

Sent: 03 February 2006 01:19
To: IT Strategy Project Team
Subject: Security and the IT Strategy Project

Having read the Transformational Government document, there is one omission that strikes me as stark: security. You are obviously keen to tear down the barriers to information flow, but some of those barriers are there for a very good reason.

Take the ID cards issue, for instance. While a secure device under the control of the user could be a very good thing (an HMG-issued PKI client certificate would cut online fraud in a very real way), that is not a part of the strategy. Furthermore, the proximity feature (AKA RFID) is based on ineptly-designed international passport systems, the cryptography of which was broken last year[1]. Unconscionably, there are no plans to scrap this security leak before large-scale deployment. The only safe way to handle such a card is to destroy the proximity chip, for instance by a short burst of power in a microwave oven.

PLEASE TAKE SECURITY SERIOUSLY.

I am not willing to sit idly by and see my security put at risk by the incompetence of others.

--

Terry Browning

[1] The Dutch biometric passport is broken into from a 10m range, utilising only 2 hours of computer time to break the codes:
http://www.theregister.com/2006/01/30/dutch_biometric_passport_crack/
and <http://www.riscure.com/news/passport.html>

The use of actual data as part of a cryptography-key is an act of frightening stupidity akin to using a paper fire guard.