

3-D Secure: A critical review of 3-D Secure and its effectiveness in preventing card not present fraud

by

Anthony Bouch

March 2011



Supervisor: Dr. Konstantinos Markantonakis

Submitted as part of the requirements for the award of the MSc in Information Security of the
University of London.

In loving memory of

Michael George Bouch

Table of Contents

Executive Summary	v
1. Introduction.....	1
1.1 The Insecure Internet	1
1.2 The Birth of E-commerce	2
1.3 Objectives.....	3
2. Background	5
2.1 Payment Models.....	5
2.2 Payment Cards.....	8
2.3 The Security of ‘Card Present’ Transactions.....	10
2.4 The EMV Standard.....	12
2.4.1 Introduction	12
2.4.2 EMV Advantages	20
2.4.3 EMV Disadvantages.....	21
2.4.4 EMV Summary.....	21
2.5 The Security of ‘Card Not Present’ Transactions	22
2.6 E-commerce via a Web Browser and SSL/TLS	24
2.6.1 Introduction	24
2.6.2 Web Browser and SSL/TLS Advantages	27
2.6.3 Web Browser and SSL/TLS Disadvantages	27
2.6.4 Web Browser and SSL/TLS Summary.....	28
2.7 An E-commerce Requirements Checklist.....	30
2.8 SET – A First Attempt at Securing E-commerce	32
2.8.1 Introduction	32
2.8.2 The SET Result.....	36
2.8.3 SET Scorecard.....	37
2.8.4 SET Summary.....	38
3. 3-D Secure	39
3.1 Introduction.....	39
3.2 The Merchant’s Perspective	46
3.2.1 Merchant Advantages	47
3.2.2 Merchant Disadvantages	48
3.3 The Acquirer’s Perspective	49
3.4 The Issuer’s Perspective	50
3.4.1 Issuer Advantages	50
3.4.2 Issuer Disadvantages.....	50
3.5 The Cardholder’s Perspective	51
3.5.1 Survey.....	52
3.5.2 Cardholder Advantages	54

3.5.3 Cardholder Disadvantages.....	54
3.6 3-D Secure Scorecard.....	55
3.7 3-D Secure Further Analysis.....	56
3.8 3-D Secure Summary.....	62
4. Alternatives.....	65
4.1 PayPal.....	65
4.1.1 Introduction.....	65
4.1.2 PayPal Advantages.....	67
4.1.3 PayPal Disadvantages.....	68
4.1.4 PayPal Scorecard.....	68
4.1.5 PayPal Further Analysis.....	69
4.1.6 PayPal Summary.....	70
4.2 iDEAL.....	70
4.2.1 Introduction.....	70
4.2.2 iDEAL Advantages.....	72
4.2.3 iDEAL Disadvantages.....	73
4.2.4 iDEAL Scorecard.....	73
4.2.5 iDEAL Further Analysis.....	74
4.2.6 iDEAL Summary.....	75
5. The Future.....	77
5.1 Activity in E-commerce.....	77
5.1.1 Trends.....	77
5.1.2 Regulatory Environment.....	77
5.1.3 Security.....	78
5.2 A Hypothetical E-commerce System.....	80
5.2.1 Customer Requirements.....	80
5.2.2 Merchant Requirements.....	80
5.2.3 Scheme Architecture and Transaction Sequence.....	81
5.2.4 E-REP Advantages.....	83
5.2.5 E-REP Disadvantages.....	83
5.2.6 E-REP Summary.....	84
6. Conclusion.....	87
Bibliography.....	91
Appendix A – The History of E-commerce.....	101
Appendix B – Survey.....	103
1. Survey Screenshot.....	103
2. Survey Data.....	104

Executive Summary

E-commerce represents a web-based Internet economy that has risen from zero, to over a trillion dollars worldwide, in just seventeen years.

However, the security challenges faced by the world's largest open (and effectively anonymous) network, have meant that the growth of the Internet – and e-commerce – has been met with an equally rapid growth in the activities of those intent on using the Internet as a vehicle for malicious and criminal activities online.

It is within the context of the growth of the Internet, and in particular e-commerce, that this report will examine current efforts to reduce the level of fraud in payment card-based e-commerce.

One of the core observations made early in this report, is that payment cards are being used in a way never intended, and that their unsuitability as an instrument of payment in e-commerce has led to several unintended consequences – including the dramatic rise of fraudulent payment card transactions online. The fraudulent use of payment cards in e-commerce also resulted in the need to create a scheme-based protection measure known as a 'chargeback'. Chargebacks allow a cardholder to shop online without the fear of suffering a financial loss from fraudulent transactions; however, they have also unfairly shifted the liability of accepting such transactions to the merchant. Merchants have been further encumbered with an industry attempt at protecting payment card data in the form of the PCI Security Standards Council Data Security Standard (PCI-DSS).

Additional findings include the observation that despite well documented weaknesses and costs associated with the use of payment cards via a web browser and SSL, there has been a lack of progress by the payment-card industry in providing suitable alternatives. Noteworthy in this report's findings is that it has taken close to a decade, from the payment industry's first comprehensive attempt at securing e-commerce (via SET), to implement a scheme designed to reduce payment-card fraud online. That scheme is 3-D Secure.

Furthermore, this report concludes, that, despite the time taken to implement 3-D Secure, the scheme suffers from failings in ownership, communication, usability and security – while simultaneously burdening Internet users (and cardholders) with yet another password-based system.

Suggested explanations for the lack of significant improvements in payment card-based e-commerce (as well as the failure of alternative schemes to gain significant market-share), include the market dominance of the two major payment card brands – Visa and MasterCard. The lack of liability for the use of their own payment instruments, and possibly conflicting

obligations between scheme members and shareholders may have also contributed to a lack of progress in the development of improved and more suitable payment systems.

This report also concludes that e-commerce as a whole is likely to see dramatic changes over the coming years as the potential for integrating smart cards and tokens with mobile devices is fully realised. What remains to be seen, however, is whether any scheme that achieves broad commercial success does so because of its merits in facilitating a safe and convenient e-commerce experience – or because of the influence and leverage of other ‘vested interests’.

1. Introduction

1.1 The Insecure Internet

There are now an estimated two billion Internet users globally [1] with over 30 million adult users accessing the Internet everyday in the UK alone [2].

From its origins as an experiment in reliable 'packet based' networking in the late 1960s and 1970s [3] – the Internet has grown into a pervasive interconnected network of computers and applications that spans the globe and is dramatically changing the world we live in [4].

The early inventors of the Internet did not anticipate its current size or impact, and while its growth might serve as a testament to the eloquence of its original design – from a security perspective, things are a little more complicated.

Early users of the Internet accessed the network from the relatively safe environment of academic institutions and protected data centres. Issues of identity and authentication were considered lightly at a time when the Internet existed within a culture of co-operation, trust and resource sharing. The result was that the foundation protocols of the Internet were vulnerable to those who saw the Internet as a convenient vehicle for malicious and criminal activities [5,6].

From a purely commercial perspective, The Internet Crime Complaints Centre (IC3) in the USA in its 2009 IC3 Annual Report stated a dollar loss in referred complaints of 559.7 million US dollars [5] – up from just 17.8 million in 2001. The UK Cards Association reported 266.4 million pounds sterling in card-not-present fraud in 2009 – from 95.7 million in 2001 [7].

The growth of the Internet has provided us with many novel and convenient methods of communication. And yet it would appear that as more 'value' moves into electronic form and onto the Internet, so too does the risk that information of value will be lost or used in ways to commit malicious and criminal acts.

It is at the confluence of these dramatic changes that we find ourselves today – with increasing value in personal, private and commercial information online, as well as increasing activity from those intent on making money from criminal activities via the Internet [8]. It is also at the confluence of these changes that most Internet users find themselves confronted by a bewildering landscape of terminology and technology. Users are expected to choose (and remember) numerous account names and passwords. Users are also expected to defend themselves from solicitous and often fraudulent emails as well as somehow determine whether the website to which they are about to hand over their credentials or payment details, is trustworthy and legitimate, as opposed to a cleverly disguised ruse designed to part them from their hard-earned cash.

Users as individuals are not alone in their efforts to defend themselves online, as security has become a major concern for the commercial and public sectors as well. However, it's at this point that the interests of larger organisations with deep technical knowledge and dedicated resources may not entirely align with the interests of the average Internet user. The average user is as potentially vulnerable to changes in the 'terms' within which they are expected to interact and exchange information online as they are to the overt actions of a malicious third-party.

It also seems unrealistic to expect users of the Internet to be able to make informed decisions about the security of their activities online – when most don't actually know what the Internet *is*. Take for example a light-hearted 2009 on-the-spot survey performed by Google employees (see <http://www.youtube.com/watch?v=o4MwTvtYrUQ>), where about fifty people were asked what a browser is. Of those asked, only about 8% were able to describe what a browser is and how it is used on the Internet.

1.2 The Birth of E-commerce

In 1989, Tim Berners-Lee wrote a note to the European Organization for Nuclear Research (CERN) management describing a global hypertext system [9] – which would eventually lead to the invention of the hyper text transfer protocol (HTTP), hyper text mark-up language (HTML), the 'browser', [10] and what would ultimately become the millions of web sites hosting web pages that we visit and view everyday via the Internet – collectively referred to as 'The World Wide Web' or 'The Web'.

Public awareness of the Internet and the World Wide Web began to rise in the early 1990s and it wasn't long before retailers began to see the opportunity to 'sell' on 'The Web'.

Presenting a catalogue of goods via a web page was one thing – allowing customers to pay securely was another. In 1994, Netscape released the 'Navigator' browser and, later in the same year, released the first version of the Secure Sockets Layer protocol (SSL) [11] – a protocol designed to establish an authenticated and confidential channel between a browser and a web server. A user using the Navigator browser was given a visual indication that they were now communicating securely with a web server via the padlock icon. The image of the padlock 'unlocked' would represent an insecure connection – while the image of the padlock 'locked' would represent a secure connection via SSL.

