ARRAY Logo

icon

Why does SSL dominate the e-payment market ?

Prof. JM Sahut, Head of RESFINE Laboratory, INT France
M. Galuszewska, PHD student, INT France

Web: www.int-evry.fr
Email: Jean-Michel.Sahut@int-evry.fr

Abstract

The crucial goal of this article is to reveal the real reasons for the SSL success. We will also analyse other e-payment solutions as well as the market of mobile payments. Finally, we will examine the repercussions of electronic payments for the banking system. The structure of the paper is as follows : identification of users� needs, presentation of existing e-payment systems, analysis of competitive, marketing and technological challenges.

1. Introduction

Since the mid-�90s, when e-payments were a major part of the Internet hype, a plethora of innovative e-payment solutions have emerged. Although insufficient security has been always considered the greatest barrier to conquering the market, reinforced security does not seem to have been strongly correlated with a market acceptance rate. Surprisingly, most security-focused systems have ended up being abandoned. The winner of the competitive battle is far from being secure. SSL (Secure Socket Layer), that has dominated the market of e-payments, is a communication protocol (not a payment protocol) and can be criticised for its imperfection as far as international payments and buyer identification are concerned. Faced with these facts, providers of e-payment solutions realised that they had not grasped the real needs of users.

2. Users� Needs

From the very beginning, service security was perceived as the most customer value-adding factor of online payment systems. Endless debates concerning net security compelled solution providers to focus on high security to the detriment of ease of payment procedures, short transaction time and low costs. However, the string of failures of security-focused systems, such as Cybercash, Digicash, eCash, SET and many others have induced solution providers to think about the users� expectations.

In fact, key success factors of a payment solution depend on security, cost, convenience and speed.

Six levels of security have to be provided :

� Identification: In order to initiate a transaction both parties have to be identified, a buyer, who is obliged to pay, and a merchant, who is obliged to provide a product or service.

� Confidentiality: Only indispensable transaction details are revealed to the parties, other data remain unknown. For instance, the vendor should not know a customer's card number when an intermediary provides him with a payment certification. The intermediary, in turn, is not supposed to be informed of purchase details. Another problem is to ensure that an unintended third party will not intercept data as their possible abusive use is the major Internet risk concern.

� Authentication: Electronic transactions have to be authenticated. Honest intentions of trading parties are ensured by the terms of transaction (product features and quantity, price, delivery date etc.). The electronic translation of this contract is the key factor of the future development of electronic commerce. Customers require a guarantee that a seller will not charge them for an imaginary purchase.

� Data integrity: During the session, payment data cannot be intentionally or unintentionally tampered with.

� Non-repudiation: Merchants want to be sure that the payment obligation will not be repudiated afterwards.

� Customer solvency: Customer solvency can be verified by a merchant or, to a certain amount, guaranteed by a bank.

Cost/security ratio: This risk factor is particularly important in the case of micro-payments as a unit transaction cost determines a minimal payment that brings profits.

Convenience attracts users. A payment system is expected to be transparent and integrated with a universal net environment (ex. SSL). Therefore, non-interoperable proprietary solutions requiring installation of additional software or equipment (ex. CyberCOMM) were rejected soon after their introduction.

Speed is the last but not the least criterion of the users� choices. The slow SET-based systems encountered a lot of resistance and had to be abandoned.

Today�s challenge is thus to introduce solutions meeting all of these needs together. Many existing systems are still focused on one feature neglecting the others.

3. Payment Systems

In Table 1, we present the classification of payments systems accompanied by a brief description of each of them. Next, we expand on their characteristics.

Table 1. Payment Systems Classification

Systems	Types	Initiators	Features	Transaction Value
ard Based stems	Traditional card based systems Alternative systems:	Cybermut Telecommerce Payline SIPS	Based on the SSL protocol Security problems with buyer and vendor authentication Alternative solutions focused on security improvement	Macro-payments (due to relatively high costs of a single transaction)
	Dynamic e-card	GIE Carte Bleue		
	Sound waves recognition	AudioSmartCard		
Electronic Money	Electronic wallet	Proton, Moneo, Geldkarte, Visa Cash	Based on smart cards or software Prepayment systems Bank does not participate in transactions	Micro-payments
	Virtual wallet	Caisse d�Epargne		

