Global Information Assurance Certification Paper

Stephen Burns

SGEC – Version 1.3 - 2002

Version 1.0 - 21 March 2002

1. Synopsis

Payments are the life-blood of commerce. With the shift to electronic means of doing business it is logical that payments will follow the same route. This has been the case as electronic means of making payments have rapidly evolved since the first computers were installed in the banking and finance system. However, initially, the electronic payment systems were under the tight control of the banks with bank personnel being the payment initiators. Even with the introduction of ATM's and EFTPOS systems, tight control was maintained over the banking networks and how payments were initiated, this requiring the physical presence of plastic magnetic stripe cards with PIN entry to authenticate the owner.

The introduction of electronic token and Web based payment methods has altered this situation, as access to the Web is uncontrolled and authentication of the payment initiator relies solely upon electronic means to initiate and authenticate the payee.

This paper discusses and highlights 1) unique characteristics of the technologies of the ecommerce world compared with traditional payment systems and 2) the way these characteristics may be exploited to compromise payment systems. An Appendix provides a table summarising the desirable attributes of a payment scheme.

2. Brief Glossary

Card Money [6] – are systems that employ tamper-proof hardware devices (i.e. smart cards) to store monetary value. The value is physically transportable in the same way as cash.

Disintermediation – where one party (e.g. a bank) becomes separated from their customer due to another party, such as a payment gateway provider, interceding in the bank's relationship with that customer.

Jurisdiction –the territory within which power, normally based upon specific laws or regulations, can be exercised. So the state of California is a separate jurisdiction from the nation of Vanuatu.

Mondex [3] - The Mondex scheme is the Mastercard/IBM developed smartcard operating system that has as one of its features card-to-card exchange of value called Mondex Value Transfer Protocol (VTP).

Network Money [6] – is stored value transferred over open networks, namely the Internet. It can be implemented in "software only" form, but unlike Card Money requires a PC to participate in the transaction via the Internet. Network money's primary purpose is to buy goods and services over the Internet.

Payer – the party making the payment.

Payee – the party receiving the funds resulting from the payment;

Non-repudiation – providing proof of the integrity and origin of data (e.g. payment request) that cannot be refuted.

3. Characteristics of Ecommerce Technologies

The following high level principles are aspects of payments impacted by the new ecommerce technologies. They will have an increasing impact upon security of payments:

- Ease of automated processing;
- Immediacy of result;
- Openness and accessibility of payment processes;
- Loss of collateral information;
- Globalisation; and
- Emergence of new business models.

3.1 *Ease of Automated Processing*

A payer can now cheaply and easily automate the generation and processing of multiple payments with minimal effort. Previously, the dependency upon banks to handle most payments and the lack of a cheap, ubiquitous communications technology made automation of payment processes expensive and difficult to establish.

3.2 *Immediacy of result*

Payment immediacy occurs because automation and the ability for the intermediate systems and providers to process payments in real-time. With the more manual, paper-based systems there was always a time delay due to the requirement for human intervention in the process.

3.3 Openness and accessibility

The availability of cheap computing and communications technology and the appropriate software enables small enterprises and individuals to access or provide a range of payment services that were previously only available to large organisations via dedicated networks or the transactional processing units of banks.

3.4 Loss of collateral information

*T*he new technology dispenses with, or alters, *collateral information* accompanying transactions. This information has traditionally been part of the transaction, and has been relied upon by the transacting parties to validate individual payments.

Collateral information can be defined as information:

- which is not essential to the meaning and intent of a transaction;
- which is typically incidental to the nature of the communications channel over which the transaction is conducted; but nevertheless
- provides useful contextual information for one or more of the parties to the transaction.

Collateral information can include many things ranging from tone of voice in a telephone call to the business cards and letterheads and apparent authority of the person with whom you are dealing.

Now that information is received only via a single channel (such as an electronic message) new processes need to be put in place to support and reinforce payments in the same way as manual systems.

3.5 Globalisation

Globalisation, or the minimisation of geographical factors in making payments, has been an obvious aspect of the new payments systems. Its affect is upon areas such as size of the payments marketplace, uncertainty as to legal jurisdiction in the event of disputes, location and availability of transaction trails, and the ability of a payment scheme to rapidly adapt to regulatory regimes imposed by one country by moving to another.

3.6 New business models

New business models are being developed to exploit the new payment technologies, in particular to address or take advantage of the disintermediation of customers from traditional payment providers such as banks.