With an apparent solution to the problem of being able to securely transmit data from the user's browser to the receiving Web server, e-commerce sites quickly began to accept credit cards as a method of online payment for goods and service advertised on the Web.

The result was the creation of the e-commerce industry, including the birth of e-commerce giants such as eBay and Amazon, and a web-based Internet economy that has risen from zero to over a trillion dollars worldwide (See Appendix A – The History of E-commerce). In the

UK alone, e-commerce is now estimated at a yearly value of 100 billion pounds, or 7.2% of GDP [12].

The challenges of keeping payment systems secure have risen proportionately – particularly in the case of payments made via payment cards over SSL and despite advances in security mechanisms in general.

These challenges include:

1. The expectation that the average Internet user is able to make informed security decisions about their personal and commercial activities online.
2. The overreliance of usernames and passwords as a primary method of authentication on the Internet.
3. The need for effective user-friendly payment methods that also represent good security practices.

1.3 Objectives

It is within the context of the need to create improved and user-friendly mechanisms for secure payment systems, as well as to ensure that all parties are fairly protected and represented, that this report will examine a recent initiative designed to reduce the level of Internet-based card payment fraud: a system called 3-D Secure.

The objectives of this paper, therefore, are as follows:

1. To present a background to payment models and the payment card industry including the developments that led to 3-D Secure.
2. To present a technical description of 3-D Secure, as well as a detailed description of the actors involved in a 3-D secure transaction.
3. To examine the motivational factors for adopting 3D Secure, as well as its reception, from the point of view of each of the main actors – including cost, usability, security, and liability issues.
4. To compare 3-D Secure with other non-payment card based options.
5. To summarise 3-D Secure and its effectiveness in preventing 'card not present' fraud.
6. To determine whether 3-D Secure represents good security practices, as well as fairly represents the interests of all involved parties.
7. To draw conclusions as to whether given the current 'state of affairs' of e-commerce and online payments systems, 3-D Secure was the right thing to do given all of the above, or whether alternative solutions would have been more appropriate.

In this chapter we have presented a brief history of the Internet as well as having hinted at some of the security challenges that have arisen as a result of its origins and rapid growth.

We have also presented a brief history of e-commerce, demonstrating that the equally rapid growth in trade on the Internet is forcing the e-commerce industry to address its own security challenges.

Chapter 2 will provide a background to the current 'state of e-commerce,' commencing with a brief history of payment models and payment cards. Next, we will look at the security of 'card present' transactions and the EMV standard – its advantages and disadvantages – and then, the security of 'card not present' transactions. From there, we will examine e-commerce via a web browser and SSL/TLS – its advantages and disadvantages, as well as an e-commerce requirements checklist. We will finish the chapter by reviewing the Secure Electronic Transaction (SET) standard – an early attempt at securing e-commerce.

In chapter 3, we will examine 3-D Secure, discussing the advantages and disadvantages, starting from the merchant's perspective, and continuing with the perspectives of the acquirer, the issuer, and the cardholder. An informal user survey is also presented in this chapter – designed to gauge public opinion and response towards 3-D Secure.

In chapter 4 we will examine two non-card-based solutions – PayPal and iDEAL. PayPal was chosen as an example of a 'three-party' system, and as such illustrates the advantages and disadvantages of such schemes. iDEAL was chosen as an example of an alternative 'four-party' system that interestingly (like payment cards themselves), was started by an association of banks in the Netherlands.

In chapter 5 we will briefly examine the future of the e-commerce industry, before moving on to chapter 6 where we will draw our conclusions as to the appropriateness of the 3-D Secure system to meet the needs of the e-commerce industry today.

2. Background

2.1 Payment Models

Few of us stop to consider why it is that we ‘trust’ the coins and notes we have in our wallets or purses. We’ve become culturally accustomed to the notion that they represent monetary value and that they can be used to buy goods and services. Money serves as a medium of exchange [13] and our trust in this medium is based entirely on the promise by the issuer that our coins and notes will be honoured, and so relied upon by the parties wishing to exchange them for goods and services. Money is an instrument of payment, and a payment is the process by which money is transferred to a creditor by a debtor for the extinguishment of a debt [13].

Coins and cash notes are physical tokens that can be used as currency; however, other tokenized forms of money exist – including electronic money.

The EU Directive 2009/110/EC of the European Parliament and of the Council defines electronic money as, [14]

“...‘electronic money’ means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer...”

If a payment is the exchange of money to extinguish a debt, then an electronic payment could be described as the transfer of monetary value from one party to another via an electronic network or device [15].

Electronic payments systems can be divided broadly into two major categories:

1. Cash-like systems that transfer money using electronic tokens that represent value with no intermediary instruments, instructions or services – such as a pre-paid e-wallet or electronic purse.
2. Account-based systems that are used to transfer a numerical value that represents money, from one account to another.

Account-based instruments such as cheques, money orders and credit cards are not money – but instead provide evidence of the intention and ability to pay via an account-based system [13].

The use of direct cash-like systems, direct account-based cheque-like or credit card-like systems, as well as indirect push and pull account systems is summarised by Peiro *et al's* payment model in Figure 1: [16]

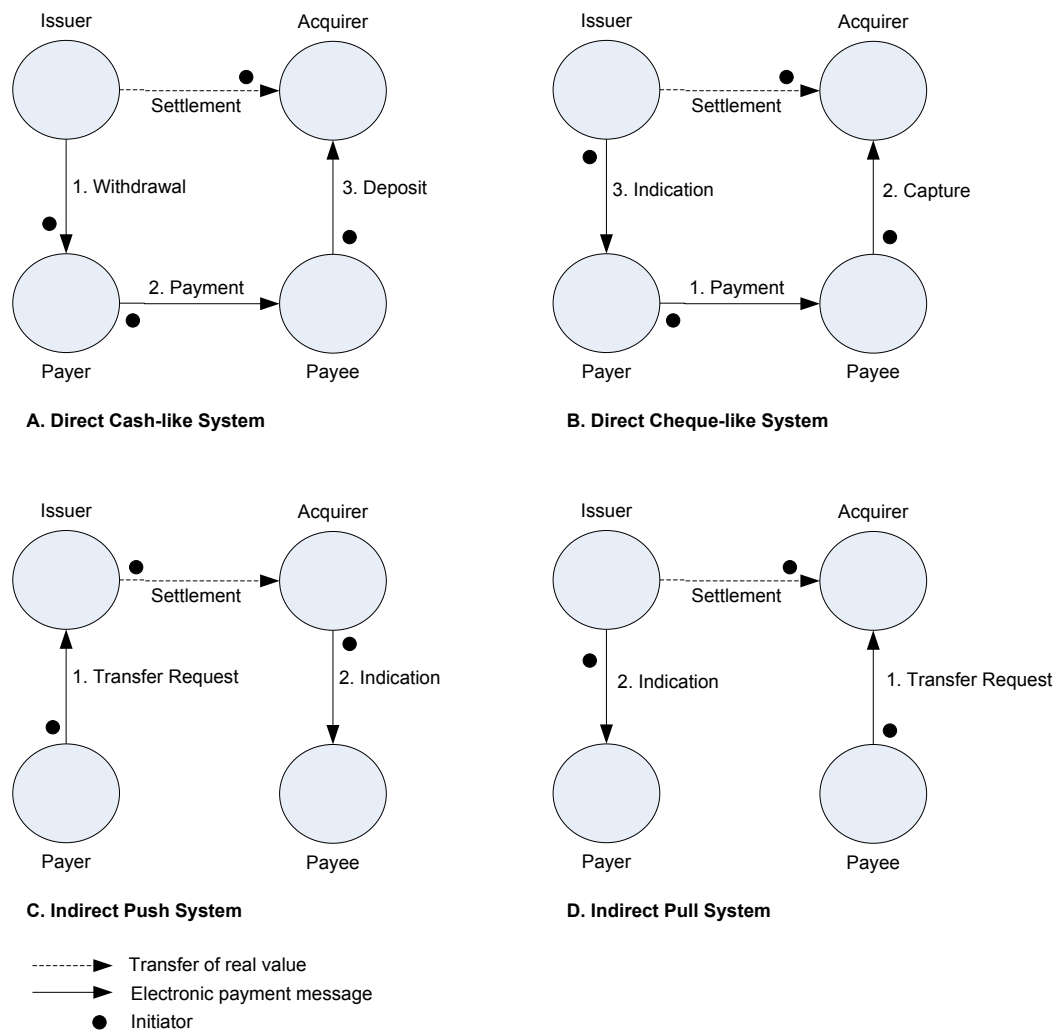


FIGURE 1 – DIRECT AND INDIRECT PAYMENT MODELS [16]

Indirect push or pull systems only involve a single initiator: either the payer, who initiates a credit transfer (as in the instructions given to a bank to transfer funds to another account); or a payee, who initiates a debit transfer (as in a direct debit or standing order).