E-mail Payments		Paypal, Billpoint, Yahoo PayDirect, Citibank�s C2it	E-mails used for notification P2P market	Micro-payments Low value P2P payments
Electronic Checks		NetChex CheckFree	Dematerialization of traditional checks Have not gained large acceptance More popular in the USA and France	Macro-payments (cheaper than card systems but still relatively expensive)
Other Electronic Solutions	Telecom kiosk	Tel2Get, EasyClick	Service included in phone bill	Micro-payments
	ISP kiosk	w-HA	Monthly payments per use, act, volume or subscription	
	Personal account	Firstgate, Clik&Buy	� Service included in Internet bill	
	Pre-paid card	EasyCode, Carte � Plus	Scratch and phone cards	
Mobile Payments	Mobile wallet Mobile data verification Built-in data-storing chip Built-in smart card reader	Platform initiatives: J2ME (SunMicrosystems) Mobile Payment Services Association (Orange, Telephonica Moviles, T-Mobile, Vodafone)	Development phase Attempts to create an interoperable platform	Planned common use for micro-payments Application to macro-payments rather doubtful

3.1. Cards based systems

Data transfer in card based systems is protected by the SSL (Secure Socket Layer) protocol. A SSL-based transaction assures the encryption and integrity of a transferred message. Merchants can use it in two versions : with or without an intermediary. The version without intermediary assures message encryption and integrity but exposes both parties to other risks. As a customer communicates their card number and expiry date directly to a merchant, the card number can be taken from an insufficiently protected server of the merchant or illegally reused. Moreover, the existence of the merchant is not ensured. The merchant in turn does not have a guarantee that the buyer exists and that they will not repudiate the purchase afterwards. The version with an intermediary assumes the participation of a third trusted party, which guarantees the existence of the vendor as well as denies them access to the buyers� card data. It increases security on the customer side assuring them the merchant authentication and data confidentiality. Nonetheless, the latter is still not able to identify the buyer. This asymmetry can be eliminated by integrating into the technology the system of an electronic signature. The electronic signature allows the authentication of the buyer. However, such a solution requires the buyer to have a card reader or an electronic certificate, which, involving additional costs, cannot gain sufficient market acceptance. In spite of the imperfection of the SSL protocol, bank card systems have dominated the market of macro-payments and e-payments in general. This fact is mainly due to two reasons. First, it is simple to use, second, it is already tested and accepted by the market. Companies are not willing to implement very complex solutions as their customers expect the service to be fast, easy and, most important, cheap.

However, e-payment providers have been continually trying to improve the systems by eliminating their main inefficiency � lack of security. Unfortunately, such great initiatives as SET (Secure Electronic Transaction) and its derivative, CyberCOMM, as well as 3D Secure, have not been successful. At present, two emerging solutions seem quite interesting : dynamic e-cards and payment via sound

waves. Dynamic e-cards allow banks to generate a one-use card and cryptogram number and expiry date every time the card user buys online. This solution does not require any additional applications and significantly minimizes the risk of transaction. The second solution facilitates the identification and authentication of a card user via unique sound waves generated by the card. However, this system is still in the development phase.

3.2. Electronic money

At the outset, electronic money included three types of payment systems : virtual money, the electronic wallet and the virtual wallet. However, the methods based on virtual money (ex. : digital currencies of Digicash, Beenz and Flooz) were abandoned after a short trial period. Nowadays, only two of them are in use.

The electronic wallet is based on smart card technology, which is used to store data about the customer's funds. Money is loaded into the e-wallet by transfer from the cardholder's account. In this way, bank is not involved in the transaction at the moment of purchase. Smart cards target mainly the market of micro-payments. At present, they can be used at points of sale, vending machines, parking meters and ticket machines, public payphones, set-top boxes for interactive TV, etc. The integration of this system into Internet payments requires installing on the customer side smart card readers. The simplest and the most realistic way to achieve it is to build such readers into mobile phones. Such a solution can accelerate the development of pay-as-you-use services, such as online games, e-gaming, music, ticketing or mass transit systems.

Systems based on the virtual wallet are quite similar to electronic wallets. The only difference is that money is stocked on the software instead of on a smart card. Such a system is usually managed by a bank or a bank card issuer. Having created an account, the buyer only has to enter their ID and password at the moment of transaction. The virtual wallet is used for micro-payments via Internet.

3.3. E-mail payments

E-mail based payments are also used for micro-payments. They are destined for small businesses as well as for P2P (person-to-person) transactions.

Online auctions constitute the largest source of e-mail payment revenues. However, they are also used to pay for online gambling, adult entertainment as well as low-value international payments.