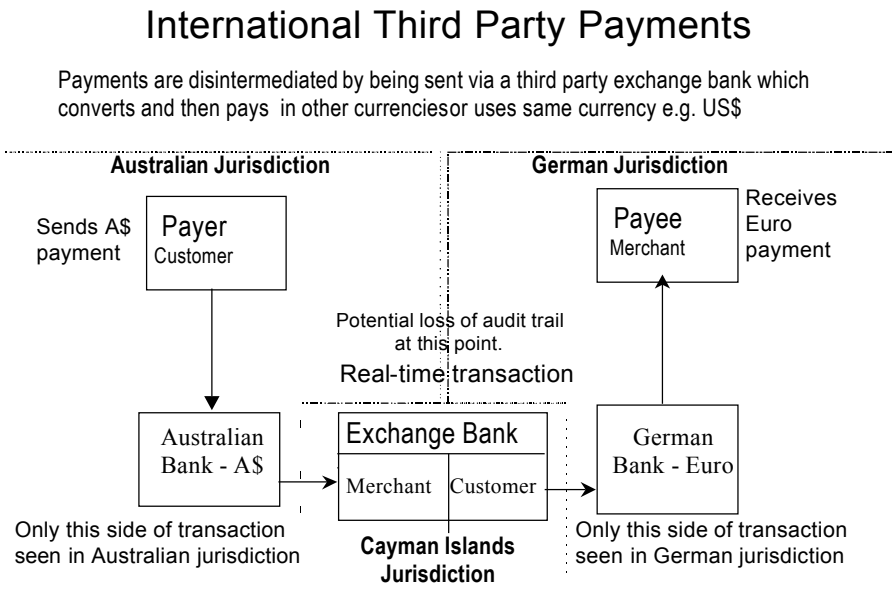
In this context, disintermediation is where the technology enables a third party to intervene between the customer and the banking system, effectively transferring the customer's trusted relationship with the bank to the new party.

4. Impacts upon Payment Systems

This section provides examples of the impacts posed by the new technologies to traditional payment systems.

4.1 International Third Party Payment Schemes

The use of third party agents for payment facilitates loss of collateral information during transmission between 2 jurisdictions resulting in loss of payment audit trail.



There is disintermediation of the payer and payee by the third party.. In this case the third party is an exchange bank in another jurisdiction. The loss of collateral information (including keys parts of the audit trail) occurs because:

- In Australia the audit trail indicates the source as being an Australian customer paying a Hong Kong based merchant via their bank;
- In Germany the audit trail indicates the source as being a Hong Kong based customer and the destination a German based merchant with no information linking that merchant to the Australian payer.

This can create problems should payments go astray and the payer needs to start legal proceedings to recover the funds, or where the payments are being traced by law agencies because the funds are illegal.

The above system uses the normal payment system for ultimate settlement. The following are variations which may or may not transact through the normal payment system.

4.1.1 International Remittance Corporations

Continuing globalisation has already facilitated underground banking with the emergence of remittance corporations such as Western Union's money transfer facilities and American Express's "Moneygrams" which can be cashed at their offices anywhere in the world.. These operate in the following manner:

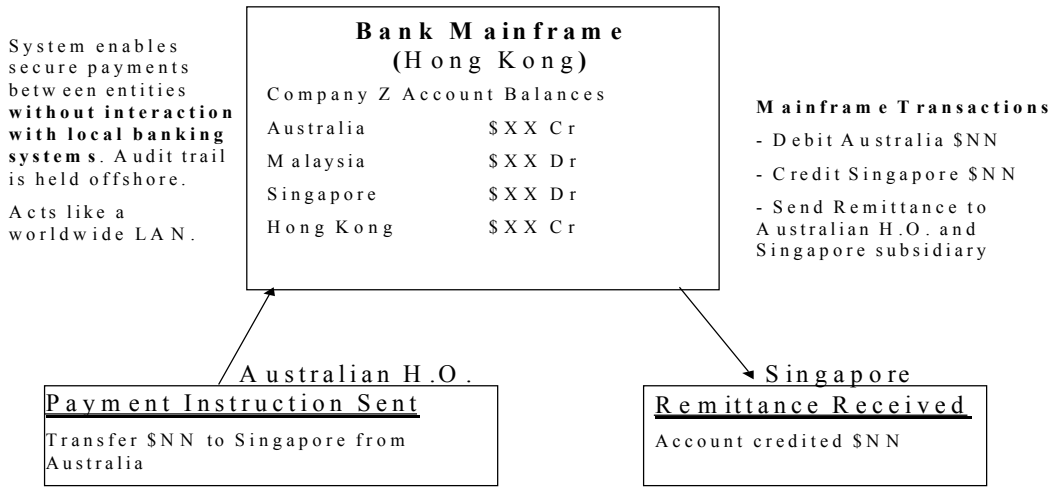
- The payer provides funds to the corporation in one country and the payee address and details;
- The corporation aggregates the payment transactions and transmits the value via the normal banking system to the accounts of Head Office which is most likely set up in a third country;