Other systems of payment classification have attempted to define payments based on the immediacy of the transaction (payment on delivery, payment after delivery, payment before delivery, etc.), the direction of the transaction, as well as the instruments or instructions of the transaction. One such attempt is a report by the European Central Bank (ECB) called 'Classifying Payment Instruments – A Matryoshka Approach' [17]. In this report, Peiro *et al's* model above is mapped, with a diminished distinction between direct and indirect payment systems, as follows in Figure 2:

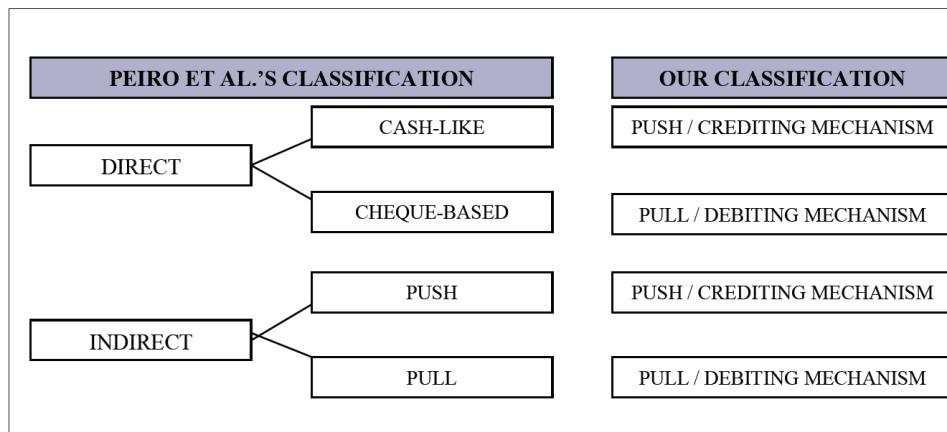


FIGURE 2 – A COMPARISON OF PEIRO ET AL'S AND THE MATRYOSHKHA TAXONOMY [17]

The Matryoshka model is an attempt to classify mechanisms, instruments or devices as belonging to one of five layers – one from each of which will combine to form a complete payment system, as shown in Figure 3 below:

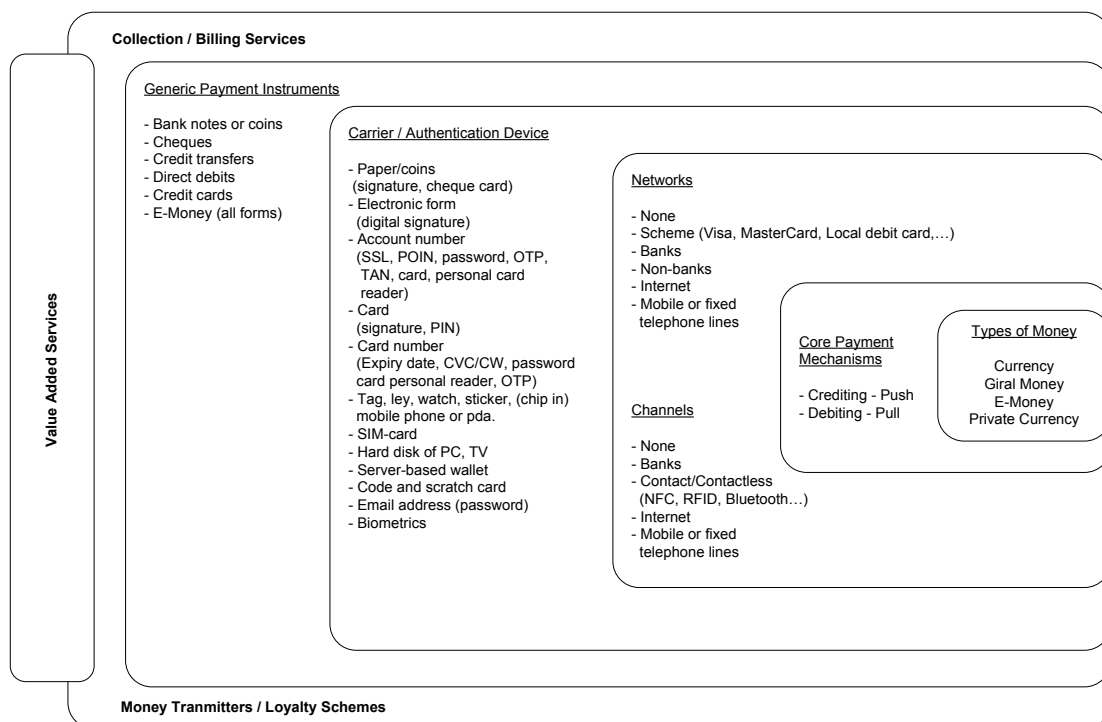


FIGURE 3 – THE MATRYOSHKHA MODEL [17] AS ADAPTED AND PRESENTED IN INNOPAY'S 'ONLINE PAYMENTS 2010' REPORT [18]

Innopay presented an adaptation of the Matryoshka model in its 'Online Payments 2010' report [18], describing the desire to produce such a visual aid in the classification of payments systems as coming from,

“..the sheer number and diversity of approaches in payment systems which can sometimes make it difficult to establish a clear understanding of how a particular scheme works.”

The Innopay report also highlights several weaknesses in such an approach. However, both the ECB and Innopay reports make it clear that the world of electronic payment systems has been, and will continue to be, a dynamic one. A report from the *Institut für Informatik der Technischen Universität München*, ‘Chablis Market Analysis of Digital Payment Systems’ in 1999 [15], documents fifty-one separate digital payment schemes including eCash [19], Mondex [20], and MilliCent [21]. However the majority of these schemes failed to reach wide-scale commercial implementations.

The rise of payment cards (credit and later debit cards), combined with SSL in e-commerce, may have also had an impact on the success of alternative electronic payment schemes. Once established, the direct account-based method of using a credit card to authorize the payment of goods and services became a culturally accepted and well understood mechanism for making payments in the real world. The ‘shopping cart’ and ‘check-out’ metaphors of web sites in the online world meant that an already established and easy to understand system for making payments was successfully applied to e-commerce. Supported by protections for the cardholder against fraudulent use, payment cards using a browser and SSL became the predominant method of payment for web-based e-commerce.

2.2 Payment Cards

The earliest form of payment cards came from oil companies and department stores which issued their own proprietary cards as a means of creating customer loyalty. The customer had an ‘account’ with the company and the company sent a monthly statement and invoice to the customer for payment. Some companies offered revolving credit, while others required the balance to be paid in full each month [22].

The first credit card, named ‘Charge-it’, was introduced in 1946 by a banker name John Biggins in Brooklyn, New York. However, the card could only be used locally – and both the customer and the merchant needed to have an account at Biggins’ bank [22].

The first wide-spread credit card was the Diners Club Card with 20,000 cardholders in 1951. Diners Club Cards are ‘charge-cards,’ meaning the bill must be paid in full at the end of each month. The Diners Club Card was originally made of cardboard (so too was the Charge-it card); not until a decade later was a plastic Diners Club Card issued [22]. American Express was the first to come out with a plastic charge-card in 1958 [22].

Bank of America is credited with the first large-scale credit card programme. In 1958, 60,000 unsolicited BankAmericard credit cards were mailed to customers in Fresno, California, in what became the first successful credit card 'drop' (mass mailing of unsolicited and working credit cards). Confirmed rumours of a competitor's pending 'drop' led Bank of America to accelerate its programme of mass mailings. By October of 1959, the entire state of California had seen over two million credit cards sent to individual addresses. The programme, however, was a financial disaster. 22% of accounts became delinquent (as opposed to the estimated 4%) and the state of California was confronted with the brand new crime of credit card fraud. What's more, with customers liable for all charges including those resulting from fraud, the scheme became the focus of intense political and media pressure. In a "massive effort," Bank of America was forced to repair the damage – issuing an open letter of apology to 3 million households, as well as implementing proper financial controls and fraud protection measures [23].

In response to Bank of America's BankAmericard, several other California banks formed their own association and issued the MasterCharge credit card [23].

By the mid-to-late-1970s, both schemes had grown nationally and internationally into licensed associations of card issuers and acquiring banks. In 1975, the international and national networks of BankAmericard were brought together under the new name of "Visa", while in 1979 the MasterCharge networks became "MasterCard" [24].

Visa and MasterCard operate under what is called a four-party system [25]. The four entities are:

1. **The Cardholder:** The individual in possession of a payment card.
2. **The Issuer:** The bank or organisation that issues the card to the cardholder.
3. **The Acquirer:** The bank which receives payment from the issuer on behalf of the merchant.
4. **The Merchant:** The entity with goods or services to sell that receives payment instructions and details from the cardholder – to be settled by their acquirer (via the scheme network) with the issuer.

Figure 4 illustrates the four-party model, including the transaction flow and related charges. Merchants typically bear the cost of both a payment processing fee by the acquiring bank as well as an interchange fee. The interchange fee is designed to recover the costs of operating the scheme network, as well as correct the imbalance in costs incurred between the issuer and acquirer [25]. While the acquirer will typically have payment devices at point of sale – a terminal or card reader, capable of accepting payments from many cardholders – the issuer

will bear the greater cost of issuing and managing payment cards and transactions for every cardholder.

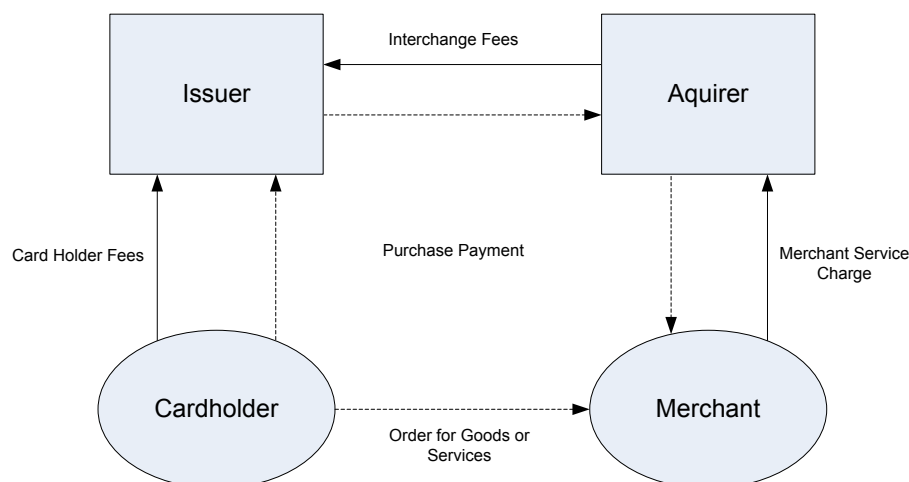


FIGURE 4 – THE FOUR-PARTY MODEL

Interchange fees range from 1-3% of the transaction value [26], with fixed caps in place for certain transactions. However, for online payment processing payment processors may charge as much as 6% of the transaction value¹.

The four-party model allows for scalable ‘trust relationships’ between multiple acquirers and issuers that are members of a single scheme or network – such as Visa or MasterCard – while allowing merchants and cardholders to establish their own accounts and trust relationships with merchant or issuing banks of their choice.

