**ТЕХНИЧЕСКАЯ КОНСУЛЬТАТИВНАЯ ГРУППА
ПО МАШИНОСЧИТЫВАЕМЫМ ПРОЕЗДНЫМ ДОКУМЕНТАМ**

Пятнадцатое совещание

(Монреаль, 17–21 мая 2004 года)

Пункт 3 повестки дня. **Доклад Рабочей группы по новым технологиям**
Пункт 3.1 повестки дня. **Обновление информации о разработке технических требований к использованию цифровых подписей PKI в МСПД**

НОВЫЙ ТЕХНИЧЕСКИЙ ДОКЛАД. PKI В МСПД

(Представлено Рабочей группой по новым требованиям и Специальной группой по инфраструктуре сертификации открытых ключей (PKI))

1. На TAG/14 был одобрен документ, в котором предлагалось использовать схему PKI для защиты электронных данных в МСПД. При этом TAG отметила, что в этом документе описывается только концепция использования контролируемого ИКАО справочника открытых ключей шифрования и описываются роли, которые играют выдающие и получающие ключи государства. Необходимо было проделать дополнительную работу, чтобы конкретно и достаточно подробно определить упомянутую схему в целях обеспечения ее внедрения. Эта дополнительная работа была проделана Специальной группой по PKI, которая была создана NTWG.

2. Был подготовлен новый технический доклад, в котором на достаточно детализированном техническом уровне описаны технические требования, которые выдающие документы государства могут применять в отношении схемы PKI для обеспечения защиты электронных данных в своих проездных документах. Установленный объект защиты документа, электронным способом подписанный выдающим документ государством, позволяет принимающим государствам проверить аутентичность и подлинность электронных данных на чипе документа.

3. Кроме того, в техническом докладе описываются требования, которые могут применять государства и организации, желающие считывать электронные данные, а также приводится описание справочника открытых ключей шифрования, который ИКАО, возможно, вскоре начнет использовать. В докладе также рекомендуется, чтобы открытые ключи подписывающего документ лица сохранялись на самом чипе МСПД, но это не обязательное требование. Справочник открытых ключей шифрования может стать ценным пособием для государств, использующих МСПД, даже в том случае, если открытый ключ включается в чип документа.

4. Кроме того, в техническом докладе приводится описание требований к дополнительным необязательным видам защиты, которые могут применяться в целях борьбы с угрозой несанкционированного съема или считывания данных с бесконтактных чипов. Эта дополнительная мера защиты, называемая в техническом докладе "основной контроль доступа", может использоваться по усмотрению выдающего документ государства.

5. Кроме того, в докладе определена еще одна дополнительная необязательная мера защиты, которая называется "активная аутентификация". Эта мера направлена на предотвращение подмены чипа и может применяться на работающих без обслуживающего персонала контрольных пунктах, когда МСПД используется в качестве электронного жетона для получения доступа.

6. В настоящее время этот технический доклад подготовлен и рассмотрен настолько, что NTWG считает, что он содержит достаточно детальную информацию, чтобы государства могли приступить к использованию электронных паспортов. Однако, скорей всего, по мере их внедрения будут возникать дополнительные вопросы, и поэтому необходимо будет постоянно уточнять этот доклад.

7. Схема PKI предназначена для защиты данных, внесенных в документ в момент выдачи, но не после их обновления. Дополнительная задача NTWG заключается в разработке интероперабельной в глобальном масштабе схемы PKI, способной обеспечить включение дополнительных электронных данных в документ в течение срока его действия. Эта работа выходит за рамки полномочий существующей Специальной группы.

8. Дополнительно к содержащемуся в TAG-MRTD-WP/10 техническому докладу был представлен документ "Ответы на вопросы, которые чаще всего задают". Этот документ подготовлен по той причине, что сам доклад по PKI носит чисто технический характер. Вопросы были главным образом подготовлены членами Специальной группы, но в дальнейшем предполагается обновлять этот документ ответами на вопросы, которые будут возникать у государств, использующих МСПД.

9. ДЕЙСТВИЯ TAG/MRTD

9.1 TAG/MRTD предлагается одобрить технический доклад "PKI для машиносчитываемых проездных документов, обеспечивающих доступ ICC только по считыванию, вариант 1.0".

– КОНЕЦ –