Forwarded by Jannie Bester on the qde-all list 8/8/08

From The Times
August 6, 2008

‘Fakeproof’ e-passport is cloned in minutes

A forged e-passport

Steve Boggan

New microchipped passports designed to be foolproof against identity theft can be cloned and manipulated in minutes and accepted as genuine by the computer software recommended for use at international airports.

Tests for *The Times* exposed security flaws in the microchips introduced to protect against terrorism and organised crime. The flaws also undermine claims that 3,000 blank passports stolen last week were worthless because they could not be forged. In the tests, a computer researcher cloned the chips on two British passports and implanted digital images of Osama bin Laden and a suicide bomber. The altered chips were then passed as genuine by passport reader software used by the UN agency that sets standards for e-passports.

The Home Office has always argued that faked chips would be spotted at border checkpoints because they would not match key codes when checked against an international data-base. But only ten of the forty-five countries with e-passports have signed up to the Public Key Directory (PKD) code system, and only five are using it. Britain is a member but will not use the directory before next year. Even then, the system will be fully secure only if every e-passport country has joined.

Some of the 45 countries, including Britain, swap codes manually, but criminals could use fake e-passports from countries that do not share key codes, which would then go undetected at passport control.

The tests suggest that if the microchips are vulnerable to cloning then bogus biometrics could be inserted in fake or blank passports.

Tens of millions of microchipped passports have been issued by the 45 countries in the belief that they will make international travel safer. They contain a tiny radio frequency chip and antenna attached to the inside back page. A special electronic reader sends out an encrypted signal and the chip responds by sending back the holder’s ID and biometric details.

Britain introduced e-passports in March 2006. In the wake of the September 11 attacks, the United States demanded that other countries adopt biometric passports. Many of the 9/11 bombers had travelled on fake passports.

The tests for *The Times* were conducted by Jeroen van Beek, a security researcher at the University of Amsterdam. Building on research from the UK, Germany and New Zealand, Mr van Beek has developed a method of reading, cloning and altering microchips so that they are accepted as genuine by Golden Reader, the standard software used by the International Civil
Aviation Organisation to test them. It is also the software recommended for use at airports.

Using his own software, a publicly available programming code, a £40 card reader and two £10 RFID chips, Mr van Beek took less than an hour to clone and manipulate two passport chips to a level at which they were ready to be planted inside fake or stolen paper passports.

A baby boy’s passport chip was altered to contain an image of Osama bin Laden, and the passport of a 36-year-old woman was changed to feature a picture of Hiba Darghmeh, a Palestinian suicide bomber who killed three people in 2003. The unlikely identities were chosen so that there could be no suggestion that either Mr van Beek or *The Times* was faking viable travel documents.

“We’re not claiming that terrorists are able to do this to all passports today or that they will be able to do it tomorrow,” Mr van Beek said. “But it does raise concerns over security that need to be addressed in a more public and open way.”

The tests also raise serious questions about the Government’s £4 billion identity card scheme, which relies on the same biometric technology. ID cards are expected to contain similar microchips that will store up to 50 pieces of personal and biometric information about their holders. Last night Dominic Grieve, the Shadow Home Secretary, called on ministers to take urgent action to remedy the security flaws discovered by *The Times*. “It is of deep concern that the technology underpinning a key part of the UK’s security can be compromised so easily,” he said.

The ability to clone chips leaves travellers vulnerable to identity theft when they surrender their passports at hotels or car rental companies. Criminals in the back office could read the chips and clone them. The original passport holder’s name and date of birth could be left on the fake chip, with the picture, fingerprints and other biometric data of a criminal client added. The criminal could then travel the world using the stolen identity and the original passport holder would be none the wiser.

The Home Office said last night that it had yet to see evidence of someone being able to manipulate data in an e-passport. A spokesman said: “No one has yet been able to demonstrate that they are able to modify, change or alter data within the chip. If any data were to be changed, modified or altered it would be immediately obvious to the electronic reader.”

The International Civil Aviation Organisation said: “The PKD ensures that e-passports used at border control points . . . are genuine and unaltered. In effect it renders the passport fool-proof. However, all states issuing e-passports must join the PKD, otherwise that assurance cannot be given.”

Going biometric

1999 International Civil Aviation Organisation begins study into possibility of worldwide use of travel documents carrying biometric data

2002 After 9/11 US announces all passports issued from 2006 and used to enter the country must contain biometric information or holder will require a visa

2006 Britain and many EU countries introduce biometric passports

2008 45 countries have introduced biometric passports. 100 million have been issued globally

Sources: Identity and Passport Service, US Government