

## EURIM Briefing No 9

January 1996

In the area of I&T (Informatics and Telematics)  
EURIM is a link between Commerce and Industry,  
Parliamentarians, Whitehall and Brussels.

EUROPEAN  
INFORMATICS  
MARKET

EURIM



# SMART CARDS

## THE EU & THE UK - OPPORTUNITIES & THREATS

This Brief identifies:     - commercial and political issues in developing Smart Card applications  
                                  - potential for constructive action by UK and European Government.

The UK has led the way in the exploitation of advanced telecommunications towards the Information Society in Europe.

There is an opportunity to build an equally successful European campaign for the development and application of Smart Cards. Apart from the progress towards the Cashless Society, this technology will be used extensively throughout industry, generating opportunities for those who best use it.

Industry in Europe is well able to exploit such opportunities provided that there is political agreement on the advantages of doing so and agreement on common standards. The UK has technical expertise but there has been too little investment in its supply industries. It may have missed the market for chip and card manufacture and may be behind Continental competitors in applications.

### The issues

The initial cost of any large scale Smart Card application is distorted by the lack of an existing infrastructure to support and service it. Potential sponsors of Smart Card applications, faced with the need for an infrastructure, can better cope with building one to support two or more applications initially, albeit at increased cost, rather than adding applications later when the cost would be much greater. There is clearly a need for an appropriate and agreed common Smart Card infrastructure, but without common standards this will not happen.

Sponsors are unlikely to have the will or resources to develop schemes that are outside their market sector. We can expect incompatible infrastructures to be built in support of diverse and industry sector specific schemes. Apart from duplication of resource there will then be an initial barrier to competition and co- operation across industry sectors, analogous to the historical development of Electronic Data Interchange (EDI) in sector specific and incompatible applications.

Common standards are best agreed between potential vendors prior to investment (see EURIM Brief No. 3). *De jure* standards arrive too late but take account of existing standards in technologies likely to converge whilst proprietary standards ignore this.

Widespread mobilisation of Smart Card Technology into every day use will only take place when common standards, in at least the following areas, are recognised:-

- Identification schemes (of articles, institutions, people)
- Central registration and certification of applications
- Physical characteristics of the card
- Technical architecture of the applications
- Operating system with standard interfaces

Of the above, physical characteristics are adequately (but not necessarily fully) covered by existing *de jure* standards, but there is much to be done in the other areas.

As Smart Card applications increase the need to carry many single use cards could have an adverse effect on consumer acceptance. Suppliers have diverse commercial interests and visual branding is

important. For this reason the consumer is likely to be faced with a bewildering array of cards, even though the technology can accommodate multiple applications on a single card. On the other hand, consumers may feel more comfortable that their personal data is secure where cards are used for one purpose only.

Protection of personal data on a card is crucial. If a card initially handles solely impersonal matters should it be bound by the restrictions imposed on a card with personal concerns, in case such data is added later? Demonstrating adherence to data protection principles where applications with different owners are present on a card introduces new complex considerations.

Does the UK Data Protection Act, being concerned with personal data which is automatically processed, adequately respond to the need to protect personal data on Smart Cards? The Data Protection Registrar has written that "the very existence of an identity card and its supporting database brings a privacy threat" The BMA seeks legislation to make the unauthorised passing of personal medical information into a criminal act. Both are comments of concern at the adequacy of the Data Protection Act where privacy of information on Smart Cards is concerned.

The EU Data Protection Directive, adopted in July 1995 allows several years for nation States to achieve implementation and allows a number of possible derogations. Data users must consider the prevailing data protection requirements in all of the countries where the cards are to be used.

Intellectual Property Rights must be considered in a fair and consistent manner. As in other industries, a balance must be struck between holding IPR too tightly and fair exploitation of innovation. The technology of Smart Cards is well protected by a minefield of patents and licences, mostly held by Innovatron of France. Many of the patents are due to expire within two years and this could lead to a flood of new applications. Meanwhile industry is divided on the issue of whether the current position is restrictive or does in fact focus activity.

## **Opportunities for Government Action**

- Strong leadership is needed now to avoid a vacuum. No market leader can achieve this. There is vested interest at stake. Government interest is needed to mandate the requirement for one set of open standards, to take the lead in the resolution of problems and to pump prime development.
- The EU needs to create a Mandate in the area of Smart Card Standards. It has done so elsewhere, when common benefit was hampered by a lack of standards- for example the EMC Directive. A fast track ad hoc grouping, analogous to the European DVB group would enable rapid development and acceptance of relevant standards.
- A commoditised multi-application smart card operating system (analogous to "MS-DOS") is needed world- wide and would be an important addition to recent ISO standards. The EU should exploit this, together with the new generation of Smart Card chips.
- European co-operation, in the form of cross-sectoral trials should be sponsored in the style of a "demonstrator". This should ensure that, as far as possible, a single infrastructure is built and compatible applications can be combined on cards where this is to the benefit of the consumer. The EU needs to encourage representation of the highest quality on the various standards bodies, redressing the balance between short term profitability and the long term health of its economy.

In the UK, prompt Government action is required, partly as catalyst, partly as marriage-broker, to ensure that industry and commerce are amongst the European leaders in the use of Smart Card applications. Despite the, as yet, unsolved political issues concerning identity and security there is no longer any doubt that Smart Card Technology is another significant step in the current technology revolution. Those that fall behind will undoubtedly lose competitive advantage.

An important long term goal should be the Government sponsored card, setting standards for essentially national applications. It has the potential to be a primer for a vast range of other services and facilities. Technically such a card could provide for Passports, Driving and other Government Licences, Birth Certificates, Social Services etc. Whilst it is likely that political considerations will determine what such a card will actually include, the ability of the card to accept multi-usage, possibly including services from the private sector, enhances the ability to recoup initial investment in it.

Whatever the agreed mix of services on such a card, EURIM believes that this will only be reached via a series of applications migrating gradually to such a card. In time, with good experience, public anxiety over data security issues will eventually be removed.