

Le passeport biométrique est finalement sur les rails

La publication ce 4 mai du dernier décret permettant la diffusion du passeport biométrique en France donne le coup d'envoi de la production en masse de ce document, censé proposer ce qui se fait de mieux en matière de sécurité. Il s'agit également de répondre aux exigences sécuritaires de pays comme les Etats-Unis. Il remplacera le passeport électronique (Delphine) mis en circulation depuis avril 2006.

Les premiers passeports biométriques devraient sortir des machines de l'Imprimerie nationale dès cet automne. Mais sa généralisation ne se fera pas avant juin 2009. En effet, l'Etat devra choisir le consortium d'industriels qui fabriquera les machines permettant la capture des données biométriques, un marché estimé à 100 millions d'euros. Thalès-Accenture, Atos-Sagem, Cap Gemini-Sopra et Bull sont les quatre consortiums candidats.

En effet, ce nouveau passeport intègre une puce RFID contenant une photo numérique du propriétaire et les empreintes digitales de huit doigts... Grâce à la puce RFID, il sera aisé pour les autorités compétentes d'accéder sans fil (grâce à un simple lecteur) aux fichiers stockés et ainsi vérifier l'identité du porteur du document.

Cinq départements auront la primeur du passeport biométrique : le Nord, l'Oise, l'Aube, la Gironde et la Loire-Atlantique. Ils testeront donc en avant première les machines permettant sa réalisation.

Le nouveau document aura une validité de 10 ans. Mais selon le décret publié dimanche, un passeport d'une durée de validité d'un an ne comportant pas de composant électronique pourra encore être délivré « à titre exceptionnel et pour des motifs de nécessité impérieuse ou d'urgence dûment justifiée ».

Il n'y a plus qu'à espérer que le passeport biométrique à la française soit exempt de failles. L'année dernière, le passeport biométrique britannique se faisait hacker en beauté.

[Pour mener à bien son attaque](#), Adam Laurie, un consultant en sécurité qui a longtemps travaillé sur la RFID (Radio Fréquence Identification) et le Bluetooth, a simplement utilisé un lecteur RFID et un code personnalisé. D'après lui cette attaque reste totalement invisible. En effet, il a réussi à littéralement siphonner les données du chip RFID d'un passeport placé dans une enveloppe sous scellée.

En 2006, un hacker, nommé Lukas Grunwald a montré lors du Black Hat de Las Vegas comment cloner ces passeports. Selon le spécialiste de la sécurité Bruce Schenier, le travail réalisé par Grunwald a été grandement simplifié par la publication du détail des technologies utilisées pour lesdits documents sur le site de l'organisation internationale civile d'aviation.