУТЫЕ DCFWG ВОПРОСЫ

4.1 Как можно узнать о наличии микросхемы в процессе машинного считывания? Хотя обложка паспорта и страница данных могут быть промаркированы визуально распознаваемым логотипом, тем не менее его изображение не распознается в процессе машинного считывания. NTWG поручила DCFWG рассмотреть возможности соответствующего изменения машиносчитываемой зоны для выполнения этой функции. Следует помнить, что в процессе выполнения этой функции нельзя полагаться на саму микросхему, поскольку она может выйти из строя, либо находиться в "закрытом" состоянии ("закрытый доступ").

4.2 Каким образом сделать процесс считывания МСЗ более точным и надежным? Даже если ряд государств и примет факультативную процедуру "закрытого доступа", то получающим такие паспорта странам придется с помощью оборудования МСЗ считывать электронные паспорта для установления ключа, применяющегося для открытия закрытой микросхемы. Если в соответствии с сообщениями уровень ошибок при машинном считывании является весьма высоким в некоторых странах, то от этого пострадает процесс упрощения формальностей, поскольку необходимо будет проверять паспорта вручную, чтобы компенсировать этот уровень ошибок.

5. ПРЕДЛОЖЕНИЕ DCFWG. НОМЕР ВЕРСИИ И НОВАЯ СХЕМА ПРОВЕРКИ ЗНАКОВ

5.1 DCFWG предлагает принять в обязательном порядке новую схему проверки знаков в зоне МСЗ с установкой номера версии, который:

a) определит МСП как электронный паспорт;

b) позволит преодолеть ограниченность имеющейся в настоящее время схемы проверки цифр;

c) в большей степени повысит защиту OCR в процессе считывания; и

d) откроет возможности для дальнейшего усовершенствования МСЗ за счет введения определителя версии.

5.2 Следует отметить, что любая модификация МСЗ, хоть самая малая (один знак) или более серьезная (несколько знаков), приведут к тем же самым разрушительным последствиям во всем мире для существующего машиносчитывающего оборудования и систем обработки данных. Однако для тех стран, которые вводят в действие электронные паспорта, усилия по модификации печати и считывания МСЗ крайне малы по сравнению с усилиями, требующимися для шифровки и считывания бесконтактных микросхем.

5.3 Таким образом, целью является создание минимального количества трудностей и сохранение некоторой степени обратной совместимости, в особенности в тех странах, в которых планируется сохранить уже существующие возможности считывания. Другими словами, в настоящее время нет планов считывания электронных паспортов, за исключением МСЗ, как это и делалось раньше.

5.4 DCFWG рассмотрела и отказалась от двух первоначальных вариантов:

a) использование комбинации "PE" в начале первой машиносчитываемой строки (и других комбинаций для виз и MROTD, например "VE" и "IE" соответственно). У этого варианта имеется преимущество сохранения существующих систем печати, считывания и обработки данных. Однако имеются также и серьезные недостатки:

   1) происходит потеря второй буквы для обозначения типа паспортов (например, "PD" для "дипломатический"); и

   2) некоторые страны уже используют комбинацию "PE" для традиционных машиносчитываемых паспортов. Если этот вариант будет принят, то это приведет к возникновению серьезных недоразумений;

b) замена первой буквы "P" в начале первой машиносчитываемой строки буквой "E" (и другими комбинациями букв для виз и для MROTD). Вторая буква может сохранить свое значение, как и раньше, например "ED" может обозначать дипломатический электронный паспорт. Однако этот вариант означает, что:

   1) все существующие считывающие устройства и системы обработки данных необходимо модифицировать, но в результате пропадает характеристика обратной совместимости. Этот вариант может привести к максимальному ущербу, не дав взамен ничего, кроме обозначения электронных паспортов; и

   2) также считается небезопасным полагаться только на один знак, указывающий на наличие микросхемы, поскольку изготовители подложных документов, желающие скрыть наличие микросхемы, попытаются убрать этот знак и перевести этот паспорт в разряд стандартного ("P").