As a matter of fact, e-mail payments are not processed via e-mail. E-mails are used for notification, but funds are transferred the way banks settle inter-bank transactions. A customer loads an amount of money from his bank account into a service provider account then specifies the sum of money to be sent and enters the email address of a recipient. Both customer and recipient are notified that the money has been sent. The recipient receives the money and withdraws it from their bank account.

3.4. E-checks

The electronic check is the transposition of a traditional check into a dematerialised environment. The customer sends their payment order to a merchant, who presents it to an e-check issuing institution in order to authenticate it and make payment. Data related to the check and the payee are transmitted via the electronic interbank compensation system whilst the bank procedure of fund transfer is the same as in the case of a paper check. Similar to the card based system, electronic checks are used for macro-payments but their unit transaction costs are lower. Nevertheless, due to their limited popularity in traditional payments (in fact, used only in the United States and France), they do not constitute a serious threaten to card based systems.

3.5. Other electronic systems

Apart from electronic/virtual wallets and e-mail payments, micro-payments can be handled by incorporating the consumption of a service into phone or Internet billing. Payments included in the phone bill are called the telecom kiosk, while Internet bill based solutions can be operated in ISP kiosks and personal account systems. Nevertheless, these solutions have some serious limits as they frequently require two telephone lines, lines using ADSL or additional applications. Another solution is based on pre-paid phone and scratch cards but it has not yet been commercially deployed.

3.6. Mobile payments

Mobile payments are the payments carried out by PTDs (personal trusted devices), such as: wireless phone or PDA (personal digital assistant) as well as by the emerging ones: set-top boxes for interactive television systems or game consoles. Mobile payments can be used for : wireless Internet shopping, face-to-face shopping, vending machines, event and public transport ticketing, P2P (Person-to-Person) payments, pay-as-you-use payments, etc.

Although mobile commerce and mobile payment seem very attractive and convenient to users, after a few years of research and different projects, their popularity is still far from ubiquitous. First reason is that customers are very cautious about sending confidential data via mobile technology. According Forrester Research, credit card security concerns prevent 52 % of customers from adopting m-commerce via phone and 47 % via PDA. Another problematic issue is that the value a mobile payment has to be shared among three participants : telecommunication operator, payment provider and bank. It can happen that the bank provides a payment solution. If it is a case, the number of participants is reduced to two. The lack of precise rules describing the role of each of the parties in a particular business model impedes the popularisation of mobile payment systems. However, strong pressure towards so-called �anytime, anywhere, with any device� solutions increases the chances for success of mobile payment platforms. Therefore, at the time being, we can say that m-commerce and m-payments are at the critical point. If they do not succeed during the next few years, it may experience gradual replacement by other solutions.

4. E-payment challenges

The challenges of the e-payment market can be divided into three general categories : competitive, marketing and technological. Competitive challenges result from the fact that the market of payments is no longer under the exclusive control of banks. Many new entrants, such as Internet Service Providers or telecommunication operators have appeared and succeeded in taking over their functions. Marketing challenges are related to the emergence of new business models and strategies. Technological challenges appear as a result of dynamic development of new systems and solutions, which grows the need for interoperability and compatibility.

4.1. Competitive challenges

With the development of innovative payment systems, banks have had to face a dynamic inflow of new competitors. We can distinguish several groups of these newcomers :

Companies from the computer industry operating low-value payments (mostly based on smart cards), such as ticketing, public payphones etc.

EDI (Electronic Data Interchange) service providers. Recently, the Financial EDI module has appeared. Its destiny is to manage e-payments and financial data exchange. The future of EDI is doubtful due to the development of XML as a standard of payment data transfer. It is however more likely that instead of the out-and-out replacement of EDI, there will be a gradual transfer to XML-based information exchange. Some of the largest EDI service providers have already started implementing translation services.

Internet Service Providers offering e-mail payments, virtual wallets and electronic checks.

Telecommunication and mobile operators developing the market of mobile payments.

At the beginning, new entrants were trying to compete with all existing players in order to convince customers that their solution is suitable for every kind of transaction. Having learnt important lessons from several serious disasters, they realised that the market was going to be segmented and solutions would have to be proposed to a particular segment. The main division criterion is transaction value, according to which we distinguish macro- and micro-payments. For instance, e-mail payments and electronic wallets are unlikely to be used on the market of high-value transactions while small payments are not going to be processed via electronic cards or checks. Having understood these strict rules, market participants have developed and articulated more reasonable strategies of positioning themselves on the market.