- Transactional details are transmitted over proprietary networks, fax/telephone, secured email etc to the Head Office;
- The payment instructions are then transmitted from Head Office to the payee's country where funds are provided to the payee in the local currency from the remittance corporations local accounts.

In this process we get aggregation and disaggregation of funds in a central corporate account which, along with the high incidence of false names being provided by the payer and the difficulty of obtaining those details, result in the loss of any audit trail (and collateral information) for such transactions.

4.1.2 Global Bank Internal Transfer Systems

These systems are of concern for specific jurisdictions due to their ability to enable payments without going through banking system of the countries in which the payment is initiated.. This style system looks as follows:



The value is transferred internally within the sponsoring bank's computerised accounting systems and may never be reported as an international currency flow, circumventing international Money Laundering reporting arrangements

Such systems have been set up for perfectly legitimate business reasons, prime of which is enabling multinational organisations to manage cash flows between their various country offices.

Issues arising from these types of systems include:

- How to stop such arrangements to be used for "smurfing" (i.e. global hopping of multiple small payments to be aggregated in a low tax country). This system appears to enable even large payments to be processed as the amount of each payment is not reported to any authority so there is no need to set the payment amount below a specific detection limit.
- When remittance information is transmitted back to the payment initiator, how would you prevent its destruction to cover illegal activity.

- How to address the reporting of payment of employees working in one country by depositing funds into overseas accounts so that there is no apparent or reduced domestic income.

4.2 Timing and Immediacy

The following highlight the impact of immediacy in payments and the importance of determining the exact timing of events.

4.2.1 Coerced Payments

The advent of home banking services based upon dedicated, proprietary, Bank-supplied PC software that enable anyone-to-anyone international payments has now been accelerated by the introduction of Internet based home banking services.

This raises the risk of criminals physically coercing people at home into initiating large payments via their desktop system. This has already been a problem but will become worse with international person-to-person payments initiated via the Internet.

This vulnerability can be countered by enabling overseas payments aver a certain aggregated amount only upon a personal visit to the local bank branch, including a 12-24 hour delay in which the transfer is revocable and establishing false account details that immediately alerts the bank that a problem has occurred but will show as a successful payment.

4.2.2 Timing Fraud

Timing fraud can be perpetrated because, currently, there is little use of trusted third party to provide time and date stamping for payment transactions (or even contracts). We normally assume the date and time provided by the system is accurate.

A timing fraud scenario is:

i. The perpetrator transmits a digitally signed and time stamped contract for payments (i.e. payment advice) or good and services that appears to be non-repudiable.

ii. Once the goods and services/payment are delivered the payer then deliberately compromises the private key used to sign the payment.

iii. From that point on all transactions using the key are illegal and invalid as they can be repudiated. The payer then claims that the contract/payment is invalid due to the time and date stamp having been manipulated to appear as if the transaction occurred before the key was compromised.

iv. If it cannot be proven that date and time have not been changed, then the transaction may be declared invalid. This is particularly powerful where a contract is involved.

A significant step to counteract this type of problem is the introduction of a trusted third party that can provide a digitally signed date and time stamp. Refer [9] for brief overview on digital notarisation process.

4.3 Facilitation of Underground Banking

Underground banking [4] completely bypasses the normal payment system controls and audit trails facilitating money laundering, tax avoidance [5] and funding of illegal activities. Underground banking is known by several names including hawala (meaning trust), Fei Chien (meaning flying money) and Chop Shop. They operate via a system of trusted intermediaries in various locations and are normally operate within specific ethnic or language groups. Such services have been available for many years but are now much more viable due to the accessibility of the new technologies and the trend towards globalisation.

