Computer Science Part II 2002
Paper 7 Question 5

JAL E-Commerce

(E-commerce question)

f. A new start-up that proposes to develop an electronic wallet, a device that can cryptographically hold electronic money, data, credit card numbers etc. Such a device might be included in a mobile phone, for example..

   a. Explain how network externalities affect the introduction of such a device; [5 marks]
   b. Explain some of the legal and regulatory issues affecting such a device; [5 marks]
   c. Sketch out the processing and infrastructure that would be needed to support such a device; [5 marks]
   d. Would such a device increase overall security? [5 marks]

Explain how network externalities affect the introduction of such a device; [5 marks]

A network effect is where the utility of something, such as e-mail or the telephone, increases with the number of users. In economics this is called an externality, as it is an external non-price factor affecting the product.
Metcalfe's law predicts that the usefulness of a network is proportional to the square of the number of users. In practice this is more likely to be an S-shaped curve, with a rapid switch from few users to the majority of eventual users.
In this case there is a chicken-and-egg effect: shops and merchants will not offer facilities to use the device unless there are enough customers with them; customers will not use them unless a sufficient number of shops offer the facility, and there is a real incentive to change from existing credit cards etc The market can be primed by giving away, or even paying people to adopt the technology, but this is both expensive and uncertain. . The Mondex experiment, for example, effectively failed at this hurdle. Associating the device with a cell-phone may be one way to quickly achieve high penetration, but this would require the co-operation (and payment to) the cell-phone companies. In Hong Kong, the Octopus card used originally for the Rapid Transport system, is now used as a stored value card for other small purchases. In this case it is unclear if the benefits of the increased security and convenience, assuming there are any, outweigh the cost of changeover.

Explain some of the legal and regulatory issues affecting such a device; [5 marks]

Consider the following transaction:
A user goes to a shop, and purchases some goods, authorising their wallet for payment and putting it in the shop's reader, or equivalent, for example via Bluetooth or IR..
The reader extracts the user's credit card number (or electronic money) and makes a conventional credit card purchase.
Here there need to be contractual relationships between the user and the wallet service, and the shop and the wallet service for the reader(or equivalent), and between them and their respective banks and/or credit card (etc) providers.

-

As a purely storage device, it is unlikely that the provisions of the Financial Services Act will apply. However if service, such as electronic currency, or money deposits are added, then FSA and other banking money laundering and, if appropriate, credit. regulations will need to be considered.
The Data Protection Act will apply, The usual sale of goods regulations, and if sold via a web-site the distance selling directives will apply. Recent legislation relating to electronic signatures might apply, depending on how the device is used.
If things go wrong, or the device stolen, some form of insurance may give customers re-assurance

Sketch out the back-end processing and infrastructure that would be needed to support such a device

The simplest implementation would allow the user to enter, for example via the mobile phone keypad their own information, such as a credit card number and associated PIN. At the store the device interfaces (and this is the tricky bit) with existing till and credit card systems, either via a special reader, or via some secure communication link The adoption by stores, and integration to till systems will be the biggest stumbling block to integration. The assistance and co-operation of the credit card and banking providers would be important. Getting universal standards defined and accepted is both time-consuming and expensive.

Different implementations will be needed depending whether the device acts as a stored value device (such as pre-paid telephone cards), or as a holder of anonymous electronic money, such as Chaum's e-cash scheme, or simply a secure repository of credit card data. More complication is introduced if value, such as electronic money, can be stored, although this could be done by an extension to the existing phone-card and top-up mechanisms for pre-paid phones.

A secure archival system may be required, so that if a user loses the device or the battery runs out, data can be restored. Although communication to and from the archive system can be secured by straightforward systems such as SSL, ensuring the archival storage remains secure is difficult, and may involve positively vetting staff and contractors. A strong identity scheme, such as password and/or biometric identity may be needed. If value is stored, additional checks will be needed to ensure double spending, for example a time stamp on transactions, cannot happen. Strong audit data will be needed to verify queried transactions, as will methods of repudiation, for example in case of theft of the device. .

Integration to external systems, such as Microsoft's .NET (e.g. Wallet. Passport identity functions, network based archival storage) is desirable.

In any case fulfilment and customer care systems (including a customer database) will be needed.

e. Would such a device increase overall security? [5 marks]

If anything the device will decrease security. The risks inherent in credit card (or other payment) mechanism remain, especially for distance purchases, while new potential vulnerabilities are introduced.

Issues include

- Authentication – since access to value is mediated by the user authentication, it needs to be comparatively strong, such as biometric or long password, which may detract from the convenience of using he device
- Tamper resistance: Since information is held internally, stealing the device should not give access to the information or value
- Logging and non-repudiation: Provision against false claims of transactions
- Revocation: for example disabling stolen devices
- Archiving and restoration

In any case, the biggest vulnerability is likely to be fraud by the merchant or by staff internal to the system, which the introduction of this device does not affect.