2.3 The Security of ‘Card Present’ Transactions

As Bank of America discovered after its large-scale ‘drop’ of credit cards in 1959 – it didn’t take long for fraudsters to realize that payment cards represented a new money-making opportunity in real world crime. Over the next fifty years, card issuers and merchants would play a cat-and-mouse game against fraudulent payment card activity.

‘Card Present’ (CP) transactions are transactions where the cardholder, card and merchant are all physically present at the time of payment authorisation using a payment card.

The two most significant forms of payment card fraud in CP transactions are the use of lost or stolen cards (including non-receipt of new cards sent to the cardholder’s address), and counterfeit cards. Losses from counterfeit, lost and stolen cards (including non-receipt) accounted for 91% of UK CP fraud in 1999 and 78% of CP fraud in 2009 [27].

¹ From this author’s own experience in implementing a payment solution in what was considered a high-risk country – via WorldPay in 2003.

While other forms of payment card fraud exist (including account takeover and fraudulent applications [28]), it's likely that the high percentage of fraud associated with counterfeit, lost, and stolen cards drove initial payment card protection measures.

Early measures designed to protect against the use of lost or stolen cards included comparing the signature on the strip on the back of a card with the signature of the person attempting to use the card at the point of sale. Policy-based measures included additional telephone authorisation for large or suspicious transactions, as well as looking up card numbers on printed lists of stolen or delinquent cards.

Physical protection measures against card tampering and counterfeit cards included embossing, holograms, tamper-evident signature strips, and ultraviolet printing. The early payment systems also relied on card embossing not only as evidence of tampering, but also to take an 'impression' of the card. Using a physical card holder, a roller was drawn across the card in order to make a carbon copy impression on a paper transaction-slip. The customer then signed the slip for the merchant to later submit for settlement as evidence of the cardholder's authorisation.



FIGURE 5 – PHYSICAL CARD PROTECTION MEASURES (Source: David Main & Karl Brincat – ‘Information and Security @ Visa - lecture presented at RHUL, February 2008)

The major disadvantage of the above measures is that they relied heavily on the merchant or sales assistant being able to verify the cardholder's signature as well as identify suspicious and possibly counterfeit cards [29].

The early 1970s saw the introduction of a magnetic stripe on the back of payment cards. This was after the successful development of magnetic stripe media and subsequent standards that were agreed upon for both the contents of magnetic stripe card data, as well as its location on plastic cards [30,31]. The result was that a standards-based point of sale (POS)

terminal could be used to 'swipe' a card to automatically read the card data, as well as automatically 'dial-up' for card authorisation.

The data contained within the magnetic stripe was eventually updated to include a cryptographic checksum – or card verification value (CVV). The CVV is used to confirm that the values supplied from the card including the primary account number (PAN), expiry date, and service code – all match those values that were used to generate the CVV when the card was first issued. The idea is that while all of the other card values could be read directly from the card, or obtained from other sources such as visually inspecting the card, receipts or correspondence – the CVV was not casually available and could not be recreated without the key that was used by the issuer to generate the CVV in the first place.

Despite physical card protection measures and magnetic stripes, sophisticated and fraudulent card manufacturing techniques (including card 'skimming' techniques that can be used to copy the entire contents of the magnetic stripe including CVV value) – meant that until recently, fraud from lost, stolen or counterfeit cards continued to rise [7,27].

2.4 The EMV Standard

2.4.1 Introduction

In 1994, Europay, MasterCard and Visa initiated the development of a new system designed to reduce CP payment card fraud [32]. The system is called EMV. It is based on smart card technology and an advanced end-to-end secure message-level protocol designed to authenticate and authorize payment card transactions.

In 2002, Europay merged with MasterCard International to form MasterCard Inc, and the EMV specification is now owned by American Express, JCB, MasterCard and Visa [32].

The EMV standard in the UK is promoted as 'Chip and PIN' – with the 'chip' referring to the electronic chip that is embedded into the plastic payment card, used in conjunction with the cardholder's secret personal identification number (PIN).

The chip that is embedded in the payment card is based on the ISO/IEC 7816 set of standards for integrated circuit cards with contacts (ICCs) [33] – generally referred to as smart cards. The ICC in more advanced smart cards is effectively a small computer – containing a central processing unit (CPU), random-access memory (RAM), read-only memory (ROM) and electrically erasable programmable read-only memory (EEPROM). Smart cards are primarily used to add security to a system since they contain several physical and security-related features that make them attractive in such a role [34].

These include:

- They are small and thin - which means they can be mounted on cards or tokens and will fit in a wallet, purse or other small device.
- They are not easily forged or copied.
- They are resistant to tampering.
- They can store data securely.
- They can run multiple security algorithms and functions.
- They are consistent and controlled (unlike a personal computer).
- They are (for the moment at least) standards-based.
- The chip-carrying card or token can be personalized or branded.
- The chip can (if required) be formally evaluated in order to provide assurances as to the integrity and reliability of the chip's security functions. Evaluations can be performed using the 'Common Criteria' to rank and assign an evaluation level to the smart card that represents the level of assurance of its security properties and services [35]. A card of the appropriate level can be chosen for a given application. Cards used in financial transactions like EMV are typically evaluated to EAL4 and above.

Figure 6 illustrates a payment card with an embedded chip (circled in red).



FIGURE 6 – AN ILLUSTRATION OF AN ISO 7816 CHIP PLACED IN A PAYMENT CARD (Source: <http://en.wikipedia.org/wiki/File:Smartcard2.png> licensed under Creative Common Share Alike)

The rollout of EMV required that new chip-containing payment cards be issued to cardholders, along with new EMV terminals and PIN entry devices issued to merchants.

The worldwide deployment of EMV is shown in Figure 7 below:

Worldwide EMV Deployment and Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Caribbean	182,185,043	26.4%	2,000,000	55.6%
Asia Pacific	305,126,927	26.6%	3,200,000	41.6%
Africa & the Middle East	16,841,874	13.7%	348,000	62.5%
Europe Zone 1	555,688,434	65.4%	9,400,000	84.7%
Europe Zone 2	22,817,271	11.5%	457,800	61.2%
United States†				
TOTALS	1,082,659,549	36.0%	15,405,800	65.0%

* Figures reported in September 2010 and represent the latest statistics from American Express, JCB, MasterCard and Visa, as reported by their member financial institutions globally.

† Figures do not include data from the United States.

FIGURE 7 – WORLDWIDE EMV DEPLOYMENT AND ADOPTION (Source: EMVCo www.emvco.com)

EMV isn't the first wide-scale application of smart card technology. Similar challenges were faced by the mobile communications industry in the late 1980s and early 1990s, when the first generation analogue mobile networks saw significant increases of mobile phone cloning and eavesdropping. The response was the introduction of the Subscriber Identity Module or 'SIM Card' in 2G networks and mobile handsets creating the largest number of smart cards (or smart tokens, since the SIM card is not actually a full-sized card) in general use for any industry to date. What's more, with over two billion 'SIM Cards' deployed, they can be credited for having pushed the envelope in technical advances and functionality in smart card technology. And that as a result, they reduced the overall cost of implementing smart card-based applications – paving the way for their adoption in finance, identity, transport, physical access control and other applications [34].

What *is* interesting about the EMV application is that it is the first wide-scale deployment of smart card technology for use in an electronic payment system.

It's worth briefly examining the EMV application in more detail for the following reasons:

1. It contains features that are important in secure systems and smart card applications, including standards-based security protocols, formal security evaluations and the use of strong cryptographic functions to provide certain assurances in payment transactions.
2. It does not completely solve or remove the risk of payment card fraud in CP transactions.
3. It initially resulted in a shift in liability or 'burden of proof' in cases where fraudulent activity still occurred.
4. It is actively being promoted as a platform upon which extra layers of security, including e-banking and 'card not present' e-commerce solutions, can be built.

The EMV specification has been published as four separate 'books' – designed to ensure interoperability between chip cards and terminals on a global basis [36].

Book 1 – Application Independent ICC to Terminal Interface Requirements

Book 2 – Security and Key Management

Book 3 – Application Specification

Book 4 – cardholder, Attendant, and Acquirer Interface Requirements

The *Normative References* section of Book 1 lists the ISO standards relevant to the EMV specification. These include ISO 7816, which defines the physical characteristics of the card, dimensions and location of contacts, interface and communication protocols, as well as security functions and application specific commands. ISO 7816 is the standard that allows payment cards (as well as any other ISO 7816 based cards) and point of sale terminals to interoperate – since a standard ISO 7816 card with a chip can be inserted into and read by a standard ISO 7816 card reader and PIN entry device.

Also included in Book 1 are ISO references to cryptographic mechanisms including hash functions, message authentication codes (MAC), digital signatures as well as symmetric and public key cryptography. A detailed explanation of cryptographic principles and primitives is outside the scope of this paper, however excellent introductions to cryptography and cryptographic mechanisms can be found in [37,38,39].

The main components of the EMV scheme are shown Figure 8.

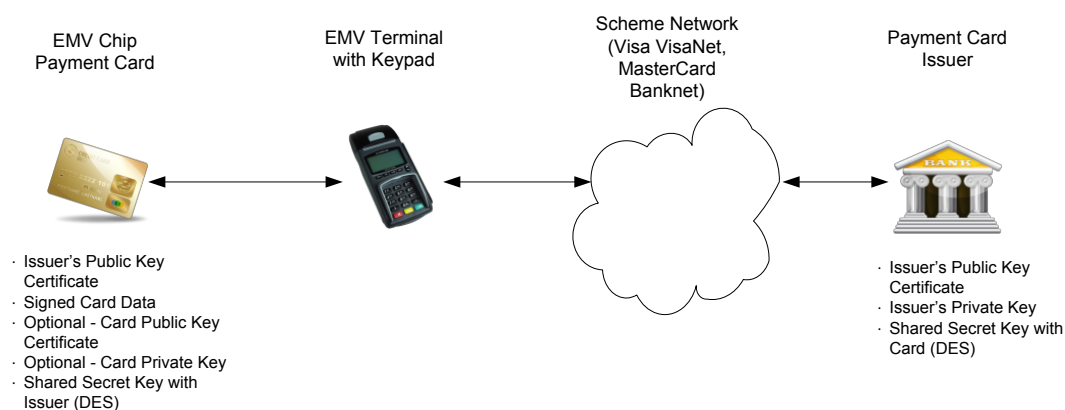


FIGURE 8 – THE MAIN COMPONENTS IN AN EMV APPLICATION

The scheme's security depends on the underlying security properties of the smart card, allowing the card to safely store secret keys that are required in an EMV transaction.