There are two main types of underground banking transactions:

- **Trade transactions** - where the invoiced charge for goods is inflated in order to transfer price funds to the seller, who then strips off the extra funds, takes their margin and distributes the funds to the nominated recipient.
- **Non trade transactions** - a trusted party in one country is provided the funds and recipient details. They contact an agent in the other country who, upon promise of settlement, contacts the recipient and pays the funds (less a commission). As this is a two-way flow of funds, the net of the amounts transferred between the two parties is normally much less than the total of the aggregated. Settlement of the difference occurs every couple of months with arrangements are made for funds to be transferred to the party who is the net creditor.

The way new technologies could be used to assist the operation of these schemes include:

- Secured email can be used for the transmission of payment instructions between agents in different countries providing a high level of immediacy, security and assurance to the recipient agent that the transaction is genuine. Currently fax or telephone can be intercepted enabling analysis of the values being transmitted but secure email would remove this capability.
- Stored value cards, such as Mondex [3], could be used in several ways. The Mondex scheme is the Mastercard/IBM developed smartcard operating system that has as one of its features card-to-card exchange of value called Mondex Value Transfer Protocol (VTP). This can be used to settle
  a. periodic payment of any net debt between agents involved in underground banking can be done by exchange of value between Mondex cards carried by the scheme operators. All that is required is a simple terminal that can be wiped of all audit trail information after completion of the transaction. Or, alternately,
  b. transfer of value could be done simply by physically transporting a charged Mondex card or cards to the respective payees. So long as it is one of the internationally supported schemes, value could be obtained anywhere particularly if is denominated in US$ or Euros. Such cards could even

circulate without ever having value removed. This depends upon the restrictions placed upon use of such systems worldwide.

Card to card transfer of value is the reason that Germany has banned Mondex from operating there as it is seen as an unregulated source of foreign exchange.

4.4 Disaggregation/Aggregation (Smurfing)

Smurfing in the context of payments involves the generation of multiple small payments that individually, do not exceed local jurisdictional rules for external payments, but in total when deposited in the ultimate payee account, exceeds significantly such rules and regulations. Motives are money laundering, payments for illegal activities or goods, and tax avoidance.

Automation of payment instruction initiation has facilitated this process, with accessibility of epayments via the Web allowing individuals to make such payments without going through traditional international electronic payments channels such as SWIFT [6].

4.5 Interface Attacks

4.5.1 Simulated Online Approval Attack

Unlike ATM/EFTPOS services where there is a tightly secured link direct to the bank, Internet payments are susceptible to attack due to the accessibility and openness of the Web. In this attack, the perpetrator compromises the merchant's Web link to their online payments gateway. Once compromised any request for payments approval will always be positive regardless of whether funds are available or not. Any authorisation from the bank, which in turn would initiate delivery of the good or services by the merchant. It would only be much later that reconciliation of the bank accounts to the online merchant facility detected any discrepancy. Purchase of goods using false credit cards/debit cards becomes feasible once the merchant link to the bank has been compromised.

4.5.2 Remote PIN Capture Attack

As traditional payments channels have become Web enabled, sophisticated techniques to capture logon IDs and PINs have evolved based upon using installation of PIN capture software on the users PC.

An example of such software are the DIRT (Data Interception by Remote Transmission) [1], Sub Seven and B02K trojans. They enable remote logging of keystrokes and capture of payments details and are installed via activation email attachments or logging onto an infected Web site. This information is automatically emailed or transmitted to the attacking party, enabling exploitation of the various services.

4.6 Vulnerabilities in Stored Value Systems

Stored Value Cards (SVCs) are the least understood of the new technologies and so have the greatest potential for exploitation. It is important to make a distinction

between electronic payment systems based on smart cards, and stored value systems (including stored value card systems).

Stored Value allows something of value, such as cash, points, phone time, etc. to be placed on a delivery instrument. Traditional paper-based examples have included gift certificates, merchandise credits, loyalty cards, membership cards, and even simple punch cards. For further reading on SVC's refer to [8].

An important distinction to make between different stored value schemes is to consider technology which stores value on smart cards (Card money) as opposed to that which creates stored value *for the Internet* (Network money*)*. In future these two forms of stored value will probably merge, but it is also likely that some systems based on smart cards only, and some used only on the Internet, will co-exist.

