What's so smart about smartcards?

Smartcards are simply microcomputers embedded in plastic, with roughly the same powers as a PC of the mid 1970s. Unlike magnetic stripe cards, a smartcard can tell what's going around it, and thereby resist a range of attacks. Smartcards can be programmed with a variety of sophisticated security features and privacy enhancements. They can act as *intelligent proxies* for their owners, as follows.

They can tell what type of reader or application is trying to gain access

Smartcards feature layered security mechanisms. In addition to often using a PIN to unlock it, a smartcard can also tell what type of reader or software program is trying to talk to it. The card can restrict access to specific areas of memory, so that e.g. business applications cannot access government related areas, and vice versa. A 'dumb' reader is not necessarily able to read all data from a smartcard.

They can tell how they're being used

A smartcard can monitor itself, to detect misuse without having to "call back to base". Smart credit cards for instance automatically track daily transactions, and flag a problem if the cap is reached. Health smartcards could similarly detect prescription shopping, without having to data-mine all innocent transactions.

They can check complex Internet security codes

A key reason why phishing and pharming are so successful is that most humans are unable to manually double-check the SSL master codes, root certificates, IP addresses and so on that underpin Internet security. Smartcards can be programmed to 'dig deep' into the security of net banking sites, government portals and so on, to detect rogue sites before its too late. They are the ideal means for Internet sign on.

They can manage multiple customer numbers

It is best for consumers' privacy that they are known to different systems by different identifiers, thereby keeping their different relationships separate. Smartcards can save multiple identifiers just as SIM cards hold phone numbers. Even better than that, smartcards can cryptographically "seal" each identifier, so that it cannot be copied or counterfeited.

Is it rocket science?

Many consumers remain concerned and confused about their privacy and the possibility that smartcard schemes might be doing something covert. To evaluate these issues properly requires just a little understanding of the technology. Most laypeople actually know quite lot about how their mobile SIM cards work, which can be instructive:

- Smartcards and SIMs both have PINs; if a wrong PIN is tried too many times, the chip locks up, and a PIN Unlocking Code (PUC) is required. If the PUC is abused, the chip shuts down permanently.
- Smartcards and SIMs both save personal data to secure non-volatile memory. Only cardholders can write to the SIMs. The chips are private; card scheme owners and mobile network operators are not able to routinely read their customers' chips.
- Smartcards and SIMs can tell what types of system they've been plugged into. This is how "SIM lock" works, a security feature that prevents certain SIMs from working when swapped between handsets.

This is not to say that smartcards are perfect, or that they don't bring certain privacy and security issues. But they can be viewed for many purposes in much the same way as mobile phone systems, and can be designed, administered and regulated in comparable ways.

Privacy benefits of smartcards

In summary, smartcards can be programmed to deliver the following privacy and security enhancements:

- Decentralise customer identifiers, literally keeping them safe in peoples' wallets, away from databases and call-centres
- encrypt each of an individual's various identifiers, to protect their privacy
- run private off-line security checks inside the chip, to catch fraud without having to aggregate and data-mine all innocent health data
- log users onto secure websites, protecting them against hacker sites
- check the veracity of e-mails, to against phishing and spam, which actually represent the most serious threats to privacy today.