The goal of the scheme is to validate payment card data – ensuring that a valid card is being used, as well as optionally perform mutual authentication between the payment card and card issuer.

The scheme can also verify the cardholder via cardholder verification methods (CVMs). One method is to request a PIN number from the user – entered into the terminal keypad. Another familiar and still valid method is to request the cardholder sign a receipt – as with previous magnetic stripe cards. The decision to use either may depend on the capabilities of the terminal and the phase of EMV adoption. Using a PIN number in conjunction with a valid card provides what is referred to as ‘two factor’ authentication: Something the cardholder ‘has’ – i.e. the payment card – as well as something the card owner ‘knows’ – i.e. the PIN number.

The scheme is flexible in terms of making risk-based decisions about how a transaction will proceed. Based on policies set by the issuer and acquiring banks, the terminal and the card can decide on which CVM method to use. Processing a transaction ‘offline’ means the cardholder is verified without connecting to the scheme network and card issuer, saving connection and network costs. Proceeding ‘online’ involves connecting to the scheme network, and performing card-to-issuer authentication and transaction authorisation. The card can be programmed to ‘go online’ depending on the number of previous offline transactions that have occurred, or based on transaction value or other parameters. The terminal can decide to go online based on: floor limit checking (to protect against an attempt to split transactions into smaller individual transactions); velocity checking (lower and upper limit checking of the number of offline transactions that can be performed before the transaction must go online); random transaction selection; or where an exception list of cards exists. In other words, both the card, and the terminal can decide to reject or approve a transaction ‘offline’ or request that the transaction proceed ‘online’ for further processing and checks.

The high level phases of an EMV transaction (as per Book 3) are:

1. **Initiate the Application Processing** – the terminal informs the chip on the card that a new transaction is beginning, and exchanges a list of files and records that contain the chip data that will be used in the processing of the transaction.
2. **Read Application Data** – the terminal reads the files and records described in step 1 above.
3. **Perform Card Data Authentication** – the terminal authenticates the card data using one of three possible data authentication schemes: Static Data Verification (SDA); Dynamic Data Verification (DDA); or Combined Data Verification (CDA). This step may be performed at any point after *phase 2 – Read Application Data* but before *phase 7 – Terminal Action Analysis*.
4. **Processing Restrictions** – the terminal checks compatible application version numbers, usage control and expiry dates. This step may be performed at any point after *phase 2* but before *phase 7*.
5. **Cardholder Verification** – the terminal assures that the person presenting the card is the person to whom the card was issued. Assuming the card can perform cardholder verification, one of the issuer-specified cardholder verification methods

(CVMs) will be executed. This may include online or offline PIN verification. This step may be performed at any point after *phase 2* but before *phase 7*.

6. **Terminal Risk Management** – depending on its capability, the terminal will perform risk management functions – as described above – including floor limit checking, random transaction checking, velocity checking. Terminal risk management may be performed at any time after *phase 2* but before issuing the first GENERATE AC command.
7. **Terminal Action Analysis** – once application processing in a normal transaction has reached this stage, the terminal makes the first decision as to whether the transaction should be approved offline, declined offline, or proceed online. If the terminal decides to approve the transaction offline, it will send a ‘GENERATE AC’ (generate application cryptogram) command to the card, requesting a transaction certificate (TC). Alternatively, if the terminal rejects the transaction offline, it may send a ‘GENERATE AC’ command to the card, requesting an application authentication cryptogram (AAC).
8. **Card Action Analysis** – in response to the ‘GENERATE AC’ command from the terminal, the card performs its own issuer-specific risk management functions: either approving the transaction offline by returning a TC, or by requesting to go online by returning an application request cryptogram (ARQC); or declining the transaction by returning an AAC.
9. **Online Processing** – if the terminal has received an ARQC from the card in response to the first ‘GENERATE AC’ command, the terminal then attempts to go ‘online’ to facilitate card-to-issuer mutual authentication via application request cryptograms (ARQC) and application response cryptograms (ARPC). Book 3 of the EMV standard describes this phase as similar to the processing of magnetic stripe card data, noting, “Actions performed by the acquirer or issuer systems are outside the scope of this specification”. In practise, cryptograms generated using the issuer’s stored keys from the card as well as from the issuer, are used to perform mutual card and issuer authentication. When the terminal receives the response from the issuer, the response is forwarded to the card – along with an EXTERNAL AUTHENTICATION command, or a second GENERATE AC command. If card and issuer authentication has succeeded and the issuer has approved the transaction (including in the replying ARPC), then the card will reply with either a TC (approved) or an AAC (declined).
10. **Issuer-to-Card Script Processing** – if the transaction has gone ‘online’ the issuer may respond with an issuer Script that can be processed by the card before or after the second ‘GENERATE AC’ command. Issuer scripts can be used to perform management functions and updates on the card.

11. **Completion** – the terminal performs this function as the last function in the transaction – after the card has indicated it is completing the transaction by issuing a TC, or an AAC in response to the first or second ‘GENERATE AC’ command.

It's worth looking at *phase 3 Perform Data Authentication* in more detail since it is this component (along with cardholder Verification) that provides the core assurances and advantages over magnetic stripe cards.

Performing Data Authentication assures the terminal that the card in use is genuine and has not been tampered with or is not counterfeit. Data Authentication relies on a complete public key infrastructure (PKI) in which the payment card scheme network (e.g. Visa or MasterCard) acts as the Certificate Authority (CA). The CA signs and creates certificates for card issuers' public keys – copies of which are placed on the payment card for retrieval by EMV terminals. The CA public key is also distributed and placed on all EMV terminals so that they can retrieve and verify the issuer's public keys on the card.

As mentioned earlier, there are three methods of card data authentication, which bear further examination here.

1. Static Data Authentication or SDA (Figure 9)

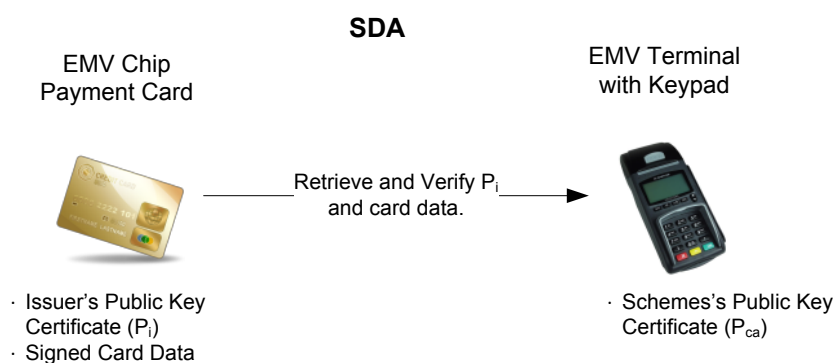


FIGURE 9 – OFFLINE STATIC DATA AUTHENTICATION (SDA)

SDA is performed as follows:

1. The terminal retrieves the card issuer's public key certificate (P_i) as well as the card data that has been signed by the issuer's private key.
2. The terminal verifies the issuer's public key P_i (which has been signed and certified using the CA/Scheme private key) using the scheme's public key P_{ca} (which is placed in all terminals).
3. The terminal then uses the verified P_i to verify the signed card data.

If successful, SDA assures the terminal that the card data has not been modified since it was issued by the issuer.

The primary advantage of SDA is that no public key cryptographic processing is required by the card. Cards without public key cryptographic processors cost less, and so, issuing SDA cards results in cost savings.

The disadvantage of SDA is that, for offline transactions, it is theoretically possible to clone the signed card data, creating a counterfeit card. A PIN would not be required for a counterfeit SDA card since the card could be programmed to accept any value for a PIN number [40].

2. Dynamic Data Authentication or DDA (Figure 10)

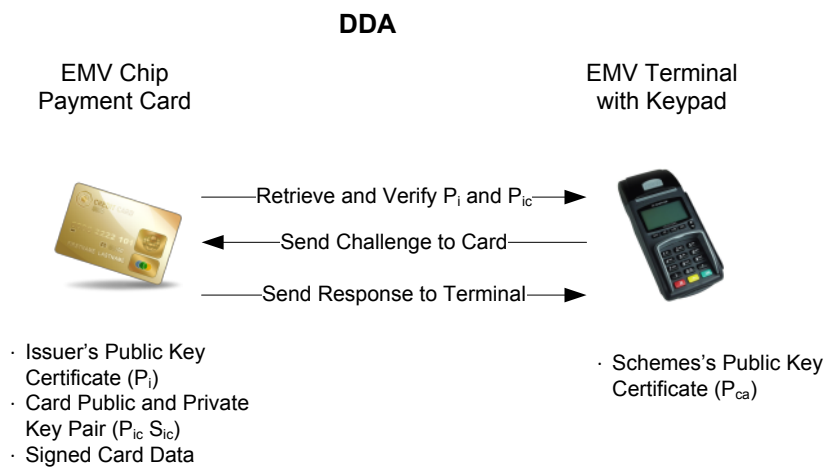


FIGURE 10 – OFFLINE DYNAMIC DATA AUTHENTICATION (DDA)

DDA requires a smart card that is capable of performing public key cryptographic functions. When the card is manufactured, a card-specific private (S_{ic}) and certified public (P_{ic}) key pair is placed on the card. The key pair is used during card data authentication as well as optionally for secure transmission of the PIN to the card during CVM.

DDA is performed as follows:

1. The terminal retrieves the issuer's public key P_i and the card public key P_{ic} certificates from the card. The issuer's public key P_i is verified by the terminal using the scheme's public key P_{ca} . The card public key P_{ic} is then verified using the issuer's public key P_i .
2. The verified card public key P_{ic} can now be used by the terminal to send a challenge that has been encrypted with the card public key P_{ic} .
3. The card decrypts the challenge using the card private key S_{ic} . The card then returns the challenge as well as the signed card data to the terminal for verification.

