# Over the Water -- The View from the UK

David G.W. Birch
Director, Hyperion
8 Frederick Sanger Road
Surrey Research Park
Guildford Surrey GU2 5YD, UK

daveb@hyperion.co.uk
Where people, networks and money intersect.......Consult Hyperion
http://www.hyperion.co.uk
info@hyperion.co.uk

## Column Two: Get Smart

At the 1996 RSA Data Security Conference in San Francisco last month, John Gould of Mastercard International quite rightly called smart cards the "link between the real world and the virtual world". Why should this be?

This first thing to note is that smart cards are computers: one shouldn't be misled by the card metaphor and see them as analagous to the familiar plastic card in one's pocket. Perhaps a more accurate (but more clumsy) name might be 'sub-personal computer', or subPC. Three or four of these subPCs in your wallet should be sufficient to support all of the applications needed by people operating in the new economy.

A subPC which identifies the holder could easily take the place of drivers' licences, access cards, house keys and so on. Another subPC which accredits the holder can take the place of Visa and Mastercards -- it would still link to their networks, of course -- while another might hold anonymous bearer instruments such as cash or frequent flyer miles. Yet another might be used to sign e-mail messages and authenticate incoming mail.

Looking at the banking and finance sector in particular, the assumption that consumers will be using smart payment cards is reasonable. They have already become the preferred implementation for payment systems because of pressures from:

- Consumers, who use plastic cards already and are very familiar with the card format.
- Banks and payment schemes, who are attracted by all of the familiar characteristics of smart cards: security, portability, capacity and so on.

Advances in cryptography have made it easy for a PC (or a subPC) to generate information with 'digital signatures' that are much cheaper to legitimately produce than a note but far harder to counterfeit. Digitally signed information can thus be used as money (electronic cash, or ecash) that is more secure than coins or paper money and can be stored, exchanged and transported at a fraction of the cost. Money isn't the only use for cryptography in cyberspace, however, and smartcards and do a lot more.

The utility of smart cards with respect to cyberspace is that they provide a secure place for a person to store the cryptographic keys that are needed to produce digital signatures and are just as portable as any other form of key (e.g. house keys, car keys, plastic card hotel keys). It is in this role that smart cards provide the crucial link between the 'real' world and the 'virtual' world.

The security of smart cards makes them ideal for use in conjunction with the ubiquitous and insecure (and therefore cheap) information superhighway. The Internet, an early incarnation of a superhighway, has already attracted the finance and banking community as a low cost way of communicating with customers but the provision of real financial services requires a secure infrastructure. Widely available smart card reader/writer devices (henceforth referred to as "card readers") will provide this infrastructure with no need to change the communications infrastructure. In other words, it will be smart cards (not telecomunications) that give us the secure marketspace.

The use of smart cards is well advanced in Europe. In France, home of the smart card, all payment cards have been smart for some time and most other European countries are following. In the UK, all payment cards will be smart by 1999 and APACS has recently announced that it has chosen Delphic Card Systems and Schlumberger to supply smart cards for testing in 1996 with roll-out to the public beginning with a pilot in 1997. The UK cards will comply with a specification called UKISv.1 which is based on the VIS1.1 specification from Visa.

The UK is an important player: there are more payment cards in circulation (86 million) than any other European country. Nearly four-fifths the population have a credit, debit, ATM or charge card and they make 3 billion transactions annually.

Overall, the world market for smart cards is growing rapidly. The latest forecasts from Gemplus (one of the leading manufacturers in the field) indicate that the world market is expected to reach 4 billion cards in 2000 up from 380 million in 1994 (a 44% average annual growth rate) with bank and loyalty cards growing 71% per annum in that period. With such significant increases in the number of smartcards in circulation, there will be a commensurate increase in the number of smartcard devices.

These figures also show a shift in the installed based from not-very-smartcards (memory-only smartcards) to very-smartcards (smartcards with microprocessors and cryptographic co-processors on board). As the cards get smarter, less and less work needs to be done in devices. In practice, this should mean that it becomes easier for standard hardware and software to use the facilities offerred by smartcards through internationally standard high level interfaces.

In the context of the Internet it is worth noting that many manufacturers already produce smartcard readers for PCs. These are generally of two types: stand alone card readers that connect to a serial port on the PC or PCMCIA (PC card) hardnesses allow users to insert an IS standard smartcard into an industry standard PC slot. PC card harnesses coupled with smartcards can do all of the processing required to interface the smartcard with software running on a PC. Since the smartcard does not need to be inserted all the way into the PC card slot -- it only needs to be inserted far enough to make contact -- there's plenty of spare space in the harness for circuitry to support advanced functions.

What this article is saying, in summary, is that smart card readers will become ubiquitous because smart cards will become ubiquitous: banks, in particular, will be able to use consumers' ready access to smartcard devices to facilitate simple and secure financial transactions in cyberspace.

This issue's quote: "Wealth depends upon commerce, and commerce depends upon circulation". Money and Trade Considered by John Law (1705).