5.5 При рассмотрении столь серьезного нарушения мировых систем считывания и обработки данных была обсуждена возможность принятия других решений:

1) уменьшить серьезность влияния этих моментов;

2) оставить потенциал обратной совместимости; и

3) предложить усовершенствованные характеристики в плане считывания OCR-B.

5.6 Таким образом, третьим и наилучшим вариантом является замена последних пяти позиций "Именного поля" новой системой проверки знаков и номера версии. Это приведет к сокращению "Именного поля" на 5 знаков. Также может стать желательным дальнейшее сокращение "Именного поля" еще на 3 знака, включив 3 разделяющих знака ("<<<") с целью четкого разграничения укороченного "Именного поля" и нового поля "Проверки знаков и номера версии".

5.7 Цель номера версии заключается в том, чтобы:

1) обозначить машиносчитываемый паспорт как электронный паспорт; и

2) при необходимости позволить внесение дальнейших изменений.

Этот первый номер версии во всех электронных паспортах будет представлять собой номер "1" в позиции 42 верхней машиносчитываемой строки.

5.8 Цель контрольных знаков сводится к тому, чтобы:

1) улучшить возможности считывания OCR; и

2) дополнительно обозначить машиносчитываемый паспорт как электронный паспорт, т. е. перестав полагаться только на один определяющий знак.

Для простой, но эффективной схемы цифровой проверки знаков были определены способы использования четырех контрольных знаков (A-Z, 0-9 и <), а также нахождение в максимальной степени ошибок и восстановление 88 знаков. Новая схема проверки знаков дает возможность более точного считывания МСЗ поскольку в нее включаются все данные МСЗ, а не только выбранные поля, как это делается в рамках имеющейся в настоящее время схемы.

5.9 Предлагаемый алгоритм работает следующим образом:

a) каждый существующий знак имеет соответствующий номер (например, 0..9 = 0..9; A = 10, B = 11 и т. д., до Z = 35; и < = 36);

b) все поля данных выстраиваются в определенной последовательности (например, тип, страна выдачи, имя, номер версии, номер документа и т. д.), включая существующие в настоящее время проверочные цифры 7-3-1. Это дает возможность написания в строку 84 знаков в машиносчитываемом паспорте (поскольку из общего числа 88 знаков на двух строках необходимо вычесть четыре новых контрольных знака);

c) в настоящее время расчет контрольного знака № 1 (CC1) осуществляется с помощью добавления всех цифровых значений, соответствующих конкретным 85 знакам. Результат делится на 37 столько раз, чтобы целое число в остатке было больше 37, а окончательный остаток представляет собой CC1;

d) расчет CC2 осуществляется с помощью той же самой процедуры, хотя в процессе суммирования значение каждого знака умножается на его положение в ряду;

e) расчет CC3 осуществляется с помощью той же процедуры, хотя суммирование первых 37 значений знаков в ряду умножается на 1, второе значение 37 знаков умножается на 2, а остальные умножаются на 3;

f) расчет CC4 производится в соответствии с процедурой [tba];

g) контрольные знаки (CC1, CC2, CC3 и CC4) располагаются в границах между 0 и 36 и каждый из них может быть согласован с единым знаком, который вслед за этим вносится на соответствующую позицию МСЗ (позиции 40, 41, 43 и 44 верхней машиносчитываемой строки); и

h) номер версии занимает 42 позицию верхней машиносчитываемой строки с целью "разбить" контрольные знаки на 2 группы по 2 знака в каждом, таким образом препятствуя произнесению непристойных слов на любом языке.

5.10 Новая схема контрольных знаков относится ко всей МСЗ, а не к отдельным полям, как это делалось ранее в соответствии со схемой цифровой проверки 7-3-1. Таким образом, непроверенные в настоящее время именное и другие поля включаются в эту новую схему. Посредством математических функций и с помощью этих контрольных знаков можно надежно определять до трех ошибок, если место расположения ошибок не известно, и исправлять ошибку, если искажена только одна позиция знака. Если месторасположение ошибки известно, то можно исправить две ошибки. Следует принять к сведению, что использовавшиеся в прошлом контрольные цифры относились только к своим соответствующим полям (номер документа, дата рождения, дата истечения срока и поле факультативных данных), и обычно могут определять ошибки, хотя иногда две или более ошибок могут аннулировать друг друга и не подлежать определению. Исправление ошибок возможно только в некоторых случаях. В общем, используемая в настоящее время цифровая схема весовой проверки 7-3-1 является малоэффективной, и применятся только частично, поскольку рассчитывается человеком. Новая схема проверки знаков обладает большими возможностями и все же может быть рассчитана человеком, хотя представляет собой отнимающую много времени задачу.