The advantages of DDA include the fact that the card is actively participating in a cryptographic challenge and response using public key cryptography. It is therefore able to authenticate the card data, as well as provide assurances that the data has been returned

from an active and valid card. This assurance is provided by the security features of the smart card – which include secure key storage and tamper resistance – making it practically infeasible for a counterfeit card to be produced that contains the private key S_{IC} .

The disadvantages of DDA include the fact that it requires a card with a public key cryptographic processor, which in turn increases the cost of the card. It is also theoretically possible to perform a ‘wedge attack’ on a stolen DDA card. This is an attack in which valid DDA data is used to pass data authentication, but where a ‘wedge’ or ‘man in the middle’ device is used to answer ‘yes’ for any PIN CVM attempt. The ‘wedge’ then simulates remaining card actions in order to obtain authorisation for payment [41]. This is effectively a time-of-check-to-time-of-use (TOCTTOU) exploitation.

3. Combined Dynamic Data Authentication with AC Generation or CDA

Combined Dynamic Data Authentication is performed at the first or second GENERATE AC command from the terminal. In this case, DDA is performed simultaneously with the response to the GENREATE AC command and so the response (TC, ARQC or AAC) can be verified **at the same point in time** as the card data is verified via DDA.

The advantage of CDA is that it makes performing the ‘wedge’ attack described above practically infeasible.

2.4.2 EMV Advantages

EMV offers the following advantages over traditional magnetic stripe CP transactions:

1. The use of smart card technology provides portable security services and secure key storage.
2. Flexible risk management options allow policy-based settings in the card or terminal to ‘decide’ if the transaction can be completed offline, or must proceed online – offering cost savings in offline transactions.
3. Despite the well documented challenges of implemented x509 certificate-based public key infrastructure (PKI) [42], EMV successfully uses public key cryptography and scheme-based PKI to allow EMV cards and terminals to engage in a dialogue that validates card data and assures the terminal – and therefore the merchant – that the payment card is authentic and valid.
4. The use of PIN entry as a cardholder verification method ‘binds’ the card to the cardholder, providing two-factors of authentication (something the cardholder possess, and something the cardholder knows).
5. The use of online processing – combined with shared symmetric keys between the card and issuer – allows the card and issuer to mutually authenticate and exchange messages via message authentication codes (MAC) and cryptograms. This is an extremely important feature of the scheme, since it provides online message-level

end-to-end security – including data origin authentication and non-repudiation services.

2.4.3 EMV Disadvantages

The disadvantages of EMV are:

1. Implementing the scheme is costly, and includes issuing new cards and terminals.
2. SDA-only cards are vulnerable to card cloning and fraud in offline transactions [40].
3. PIN codes can be observed via ‘shoulder surfing’ while a cardholder enters their PIN into a terminal.
4. The terminal itself is outside of the cardholder’s control and so the cardholder could be ‘tricked’ into inserting their card into a fake EMV terminal. Fake EMV terminals can collect PIN and card details, which can be used to create either counterfeit magnetic stripe cards, or counterfeit SDA chip cards for offline authentication [43].
5. Although requiring careful co-ordination and an active attack against the cardholder, EMV cards (including DDA cards) could also be vulnerable to a ‘relay attack.’ In a relay attack, the cardholder places their card in a fraudulent terminal. The data and instructions from the valid card are then relayed to another terminal, where the products, services and price can be changed before authorising the transaction [44].
6. Prior to 2009 in the UK, banks (card issuers and acquiring banks) operated under a voluntary code of practise known as *The Banking Code*. Under this scheme, the technological advances of EMV shifted the ‘burden of proof’ and ‘reasonable care’ to the cardholder for any fraudulent activity involving chip and pin cards. The claim made by the banks in this case was that their system was ‘secure’ and so, therefore, any fraudulent activity must be the fault of the cardholder for not taking ‘reasonable care’ to ensure that their payment card was safe and being used correctly. This was seen by some as the banks ‘dumping’ their payment card risk onto their customers [40]. On the 1st of November 2009, responsibility for the regulation of deposit and payment products transferred to the Financial Services Authority [45]. Under the FSA, the onus has returned to the banks to prove negligence or fraud by the cardholder.

2.4.4 EMV Summary

In summary, the intrinsic security features of smart card technology, combined with a standards-based implementation, has meant that EMV has increased the security of CP transactions. This has resulted in a significant reduction of CP transaction fraud [27]. That said, the security of any system represents at best, a balance between usability, effectiveness, cost, and the acceptance of any unmitigated or residual risks that remain after the system has been implemented. It remains to be seen how over the long-term, EMV will

perform, and whether documented and more sophisticated payment card system attacks will force the payment card industry to further revise and improve the security of the scheme.

More interestingly, and particularly relevant to the remainder of this paper, the success of EMV has been attributed to a rise in fraudulent ‘card not present’ transactions [46], such as the use of credit or debit cards to make payments online via the Internet. Fraudsters have shifted their attention to what may now be perceived to be the weakest link in the use of payment cards: payment cards used in e-commerce.

2.5 The Security of ‘Card Not Present’ Transactions

Visa defines a ‘card not present’ (CNP) [47] transaction as:

“... a transaction that takes place remotely – over the internet, by telephone or by post.”

Mail order (by post) and telephone order transactions are also sometimes referred to as MOTO transactions.

CNP transactions are particularly vulnerable to fraud for three significant reasons:

1. The card data cannot be verified via a magnetic stripe or EMV chip.
2. The cardholder cannot be verified by comparing a signature with the signature stripe or by entering a PIN into an EMV terminal.
3. The cardholder may initially be unaware that their card details are being used fraudulently in CNP transactions (unlike the physical theft of a payment card).

CNP transactions also require a very different trust relationship between the customer and merchant, since goods cannot be given to the customer at the time of payment.

In MOTO transactions, the cardholder can establish a degree of trust via traditional means, including:

1. Dealing with well known or recognised brand.
2. Ordering from a well-known catalogue. A company that is going to make the investment required to print and distribute a catalogue is perhaps ‘more likely’ to be a legitimate merchant than not.
3. Verifying the merchant’s telephone number, address and directory listing.
4. A recommendation from a friend.
5. Previous experience.

There is still a chance that a merchant could act in bad faith – not delivering goods and services.

Consumer protection legislation combined with the rules and regulations of the scheme will provide the cardholder protection against fraudulent merchant activity as well as the fraudulent use of their card details [48]. Scheme protection in particular will allow a cardholder to dispute a fraudulent payment transaction in order to receive a refund. If a disputed claim is successful, it will result in a 'chargeback' initiated by the card-issuing bank against the acquiring bank and merchant. The merchant's account will be debited and the funds returned to the cardholder.

'Chargebacks' are an important form of consumer protection from unscrupulous merchants, encouraging merchants to supply the goods and services as advertised. However, they also represent a significant risk to 'good' merchants from payment transactions that have been deemed fraudulent (for example where payment card details have been used without the consent of the cardholder).

In an attempt to reduce the merchant's risk of fraudulent CNP transactions, payment card manufacturers added another cardholder verification method: a three-digit value printed on the back of the payment card, known as CVV2. As mentioned previously, the first CVV value to be used was a cryptographic checksum stored in the magnetic stripe of the card in an attempt to validate card data. The CVV2 value printed on the back of the card is also a cryptographic checksum; however it is not hidden, and can be requested during a CNP transaction.

CVV2 was an attempt to add 'something known' only by the cardholder to the transaction. Historically, card details including embossed PAN, expiry date and cardholder name could be retrieved from receipts, casual observation, or even overheard during a telephone transaction. The CVV2 value is not part of regular CP transactions; it is requested in CNP transactions. However, the fact that it is visible on the reverse side of the card, for anyone who handles the card to see, means that the CVV2 is also vulnerable to collection, and is a weak form of cardholder authentication.

The methods of establishing trust and authorisation in MOTO transactions have mostly been carried forward onto the Internet via the use of a web browser and SSL. These methods have included the use of CVV2 values, as well as cardholder protection in the form of merchant chargebacks. However, there are additional risks when payments are made online – risks that are unique to the use of an open and effectively anonymous communication network like the Internet.

On the Internet, it becomes increasingly difficult to verify the identity and establish the trustworthiness of communicating parties – whether it is the 'trustworthiness' of a web site, or the 'trustworthiness' of the payment card details. (A problem now famously epitomised by Peter Steiner's cartoon and caption published in *The New Yorker* on July 5, 1993 – "On the Internet, nobody knows you're a dog." [49,50].)

The next section examines some of these issues and how they relate to e-commerce payments made using a web browser and SSL.

2.6 E-commerce via a Web Browser and SSL/TLS

2.6.1 Introduction

As established in section 1.2 – *The Birth of E-commerce*, SSL and its successor Transport Layer Security (TLS) facilitated growth in e-commerce. However, the difficulty of establishing the ‘trustworthiness’ of communicating parties on the Internet also highlights several fundamental weaknesses that occur when attempting to transfer a real-world ‘payment instrument’ onto the Web.

Figure 11 illustrates the ‘straight-line’ communication between a user, using a web browser, and an e-commerce merchant, using an SSL certificate, to enable a secure channel between the browser and the merchant’s website.

