Oyster – Smart Card Payment Systems on the London Public Transport Network

Background
The Oyster smart card for public transport in London is one of the largest and most complex smart-card enabled ticketing projects of its kind in the world. It was completed in 2004, almost six years after the contract for the Finance Initiative (PFI) contract was awarded to TranSys, a consortium of companies led by Electronic Data Systems (EDS) and Cubic Transportation Systems (CTS). TranSys and its partners have responsibility for all aspects of the Oyster project, including: design, installation, day-to-day operations and ongoing maintenance.

Oyster cards are credit card-sized plastic cards which are loaded with Philip's Mifare microchip technology. Philip's Mifare is the world’s leading smart-card manufacturer with an estimated share of nearly 80% of the global public transport smart-ticketing market. TranSys at first estimated that it would need to produce in the region of three million cards. However, the popularity of the Oyster with London Transport (LT) customers has proved so great that this initial estimate has had to be radically revised. Upwards of ten million Oyster cards have now been issued, while approximately five million are in regular use on the network.

Uses
Oyster was incrementally introduced for several types of travel, including weekly, monthly, annual season and pre-pay tickets at the end of 2002. Firstly, LT staff were provided with cards as part of the free travel allowance that comes with their jobs. Upon its launch the ex-Mayor of London, Mr Ken Livingstone was moved to comment: "We are at the start of a new era of ticketing in London. The travelling public can look forward to having to queue less for tickets and to moving faster through ticket gates at underground stations and on to buses." Since 2002, the card has been released to the general public who can now use it for all types of season ticket and for pre-paid journeys.

Features
Oyster offers significant advantage to passengers, including the choice of being able to purchase and top up their smart cards at non-station outlets, such as newsagents, and through media channels such as the internet or telesales centres, and of having the card revoked if it is mislaid or stolen so that it cannot be used by anyone else.

TranSys has worked hard to build on the success of the earliest Oyster system implementation and has incrementally improved the system so that it now has the following:
new touch-screen and multilingual ticket machines that accept payment by credit and debit cards, as well as cash in note or coin form
- 15,000+ Oyster card readers on LU ticket gates and on entry points to buses
- smart card technology in 255 Underground stations and 28 national rail stations served by LU
- Oyster compatible ticket machines at 2300 local ticket outlets
- a PrePay ticket that allows customers to credit money on to the card
- An online payment system ([https://oyster.tfl.gov.uk/oyster/entry.do](https://oyster.tfl.gov.uk/oyster/entry.do))
- Networked payment terminals in newsagents across the capital
- An auto-top-up scheme that deducts funds directly from a passengers bank account by direct-debit

**Scope**

Oyster is valid for journeys on London Underground, London Buses, national rail services servicing London stations, the Docklands Light Railway and the Croydon Tramlink. Some rail services which serve London, such as inter city services, and the Heathrow and Gatwick Express airport services are currently not covered by Oyster. However, the current Mayor is in negotiation with several rail companies to allow Oyster cards to be used for all rail journeys coming in and out of London.

Of all the Oyster options available, the seven day travelcard has turned out to be the most popular option with up to half-a-million sold on weekly basis.

Oyster is currently available for travel only. However, there is already research into how it may be extended to include payment for municipal services such as car parking, leisure centre services, libraries, etc.

**Technology**

Oyster cards work through an aerial and a tiny microchip built into the (smart) cards themselves. This microchip acts as a data storage device, storing data about the ticket type purchased, card ownership and current credit. The aerial is used to send and receive data when a card is positioned in proximity to a card reader on a ticket machine or ticket gate. When this happens, a signal flows through the aerial and data flows from the card to the reader and back again. Communication is by radio signal and an individual transaction takes less than 0.20 of a second. Data can be read from the card by the card reader or can be sent to the card. Oyster cards do not have a battery. For power, they use a ‘built-in inductor’ that captures part of the incident radio-frequency interrogation signal from the card reader and employs it to charge the card for as long as it takes to conduct a transaction.

The relationship between Oyster cards and the central Oyster database is quite complicated. Account data is held electronically on individual cards rather than on the central database. The central database does, however, keep a record of individual card use. It receives this data from ticket machines and ticket gates as customers navigate the transport system. The main database also holds data on credit and tickets bought online. Records of tickets or credit bought online are stored in the central database ready to be loaded onto a customer’s card when he or she passes through a pre-selected barrier.
Oyster cards are ‘contactless’ cards. These cards require only close proximity to a reader to complete transaction. This type of card is frequently used when transactions must be processed quickly or hands-free. Although, Oyster is contactless and can remain in its plastic wallet, it still has to be placed against or right next to the card reader for it to work. This inevitably reduces the efficiency of the system in comparison to other truly contactless’ systems, which in some instances can function with the card a significant distance from the reader. One of the problems of Oyster has been passengers causing a hold-up at barriers by not touching the card against the reader or touching it at the wrong angle.

Security
It is claimed that smart cards are a very secure way of storing information and TranSys assert that Oyster users, "...can be sure of the security of the data held on their cards". Access to the data is possible only by using secret codes that are specific to each card and is only possible by devices permitted to process the cards.

"These cards are very difficult to break into, making them very secure. In the unlikely event that a card has its key broken, then the system, and all other cards, will remain secure. Information from the system is analysed regularly to detect possible security breaches and ensure that the integrity of the system is maintained," says TranSys.

Despite TranSys’s claims to the contrary, there is still anxiety that the security of the Oyster card system could be compromised. Each Oyster card is uniquely numbered, and registration is required for monthly or longer tickets. Card usage data is stored on the card and also on the central database for up to 8 weeks. Usage data is tracked by TFL information systems in order to make sense of how the system is running. However, usage data is increasingly being used by external agencies, especially law enforcement agencies. Indeed, the police have used and continue to use Oyster card usage data as an investigative tool. For example, between August 2004 and March 2006, records show that the Information Access and Compliance Team at TFL received approximately 450 requests from the police for Oyster card records. Of these requests, approximately 400 were allowed.

Security concerns regarding Oyster have been heightened in recent months as new uses for the card have been proposed. The proposal that has caused so much concern is the use of the Oyster card as e-money,
a kind of debit card light. Apart from concerns regarding the costs of setting up the required infrastructure for the scheme, security experts believe that storing exchangeable currency on the card will make them an attractive target for criminals, who in the past have ignored them as they hold no transferable value. “If Oyster can suddenly be used to purchase goods”, argues Graham Mather of Barrier One Security, “then you will see the rise of attempts to hack and clone the cards in the same way that criminals currently put so much effort into hacking and cloning debit and credit cards.”

References and additional reading:

*Easing travel in London’s congested public transport network,* ‘MIFARE.net’
http://mifare.net/showcases/london.asp

*Oyster data use rises in crime clampdown,* March 13 2006, ‘Guardian Unlimited’
http://www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation

Oyster, Transport for London
https://oyster.tfl.gov.uk/oyster/entry.do

http://www.spy.org.uk/spyblog/2004/02/foiling_the_oyster_card.html