The oldest players � the banks � have maintained their dominance on the market of macro-payments

(cards and electronic checks) as they participate in most transactions as a trusted party. Nevertheless, their role in micro-payments seems to have significantly decreased. In all of the systems : electronic money, e-mail payments, mobile solutions and new electronic systems, transactions are processed independently of banks. Their functions are limited to periodical transfers of funds to other payment tools, such as Internet accounts, smart cards or data storing software. Then, EDI or Internet service providers operate transactions.

As far as electronic money systems are concerned, we can observe a strong tendency to make partnerships and mergers in order to eliminate competitors as well as provide a cheaper and more complex service. For instance, two competing French electronic wallet systems : Moneo and Modeus merged in 2000 in order to dominate the French market. We can also observe many initiatives tending to introduce common standards, such as CEPS (Common Electronic Purse Specification). However, so far such initiatives have not been successful.

The strongest competition can be observed in e-mail payments. Although Paypal has a major market share of 27%, Billpoint with its 11% is not going to give up (Gartner Group, February 2002). Less important players, such as Yahoo PayDirect and Citibank, are also making a great effort to stay in the market.

E-check providers seem to be rather unsuccessful. They lose with card systems as far as high value payments go and do not spark much interest in the micro-payments market, due to relatively high transaction costs as well as the variety of other competitive solutions. Probably, the reason is that they have never been ubiquitous in traditional payments.

Telecommunication operators and ISPs are also attempting to earn on electronic payments proposing different innovative tools such as telecom and Internet kiosks, phone cards etc.

Finally, the market position of mobile operators is still very weak. They cannot get users into the mindset that mobile payments are secure. However, they are also trying to join forces and create a large, secure and interoperable mobile payment platform. If the trust barrier is broken, the convenience of mobile payments may attract a large mass of customers.

4.2. Marketing challenges

Developing a unique strategy which can attract customers seems to be quite a challenging task in the market of e-payments. Designing innovative and complex solutions is limited by three very basic, but very strict, user criteria : low cost, convenience, speed and security. Both of the online payments parties, vendors and buyers, expect the services to be processed with no problem. They do not want to waste their time fulfilling in pages of application forms or waiting until the transaction is completed. Observing different strategies, we can state that the secret of the successful one lies in such a combination of security and convenience that security procedures are not burdensome for users but visible to the extent that the latter are not afraid of a fraud. We could even suppose that although customers frequently mention insecurity as a main barrier to e-payment systems development, in reality, they are ready to accept much more risk than they declare. It could partially explain the mysterious success of SSL.

Electronic payments can also be integrated into a larger set of services, such as web creation and management. These solutions are proposed to small and medium companies that need some backup to design and manage their e-business. Another solution is to start co-operation with a commercial portal. At the moment of transaction, the buyers are automatically transferred from the shopping portal to the website of the payment provider. To increase the attractiveness of such solutions, customers can be awarded fidelity points for each completed transaction.

4.3. Technological challenges

Nowadays, we can notice many innovative strategies appearing on the market. Most put an emphasis on speed, convenience, interoperability and enhanced security at the same time. Such solutions as the dynamic e-card or the sound wave based recognition system are the best examples. Nevertheless, very few of them have been already launched on the market. Payment security still constitutes an open topic and awaits new solutions to be introduced and accepted, while interoperability and common standards are still very problematic and need to be eliminated as soon as possible.

Conclusion

Since the emergence of electronic payments, their features and strategies of development have been constantly changing. At the outset, e-payment providers focused exclusively on security issues proposing proprietary systems that were quite expensive and user unfriendly. Having realised that the market rejects such solutions, they started concentrating on costs and ease of use, proposing less secure systems. Surprisingly, they did much better. The best example is the SSL protocol, which has always been heavily criticised for its insecurity. Its leading position in macro-payments is due to several factors : simplicity, interoperability and popularity of the original payment mode (offline transactions by card) in traditional payment systems.

The present situation on the market of electronic payments can be compared with the state of non-optimal equilibrium. The widely accepted solution is not optimal but the market players have found a common denominator meeting their needs and are not willing to change it.

The first step to get out from this vicious circle is to make all interested parties realise that the change in the present state can bring important benefits. The introduction of a new more advantageous system can increase the level of payment service security, decrease losses caused by frauds as well as allow the better positioning of participants within the value chain. However, the real introduction of such a system requires a joint effort of all parties and this condition is the fundamental factor impeding the changes. Although governmental interventionism is inconsistent with the rules of free market economy, it seems that imposing legal restrictions could constitute an efficient way to induce some changes. The introduction of normalisation standards or administrative constraints are the examples of possible state actions.