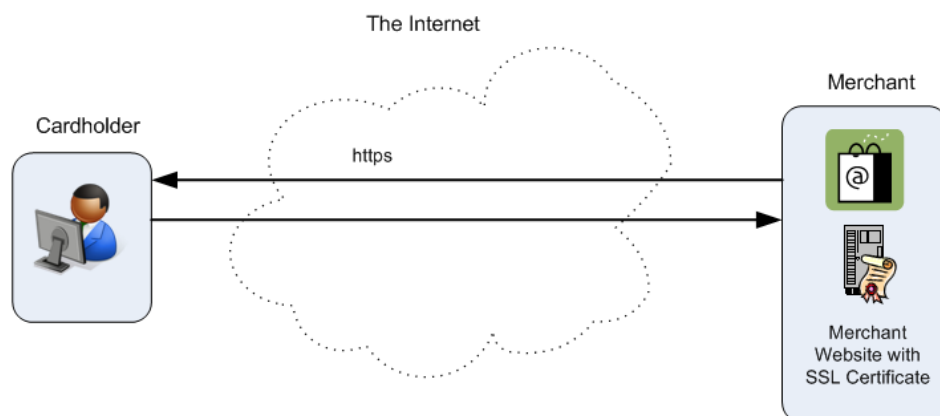


FIGURE 11 – E-COMMERCE VIA A WEB BROWSER AND SSL/TLS

Figure 12 shows Microsoft’s Internet Explorer browser visiting the ‘Sign In’ page for Amazon.com. The only indication the user has been given, that they are visiting a web page that is ‘secure,’ is the small padlock symbol to the right of the address line in the browser window (circled in red). More astute users may also notice that there is now an ‘s’ appended to the ‘scheme’ portion of the Uniform Resource Locator (URL) of the page – https – indicating the use of Hypertext Transfer Protocol Secure (HTTPS).

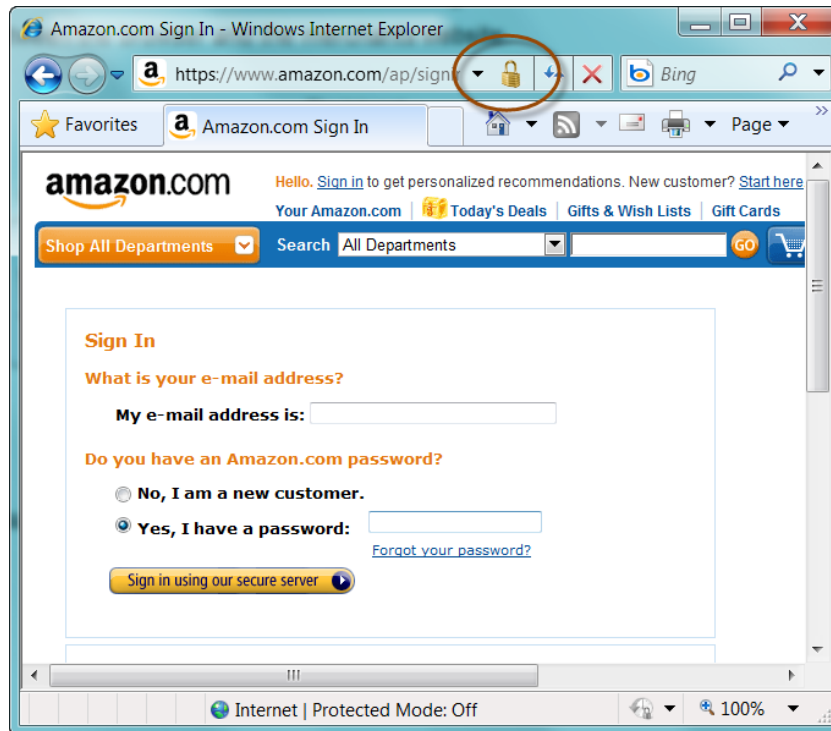


FIGURE 12 – A WEB BROWSER VISITING A SECURE PAGE AT AMAZON.COM

In Figure 12, the user is about to enter their email address and password. However, from the visual cues provided, it's unlikely that the average internet user is going to be aware of the current 'state' of their connection to the website. Amazon – perhaps realizing this, and in an effort to establish trust – has included another visual security cue in the form of a descriptive button which reads: 'Sign in using our secure server.'

Nevertheless, the user is expected to 'trust' that the site they are visiting is in fact Amazon.com – again by paying careful attention to the address line in their browser window. Page artwork, logos, and text on the page certainly give the impression that user is visiting Amazon.com. But this artwork and text could have been copied, and the site they are visiting could be <http://www.amazo.com>, <http://www.amazon-deals.com>, <http://www.amazon-sign-in.com>, or even <http://www.amazon.ru>.

The user could attempt to verify the SSL certificate that has been issued to the website.

Figure 13 shows an image of the pop-up window that appears in Internet Explorer when a user 'clicks' on the secure padlock icon.

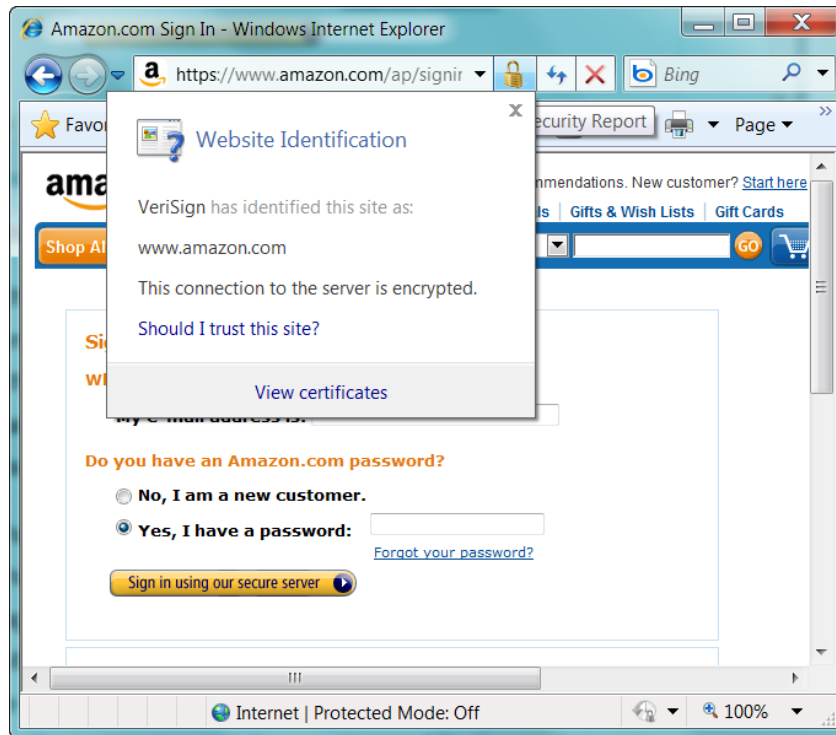


FIGURE 13 – VIEWING CERTIFICATE INFORMATION FROM AMAZON.COM

Although there is helpful text available that describes some of the issues associated with trusting a website, clicking on the View certificates link reveals the following in Figure 14:

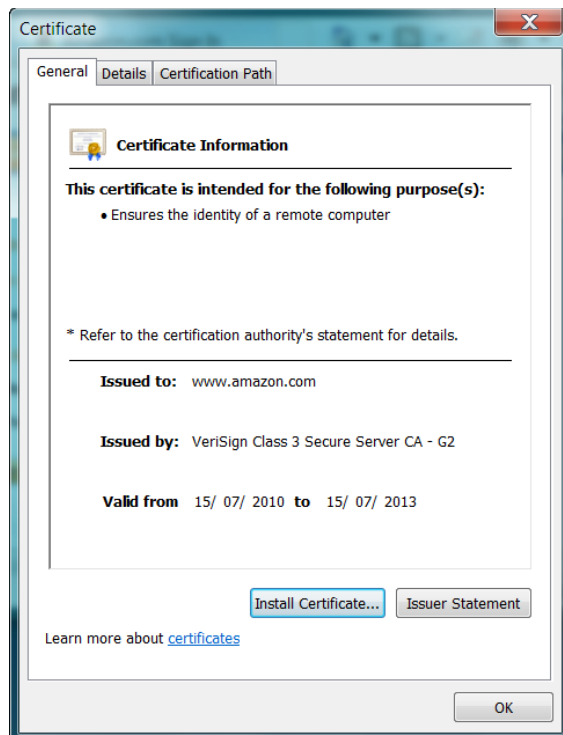


FIGURE 14 – CERTIFICATE INFORMATION FOR A WEBSITE

It's unlikely that the user is going to understand what SSL/TLS, HTTPS, or the certificate details above actually mean in terms of their connection to the website in question.

What's more, the challenges a user faces in correctly identifying a web site, the address of a website, and the current state of their browser's connection to a web site have been effectively exploited in what are commonly referred to as 'phishing attacks'. A phishing attack is an attempt by a malicious party to masquerade as a 'trusted' source or website in an attempt to retrieve sensitive information like usernames, passwords and payment card details. Phishing attacks are a form of 'social engineering' and have been highly effective on the Internet [51,52,53,54] – mainly because of the 'poor usability' issues described above.

Of course, it can't all be bad. The latest versions of the major Web browsers (Internet Explorer, Firefox, Chrome) have made modest improvements in helping to warn a user if the site they are visiting is a potential phishing site, or whether there are problems with the SSL/TLS certificate the website is using. Major e-commerce sites and banks are also vigilant in monitoring and initiating the removal of fraudulent or 'phishing' websites. Most have also implemented awareness and user education campaigns in order to help users understand the importance of the domain name portion of the URL and site certificates. Users are still vulnerable to phishing attacks – however these efforts, along with a familiar 'direct account-based' method of payment card authorisation have meant that the e-commerce industry has been able to grow to the size that it is today.

2.6.2 Web Browser and SSL/TLS Advantages

The advantages and disadvantages of e-commerce via a web browser and SSL/TLS can be summarized as follows:

1. The use of a payment card as a payment authorisation technique is well known and understood by consumers and merchants.
2. The SSL/TLS protocol comes free with most web browsers.
3. The major SSL/TLS certificate providers have root certificate authority public key certificates pre-installed with all major web browsers.
4. Apart from a web browser, no additional software is required by the customer.
5. The shopping cart and check-out metaphors employed by many e-commerce websites are generally easy for a user to understand and use to successfully 'check-out' and authorize payment.
6. Scheme protection against fraudulent activity in the form of chargebacks allows cardholders to shop online with increased confidence.