4.6.1 Exploits

Since stored value systems are not in widespread use today, any threats discussed here have to be seen in the context of the future development of this market. Any of these characteristics could be exploited.

i. **Direct attacks** could be done by breaking system security measures, or by attacking user or operator facilities (theft of cards with loaded value, tampering with terminals, etc.).

ii. **Levels of traceability** of transactions in stored value systems have different implications, but SVCs could be designed to provide reduced traceability of transactions to conduct illegitimate transactions without being easily traced.

iii. **Transferability of value** as a characteristic in stored value systems could be used to further reduce the audit trail, by using a succession of transactions in order to hide true source and/or destination of funds. Mondex currently has this capability.

iv. **Source of value, location of funds, and/or location of transaction records** outside local jurisdictions can make it difficult or even impossible to investigate transactions. Furthermore, it could make it questionable as to which jurisdiction actually applies, when any of the parties are located overseas.

v. **Transportability of electronic funds** could be exploited as an advantage over cash when making illegal transactions. Physical transportation is easy in the case of Card Money, and not even required at all in the case of Network Money. Similarly, electronic funds could be stored outside bank accounts in a much more secure way than cash when using stored value systems.

vi. **Finality and irreversibility of payments** pose threats when fraudulent transactions are processed, as they may not be possible to reverse. This makes a system more attractive for illegitimate use.

vii. **Low transaction cost and time**, while without doubt economically desirable, could pose a threat in that they facilitate smurfing, as well as using a chain of transactions to hide source and destination of funds.

viii. **Rogue SVC scheme operators** would allow unwanted transactions to fund illegal activities that would be difficult to control through local legislation. Such operators would be similar to a rogue bank. With the cost of such systems at this stage being several million dollars, it requires a major investment. Yet, this need not be a problem, and the technology can be expected to become much cheaper in future.

5. Conclusion

The vulnerabilities discussed are by no way comprehensive. My focus has been upon aspects such as loss of collateral information through techniques such as aggregation and disaggregation of payments and use of third party intermediaries These pose great risks for businesses using such systems of payments as they may well leave the parties with no legal recourse should problems occur, particularly for international payments.

From a national perspective, the loss of control over payments for supervisory authorities in the various jurisdictions is also crucial as the new technologies threaten basic aspects such as the taxation base in each country and law enforcement authorities ability to track and address criminal activities that exploit these vulnerabilities.

Other issues such as timing fraud, and the significant areas that need to be addressed in respect of stored value systems are rapidly evolving aspects to payments security and integrity that will require significant focus as globalisation and accessibility open up such systems to greater scrutiny.

6. References

1. Greene, Thomas C. – "Reg duped by crime-busting D.I.R.T Trojan" The Register, posted: 06/06/2001 at 00:04 GMT

http://www.theregister.co.uk/content/archive/19480.html, (25 March 2002)

2. DOSHelp.com – "Trojan and Remote Access Service Ports", last modified Tuesday, March 19, 2002, http://www.doshelp.com/trojanports.htm , (25 March 2002)

3. Mondex USA – "How Mondex Works", http://www.mondexusa.com/html/content/technolo/technolo.htm , (25 March 2002)

4. Passas, Nikos , LL.B., Ph.D. Professor of Criminal Justice – "Informal Value Transfer Systems and Criminal Organizations; a study into so-called underground banking networks" – 1999, http://www.minjust.nl:8080/b_organ/wodc/publications/ivts.pdf , (25 March 2002)

5. Geiselhart, Karen Dr, "Will Income become Virtually Untaxable?" 2000 http://ausweb.scu.edu.au/aw01/papers/refereed/geiselhart/paper.html, (25 March 2002)

6. SWIFT, "SWIFT in Figures- February 2002" - Feb 2002 http://www.swift.com/index.cfm?item_id=4329 , (25 March 2002)

7. Bank for International Settlements (BIS), "Implications for Central Banks of the Development of Electronic Money" - October 1996

http://www.bis.org/publ/bisp01.pdf ., (25 March 2002)

8. Clarke, Roger Dr, "Smart Cards in Banking and Finance", 25 March 1997, http://www.anu.edu.au/people/Roger.Clarke/EC/SCBF.html , (25 March 2002)

9. Surety Ltd, "Digital Notarisation Technical Overview" – PDF, http://www.surety.com/sitemap/dns-presentations.html , (25 March 2002)

Appendix - Desirable Attributes of a Payments Scheme

The first table summarises the main attributes required to provide security and privacy in an electronic/Internet payment scheme, while the second table highlights other attributes that benefit the customer, merchant or financial institution.

