Press Release: Budapest Declaration on Machine Readable Travel Documents (MRTDs)

By failing to implement an appropriate security architecture, European governments have effectively forced citizens to adopt new European passports which dramatically decrease their security and privacy. Whilst still susceptible to traditional ID document abuse scenarios, such Machine Readable Travel Documents (MRTDs) introduce numerous additional threats. From these the following are of particular importance:

- In contrast to traditional ID documents, European MRTD data can be remotely read or eavesdropped from distances of up to 10 metres. This is compounded by vulnerabilities in access control which is susceptible to circumvention or hacking. The result is a risk of ubiquitous, unobserved access to MRTD data by authorised or unauthorised third parties, and enables tracking of people carrying a passport, for example when residing as a tourist in a foreign country.
- Use of biometric data stored on ID documents is exploitable by both the public and private sectors for additional purposes − a violation of European privacy principles. Moreover, since biometrics themselves are based on probabilities, false positive and negative authentication are unavoidable and will potentially affect many European citizens every day at airports or other border controls.

Put simply, the current implementation of the European passport uses technologies and standards that are poorly conceived for its purpose. In the “Budapest declaration” (styled at the September 2006 Budapest meeting of the FIDIS “Future of Identity in the Information Society” Network of Excellence, www.fidis.net) researchers on Identity and Identity Management set out their assessment of MRTDs and their recommendations for adoption by governments and industry alike. The “Budapest declaration” is available in a selection of European languages from:
www.fidis.net/home/single-news/article/budapest-declaration-on-machine-readable-travel-documents-mrtds.