



**RFID**protect<sup>SM</sup>

case studies 2011

[www.rfidprotect.co.uk](http://www.rfidprotect.co.uk)



## Case Study # 16:

# US Passports now have foil linings - why?

*RFID Journal* recently reported that all new generation US e-passports will have a protective foil lining inside their covers.

Why you may well ask?

The logic is simple – the foil provides an effective barrier, or shield, that protects against unauthorised access to sensitive passport information contained within the RFID chip.

(In many European countries, including Britain, passports issued since 2006 have embedded RFID or 'contactless' chips containing information about the passport holder.)

With this new improvement, US passport holders would have to have their passport open all of the time for it to be traced or intercepted. This development is clearly terrific news for American citizens!

But it's not such a bright outlook for other countries that have been slow to adopt foil linings.

Of course for UK citizens there's a simple – and 100% effective – solution until Britain catches up with the States and issues new generation 'foil lined' e-passports. RFID Protect supplies a range of shielding products for British e-passports and is law enforcement partnered so you can be sure of an effective solution and decent customer support.

By placing your e-passport within one of RFID Protects' shielding sleeves, wallets or holders there is no way on Earth anyone is going to scan your passport data remotely.

In fact – it's like giving your passport its own portable firewall!

For more information visit us at:

<http://www.rfidprotect.co.uk/products.html>

Author: RFID Journal / Contactless | Circa 3 August 2011

1: <http://contactless.wordpress.com/2011/08/03/us-passports-now-have-foil-linings-we-wonder-why/>

## Case Study # 17:

# BlackBerry – erasing your smart card data?

News has come to light that *BlackBerry* mobile (cell) phones pack more of a punch than perhaps their designers had bargained for! It seems that the devices can emit an Electro Magnetic Pulse (EMP) when in use that's so powerful it can wipe the data from certain smart cards when in close proximity; (in the main hotel passes and e-gift cards are at most risk). This can be really frustrating if you find yourself locked out of a hotel room after hours!

The good news is that most credit, debit, ATM and ID cards remain unaffected by this phenomenon. Also, by placing e-gift cards or hotel passes within a RFID protective shield there's no problem keeping your *BlackBerry* mobile in the vicinity of these items.

*Newbie.com* has conducted extensive research into this issue, providing the following useful thoughts:

*"...my testing provides strong evidence – if not irrefutable proof – that a cell phone in a holster/case with a magnetic latch [or a cell phone alone [without its holster/case], can damage a gift card."*

*"...this testing strengthens my belief that a cell phone with [or without a holster case] can probably damage a hotel room key card."*

Sources: 1. <http://newbbie.com>  
2. [Contactless.wordpress.com](http://Contactless.wordpress.com) | 29 July, 2011

<http://contactless.wordpress.com/2011/07/29/blackberry-mobile-phones-implicated-in-erasing-smart-card-data/>

**RFIDprotect**

[www.rfidprotect.co.uk](http://www.rfidprotect.co.uk)



## Case Study # 18:

# Eavesdropping attacks on RFID devices

An extraordinary academic paper, with its practical experiments, presents actual 'proof-of-concept' eavesdropping attacks across a range of RFID enabled devices.

The author, G.P. Hancke (of the British-based *Smart Card Centre / Information Security Group* at University of London), demonstrates how he implemented successful attacks on the three most popular High Frequency (HF) standards: ISO 14443A, ISO 14443B and ISO 15693.

What some may find particularly disturbing is that in each case Hancke not only describes the equipment needed to execute an attack, but also how an effective RFID receiver kit can be constructed for less than £50.

*"Even though the self-build RF receiver did not achieve the same results as commercial equipment – it does illustrate that eavesdropping is not beyond the means of the average attacker",* says Hancke.

Read the full PDF report here:

<http://www.rfidblog.org.uk/Hancke-RFIDsec08-Eavesdropping.pdf>

And then protect yourself against unauthorised 'contactless' eavesdropping at:

<http://www.rfidprotect.co.uk/products.html>

Original source: <http://contactless.wordpress.com/2011/06/11/eavesdropping-attacks-on-high-frequency-rfid-tokens/>

From an article by 'Contactless' | 11 June 2011

**RFID**protect

[www.rfidprotect.co.uk](http://www.rfidprotect.co.uk)



# Contacting us

Business hours are 9:30am to 5:30pm GMT

For further information:

T: +44 01234 772632

E: [sales@rfidprotect.co.uk](mailto:sales@rfidprotect.co.uk)

© Alchemy Creative Solutions Ltd., 2009-2013. All rights reserved.

This document is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this document, or any portion of it, may result in severe civil and criminal penalties.

Whilst every effort has been made to ensure that all third-party 'active links' within these case studies were fully functional at the time of first publication, we cannot accept liability for subsequent failure thereafter.

Furthermore, the facts and quotes in these case studies are gathered from information already in the public realm, and from third-party sources believed to be dependable. Alchemy Creative Solutions Ltd (RFID Protect) is unable to guarantee the accuracy, adequacy or completeness of any of the facts, specifications or claims made. We cannot be held responsible, or liable for, any errors, losses or omissions, or for the results obtained from the use of such information.