Security and Privacy attributes

Attribute	*Description*
Communications integrity	The scheme should ensure that communications between customer, merchant and financial institutions are secured from alteration.
Communications confidentiality	The scheme should ensure that communications between customer, merchant and financial institutions are kept confidential.
Customer authentication	The customer must be authenticated in order to determine that they have the right to authorise the payment. This is to prevent stolen or copied cards/payment instruments being used fraudulently.
Payment scheme authentication	The party accepting the payment instructions should be authenticated in order to prevent capture of payment details for fraudulent purposes by third parties. Spoofing of bank or merchant Web sites is an example
Non repudiation of payment	System should ensure the customer cannot repudiate or deny that the transaction took place in order to obtain a refund of the payment. It provides certainty to the payee.
Payment details confidentiality	Payment details should not be made available to the merchant. The merchant should only know the details of what is being purchased. This protects privacy on a need-to-know basis.
Purchase details confidentiality	The nature of the goods and services purchased should not be made available to the bank/financial institution approving the payment. This protects privacy on a need-to-know basis.
Validation of payment	Payment instructions must be confirmed by the bank/financial institution holding the funds or providing the credit. Where anonymity of the payee is desired, digital bearer bond style schemes may be required.
Prevention of reuse of value.	Where a scheme uses a digital token or coin, it should prevent copied tokens from being exchanged for goods and services. This is normally done by reference back to the institution which "minted" the coin to ensure that the value for that specific token has not already been claimed.

Payer anonymity.	Anonymity for the payer is a key benefit of cash. It allows the payer to make purchases in the confidence that there is no audit trail via the payments system. This is because cash can circulate freely with there being no requirement to interface to a central payments clearing system that would enable identification of the party making the payment. For electronic payments, there are certain classes of electronic token schemes that can be used to provide anonymity to a payer where they require it.
Payee (recipient) anonymity.	Anonymity for the recipient (payee) is also key benefit of cash. It allows the payee to sell goods and then spend the funds on further purchases in the confidence that there is no audit trail via the payments system. Law enforcement agencies would debate whether this attribute is desirable or not, however it is a fact of life when using cash. Payee anonymity is very difficult even for electronic token systems as validation of the token normally requires interfacing with the "bank" that guarantees the value of the payment. This in turn normally requires lodgement into an account that is linked to the specific payee, allowing identification of the payee. Electronic token schemes such as digital bearer bonds or direct card to card transfer under schemes such as Mondex can be used to provide anonymity to a payer where they require it. However in the case of digital bearer bonds, this requires the payee to trust that the bond will be honoured for the same value by the next recipient.

Other attributes

Attribute	*Description*
Does not financially penalise Customer	The customer should not be required to spend more than a reasonable amount to be able to make payments to an Agency.
Equity of Access	The payment facility should ensure that all customers are able and capable of using at least one of the selected payment methods.
Quick processing	The schemes should employ simple messaging protocols that enable quick processing by the technology employed by the average merchant/financial institution. If a payment authorisation response is not received in a reasonable time (i.e. within 5 seconds) then agencies will be wary of joining such schemes.

Non-proprietary system	A scheme should be open to all participants and be available to all interested Agencies and financial institutions. It is desirable that it not "lock-in" the participants to a particular scheme promoter or technology as the rate of change can leave a particular payments scheme and its users in a technological "backwater"..
Variety of payment methods	The payee should enable payment by a variety of methods according to the customers wishes. This can be by credit card, direct debit from a bank account or by using the various electronic token schemes.
Minimal specialised software required on customer system.	Use of standard software (e.g. standard Netscape or Internet Explorer browsers) on the customer's computer removes the need to maintain specialised software which may become out of date and impose a cost on the customer.
Speed of settlement	The scheme should ensure the payee has access to funds as quickly as possibly after the payment has been made. This assists in maintaining cash flow.
Balancing security cost to payment value	A variety of schemes will provide security commensurate with the size of the payment. For small payments the level of security will be lower than for a high value payment. The payment value/security hierarchy would most likely be micro-payments to electronic tokens to credit cards. This ensures that the cost of security is not unduly high.
Timing of account debit	The schemes should allow the payer to elect to have value debited from their accounts at different times, these being in the **past** (i.e. electronic tokens), in the **present** (i.e. by direct debit) or in the **future** (i.e. by credit card). Small businesses are particularly sensitive about controlling account debits that restrict cashflow.
Legally Viable	Legal or policy directives by the payee may proclaim that certain schemes are not to be used for various reasons such as excessive merchant fee costs for large payments made by credit card or a high probability of repudiation of payments etc. Government agencies are most likely to be affected by regulations legally preventing the use of certain payment schemes.
Financially Viable	Minimisation of processing overheads is required to ensure that the cost of initiating, processing and settling the payments does not exceed the margin charged by the payment scheme.