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

QUINZIÈME RÉUNION

Montréal, 17 – 21 mai 2004

Point 3 : Rapport du Groupe de travail des technologies nouvelles (NTWG)
3.1 : Bilan de l'élaboration de spécifications concernant l'utilisation de signatures numériques activées par la PKI dans les MRTD

NOUVEAU RAPPORT TECHNIQUE — PKI POUR LES MRTD

(Note présentée par le Groupe de travail des technologies nouvelles [NTWG] et l'Équipe de travail sur l'infrastructure à clés publiques [PKI])

1. À sa 14e réunion, le TAG a entériné une note proposant le recours à un mécanisme PKI pour assurer la sécurité des données électroniques contenues dans les MRTD. Le TAG a pris acte du fait que la note se limitait à décrire les concepts entourant l'utilisation d'un annuaire de clés publiques géré par l'OACI, ainsi que le rôle des États émetteurs et des États récepteurs. Il a été convenu qu'il fallait poursuivre les travaux afin de recueillir suffisamment de précisions techniques sur le système pour en permettre la mise en place. Ces travaux supplémentaires ont été effectués par l'Équipe de travail sur les PKI instituée par le NTWG.

2. Un nouveau rapport technique a été préparé, qui présente, détails techniques à l'appui, les spécifications pouvant servir aux États émetteurs pour mettre en œuvre les PKI afin d'assurer la sécurité des données contenues dans les documents de voyage qu'ils délivrent. Grâce à la signature électronique de l'État émetteur, l'objet de sécurité spécifié sur le document de voyage permet à l'État récepteur de vérifier l'authenticité et l'intégrité des données électroniques stockées dans la puce du document.

3. Le rapport technique énonce également les exigences visant les États et les organisations qui souhaitent lire les données électroniques et décrit un annuaire de clés publiques que l'OACI pourrait créer. Le rapport recommande que les clés publiques des entités qui signent les documents soient stockées dans la puce des MRTD, bien que cette mesure soit facultative. L'annuaire de clés publiques sera d'une grande utilité pour les émetteurs de MRTD, même si la clé publique est comprise dans la puce du document.

4. Le rapport technique présente en outre des spécifications relatives à d'autres caractéristiques de sécurité facultatives pouvant être adoptées pour contrer des menaces comme l'interception illicite et «l'écrémage» (copie frauduleuse) des données contenues dans les puces sans

contact. Ainsi, l'État émetteur peut, à sa discrétion, adopter l'élément de sécurité supplémentaire, appelé dans le rapport technique «contrôle d'accès de base».

5. Le rapport décrit une autre caractéristique de sécurité facultative, «l'authentification active». Ce dispositif, qui vise à prévenir la substitution des puces, peut être mis en service aux postes de contrôle sans personnel, où le MRTD est utilisé comme laissez-passer électronique permettant l'accès.

6. La rédaction et la révision du rapport technique ont progressé à un tel point que le NTWG estime qu'il contient suffisamment d'informations détaillées pour permettre aux États de commencer à émettre des passeports électroniques. Cependant, des problèmes surgiront au fur et à mesure de la mise en œuvre, d'où le besoin de continuer à réviser le rapport.

7. Le mécanisme PKI est conçu pour protéger les données inscrites au moment de la délivrance du document, sans mise à jour. Le nouveau défi pour le Groupe NTWG est de concevoir un mécanisme PKI interopérable à l'échelle mondiale qui accepterait des ajouts aux données électroniques pendant toute la durée de validité du document. Or, une telle tâche dépasse le cadre du mandat actuel de l'Équipe de travail.

8. Une «Foire aux questions» est jointe à la note TAG-MRTD-WP/10, à titre de complément au rapport technique. Ce document a été préparé en raison de la nature technique du rapport. La plupart des questions ont été inventées par les membres de l'Équipe de travail, mais on prévoit d'actualiser le document en intégrant de véritables questions posées au fur et à mesure de la mise en œuvre par les services émetteurs de MRTD.

9. SUITE PROPOSÉE AU GROUPE TAG-MRTD

9.1 Le TAG-MRTD est invité à entériner le rapport technique «PKI for Machine Readable Travel Documents Offering ICC Read-only Access» (Application de la PKI pour les documents de voyage lisibles à la machine permettant uniquement la lecture des puces), version 1.0.

—FIN—