5.11 Существом этого третьего варианта является наличие номера версии и пересмотренная схема проверки знаков, которые покажут, что машиносчитываемый паспорт является электронным паспортом. Традиционная весовая поверка цифр в позициях 10, 20, 28, 43 и 44 нижней машиносчитываемой строки остается, как и прежде, без изменения с целью максимальной обратной совместимости.

5.12 Новая схема проверки знаков приведет к значительному усовершенствованию считывания OCR-B. Это становится необходимым, если МСЗ должна надежно считываться с целью получения "ключа" или "пароля" для открытия "закрытой" бесконтактной микросхемы.

5.13 Этот третий вариант считается наиболее приемлемым из всех рассмотренных с точки зрения обратной совместимости. Получающие паспорта страны с традиционными устройствами для машиносчитывания и системами обработки смогут и дальше продолжать считывание МСЗ е-паспортов. Однако новые знаки в конце именного поля можно будет определять как часть имени, вызывая тем самым ошибки при сравнении с базой данных. Использование трех разделительных знаков ("<<<") с целью отделить именное поле от нового поля может во многих случаях воспрепятствовать возникновению этой проблемы. Государства следует побуждать к обновлению своих традиционных систем и оборудования для машинного считывания с помощью перепрограммирования или замены такого оборудования на приспособленное к работе в рамках новой схемы.

5.14 Страны, занимающиеся усовершенствованием или установкой нового считывающего оборудования и систем, смогут считывать оба типа проездных документов (т. е. традиционный МСП или электронный паспорт). Введение новой схемы проверки знаков и сокращение длины именного поля

необходимо осуществить в рамках программирования. Эта задача представляет собой небольшую часть усилий в области считывания бесконтактных ИС.

5.15 В результате обсуждения вопросов на совещании DCFWG была предложена похожая альтернативная схема, но в конечном итоге от нее отказались. Эта альтернатива заключается в использовании номера версии и новой схемы проверки знаков для замены существующей взвешенной цифровой проверки 7-3-1. Номер версии становится "буквой" (начиная с "A") и заменяет общую проверочную цифру на позиции 44 нижней машиносчитываемой строки. Новые контрольные знаки заменят применяемые в настоящее время контрольные цифры на позициях 10, 20, 28 и 43 нижней машиносчитываемой строки. Эта альтернатива была отклонена в результате следующих причин:

a) существующие считыватели будут подвержены большому риску неверного считывания, поскольку существующие схемы контрольных цифр не будут приниматься в расчет, и электронные паспорта, по всей вероятности, будут обозначаться как поддельные; и

b) инспекторы потеряют ценный инструмент для обнаружения фальшивых паспортов, поскольку они уже не смогут рассчитывать контрольные цифры вручную. Изготовители подложных документов часто получают неверные контрольные цифры. Конечно, остаются те же самые средства определения и при наличии новых контрольных знаков, и новый алгоритм значительно труднее рассчитать вручную.

5.16 Следует принять к сведению, что использование поля факультативных данных в МСЗ, (позиции 29–43 нижней машиносчитываемой строки) для проверки знаков и номера версии становится невозможным, поскольку многие государства-изготовители паспортов используют это поле для других целей.

6. ДЕЙСТВИЯ TAG-MRTD

6.1 DCFWG предлагает TAG-MRTD:

a) принять к сведению результаты работы и методику DCFWG по идентификации электронных паспортов с помощью МСЗ, а также новую схему контрольных знаков для МСЗ; и

b) одобрить методику и результаты работы, проведенную до настоящего времени DCFWG, и одобрить разработку более точных технических требований для включения их в документ Doc 9303.

– КОНЕЦ –