Network and security managers are always having to deal with identification and authentication. In today’s column I’m looking at a dust-up between Europe and the US over how to enforce strong authentication of travelers’ identity. Although the topic is not directly related to our daily work, I think we have contributions to make to the popular and political debates about such issues based on our applicable technical expertise.

Passports in their modern form were introduced in the early 20th century. Until that time, travel documents were issued by national governments for specific voyages through specific regions. “In this way, early passports are more similar to modern visas than to modern passports, whose primary function is to prove the identity and nationality of the holder.” [“Passport,” from Wikipedia <http://en.wikipedia.org/wiki/Passport#History>]. Passports have space for visas but are much longer-term documents, usually valid for five years or more.

Today, passports have assumed a central role in preventing the entry of politically undesirable or dangerous people (they are not necessarily the same category) into the United States. For example, the British activist Yusuf Islam, once widely known as the singer Cat Stevens, was refused entry into the United States in September 2004 on nebulous grounds that sparked ridicule and outrage worldwide as well as among his fans in the US <http://news.bbc.co.uk/2/hi/americas/3678694.stm>.

The most important issue to remember about passports as a security measure is that they bind a real-world identifier to a picture and a document; they tell us nothing in themselves about the bearer of the passport. All the terrorists who flew planes into the World Trade Center towers had passports that got them into the USA.

Being made of paper and bearing simple photographs, passports have been relatively easy to counterfeit. For example, an article by Philip Shishkin in the Wall Street Journal (Oct 8, 2001) reported that fake passports were a big business, with prices for forged US passports ranging from $2,000 to $12,000.

To help make forgery more difficult and identification of fraudulent holders of passports easier, the US State Department has mandated that passports used to enter the US be equipped with machine-readable biometric information. USA passports issued after October 2005 will also be so equipped. “The proposed U.S. Electronic Passport is the same as a regular passport with the addition of a small contactless integrated circuit (computer chip) embedded in the back cover. The chip will securely store the same data visually displayed on the photo page of the passport, and will additionally include a digital photograph. The inclusion of the digital photograph will enable biometric comparison, through the use of facial recognition technology at international borders. The U.S. “e-passport” will also have a new look, incorporating additional anti-fraud and security features.”<http://travel.state.gov/passport/eppt/eppt_2498.html>.

According to a review by Duncan Graham-Rowe, differences in how the US and the European Union intended to integrate biometric data into their passports may spell trouble for people on
both sides of the ocean [“ID row bad news for transatlantic travellers,” _NewScientist_ 16 Apr 2005 <http://www.newscientist.com/article.ns?id=mg18624956.500>]. For example, the original design for the chip-equipped US passport was supposed to allow remote reading – until critics pointed out that having the details of someone’s passport readable from inside their pocket, briefcase, purse or knapsack might be dangerous in many parts of the world, especially with the recent worldwide decline in popularity of Americans due in part to the invasion of Iraq <http://pewglobal.org/reports/display.php?ReportID=247>. It appears that the new plans may include lining the new passports with foil to reduce the incidence of unauthorized data extraction.

Let’s hope the EU and the US can resolve these disagreements before international travel becomes even more unpleasant than it already is.

* * *

Author’s note: if you are interested in airport safety, see my analysis at <http://www.mekabay.com/opinion/airport_safety.htm> or <http://www.mekabay.com/opinion/airport_safety.htm>.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to _Network World_ to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.