2.6.3 Web Browser and SSL/TLS Disadvantages

The disadvantages of e-commerce via a web browser and SSL/TLS can be summarized as follows:

1. The user and the merchant both have significant 'trust' challenges. The user is expected to reliably determine that they are communicating securely with the intended merchant's website by viewing the 'closed padlock' and other browser indicators including the domain name and other certificate symbols, information or warnings. In this respect 'phishing attacks' have substantially increased the risk to the user from rogue or 'faux' websites [51].
2. Even if a user is savvy enough to determine that the SSL certificate and domain name of an e-commerce site is in order, the merchant has no equivalent method of verifying the user. Mutual authentication via SSL is almost never performed. It is therefore difficult for the merchant to determine that the payment card details they had received were supplied by the cardholder, and not someone impersonating the cardholder for fraudulent purposes.
3. Securing the connection between the browser and a website via SSL/TLS says nothing about how sensitive information like credit card and payment details might be handled **after** they have been delivered to the receiving end of an SSL connection. SSL/TLS is not an end-to-end payment transaction protocol. It is a means to secure the communication between two points only. The payment cards details (include all of the details required to initiate a transaction elsewhere, including PAN, cardholder name, expiry date, address and CVV2 values) are transmitted without anything equivalent to an electronic signature or other cryptographic protection. What's more, the same details are being used over and over again at many different sites, increasing the risk of this information falling into the hands of fraudsters with each use. (As an aside, if the PAN and related data were considered the 'keys' to the transaction then from a 'cryptographic' point of view their use in this way would be considered a particularly bad key management strategy.)
4. Since the user's details including full name and address almost always accompany the payment card details, the user has no way of performing an anonymous transaction (unlike the use of cash).
5. There is limited protection to the merchant from chargebacks, whether from fraudulent use of payment card details, or repudiation by the client in the case of a 'false' claim.

2.6.4 Web Browser and SSL/TLS Summary

As we can see, the security of CNP transactions via a web browser and SSL/TLS are lacking in many respects. They are without even the (now relatively weak) protections afforded by magnetic stripe transactions, and with none of the protections afforded by EMV.

As a result, several additional verification and policy-based protection measures have been used to help reduce levels of fraud in payment card based e-commerce, including:

1. Where available, an address verification service (AVS) can check that the numerical address, entered by the user as their 'billing address' during check-out, matches the numerical portion of the registered cardholder's address .
2. Payment processing companies (acting on behalf of merchants) may also perform additional checks – including attempting to verify that the customer is using a computer and web browser with an IP address that originates from the same country as the cardholder's address.
3. Merchants may also implement their own policy-based controls – such as allowing a customer to request purchased goods be delivered to an address other than the cardholder registered address only **after** they have made one or more 'good' purchases from the site.

Despite these attempts at protecting CNP transactions, payment card fraud in e-commerce continues to rise. The HSBC UK website has the following to say about fraudulent activity in CNP transactions [46]:

“Card not present (CNP) fraud is perpetrated by telephone, mail order, fax or the internet and has seen a dramatic increase from £29.3m in 1999 to £290.5m in 2007. It is now the most prevalent category of fraud in the UK.

This figure is expected to continue to rise as fraud becomes more difficult to undertake in the face-to-face environment as a result of initiatives like chip and PIN.”

The success of EMV itself combined with the above noted weaknesses in relying on web-based e-commerce via SSL/TLS highlights the use of payment cards online as an attractive target for fraudulent activity.

In fact, it could be argued that the use of payment cards in a way never intended (like the Internet itself) is in part responsible for another entire industry of payment card related processing, security, security consulting and compliance related activities. The most significant of these developments is the PCI Security Standards Council Data Security Standard (PCI-DSS) [55]. The standard was created by Visa and MasterCard and includes a set of over 200 auditable controls designed to protect payment card data. Levels of compliance with the standard are set depending on the levels of transactions being processed. High-profile security breaches such as the loss of 40 million credit cards by CardSystems solutions in 2005 [56] are an indication of the size of the problem, as well clearly defining the motivation behind the creation of such a standard. However compliance

with the standard introduces additional costs to the merchant, in the form of upgrading systems, verifying compliance (internal or external audits) and maintaining compliance [57].

2.7 An E-commerce Requirements Checklist

The current technological convergence of the Internet, e-commerce, smart card technology and, in particular, mobile technology, suggest that opportunities exist to improve the security of e-commerce using payment cards. Opportunities may also exist to introduce alternative schemes, possibly even 're-introducing' some of the advantages that exist in cash and cash-like schemes. What's more, the current figures for losses against CNP transactions would suggest that alternatives to web browser based SSL/TLS payment card e-commerce can and should now be justifiably funded.

An ideal requirements wish-list for online payments in e-commerce might look something like the following:

1. **Confidentiality** – The payment scheme should offer optional levels of confidentiality – allowing details of the transaction to only be made known to those parties to whom the customer or merchant so wishes.
2. **Integrity** – The scheme should maintain the integrity of the transaction – making tampering or changes to the details of the transaction practically infeasible.
3. **Authentication** – The scheme should provide methods for the authentication of communicating parties and/or the authentication of messages that are relied upon for payment authorisation – making fraudulent activity difficult.
4. **Non-Repudiation** – The scheme should provide non-repudiation services – protecting both the merchant and customer against false claims.
5. **Availability** – The scheme should be highly available – allowing customers and merchants to participate in payment transactions when required.
6. **Implementation** – The scheme should provide clear benefits to merchants and customers justifying any costs associated with the scheme's implementation. The implementation details should attempt to abstract complexity and provide interfaces with merchant systems that represent good practises in software development in general.
7. **Interoperability** – The scheme should be interoperable – providing the widest possible access to merchants and customers.
8. **Ease of Use** – The scheme should be easy to understand and use for the customer.
9. **Scheme Protection** – The scheme rules and policies should continue to provide consumer protection from unscrupulous or fraudulent merchants. The scheme rules, policies and regulations should also continue to protect the payer when a claim of fraudulent activity is made. The onus should be on the scheme owners to disprove the validity of the claim, and not rely solely on the mechanisms of the scheme to automatically dispute such claims.

With our requirements ‘wish-list’ in hand, and our list of advantages and disadvantages of e-commerce via a web browser and SSL/TLS above, let’s see how the two compare.

Web Browser and SSL/TLS Score Card		
Requirement	Result	Comments
Confidentiality	Poor	Apart from the secure channel between the web browser and the web server via the use of SSL/TLS, there are no message-level assurances (encryption or digital signatures) for card and order details. Both the complete payment card and order details will be available to the merchant.
Integrity	Poor	As in ‘Confidentiality’ above, the lack of message-level assurances (encryption, digests or signatures) means that the integrity of a payment transaction cannot be assured.
Authentication	Poor	Only the merchant website is authenticated via a server certificate that is bound to the domain name of the merchant website. Modern web browsers assist users in determining the validity of a web server certificate. However, user awareness and education are also required in order to ensure that the customer is visiting the intended site with a valid certificate. The authentication of payment instructions performed by CVV2 verification, and optionally AVS where available – are considered weak forms of cardholder authentication.
Non-Repudiation	Poor	The lack of message-level signatures means that assurances for non-repudiation are not provided.
Availability	Good	Modern browsers, including mobile variants and web servers, are able to negotiate SSL/TLS sessions. There are no intermediate services or entities involved and so, the availability of the system is ‘as good as’ well established web server technology and SSL/TLS implementations.
Implementation	Good	All modern browsers include SSL/TLS. The process of applying for and installing server-based SSL/TLS certificates is straightforward and relatively inexpensive. Since SSL/TLS is a transport layer protocol it can be implemented with minimum application level changes.
Interoperability	Good	SSL/TLS is an Internet Engineering Task Force (IETF) standard, and nearly all modern browser and web servers are able to successfully negotiate SSL/TLS connections.
Ease of Use	Good	Apart from a web browser, no additional software is required by the user. The SSL/TLS session can be established by the server by redirecting the client to a secure page.
Scheme Protection	Good	Scheme protection against fraud on behalf of the cardholder in the form of chargebacks has meant that – despite weaknesses in confidentiality, integrity, authentication, and non-repudiation – consumers have generally been willing to use their payment cards online.

It’s interesting to note that the ‘good’ characteristics of availability, implementation, ease of use and scheme protection appear to have outweighed the ‘poor’ characteristics for confidentiality, integrity, authentication, and non–repudiation in the adoption of web browser based e-commerce via SSL/TLS.

We’ll now briefly examine a scheme that attempted to satisfy each of the major requirements in our e-commerce checklist above, in an effort to remedy the major security deficiencies of using payment cards via a web browser and SSL/TLS.

2.8 SET – A First Attempt at Securing E-commerce

2.8.1 Introduction

In 1996, the Secure Electronic Transaction (SET) protocol was announced by Visa and MasterCard. The aim of the protocol was to establish an open, multi-party scheme for secure payment card transactions over the Internet.

On December 19th, 1997, MasterCard and Visa formed Secure Electronic Transaction LLC (aka SETCo) to manage and oversee the SET specification [58].

On May 31st, 1997 [58] with assistance and input from GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa and VeriSign – version 1 of the SET protocol was published in three separate books ²:

- Book 1: Business Description
- Book 2: Programmer's Guide
- Book 3: Formal Protocol Definition

Book 1 describes the detailed objectives of SET as:

1. Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
2. Ensure the integrity of all transmitted data.
3. Provide authentication that a cardholder is a legitimate user of a branded payment card account.
4. Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
5. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
6. Create a protocol that neither depends on transport security mechanisms nor prevents their use.
7. Facilitate and encourage interoperability among software and network providers

The SET objectives overlap well with our e-commerce requirements wish-list – particularly in providing message-level authentication and confidentiality services.

SET, like EMV, relies on a complete public key infrastructure (PKI). However, unlike EMV, public key certificates are also issued to customers for use with special software that must be installed on their personal computers.

The SET certificate hierarchy is illustrated in Figure 15.

²SETCo website www.setco.org and specifications are no longer available. However, copies of the three books were retrieved from the Cambridge University Security Group and are available from <http://www.cl.cam.ac.uk/research/security/resources/SET/>.

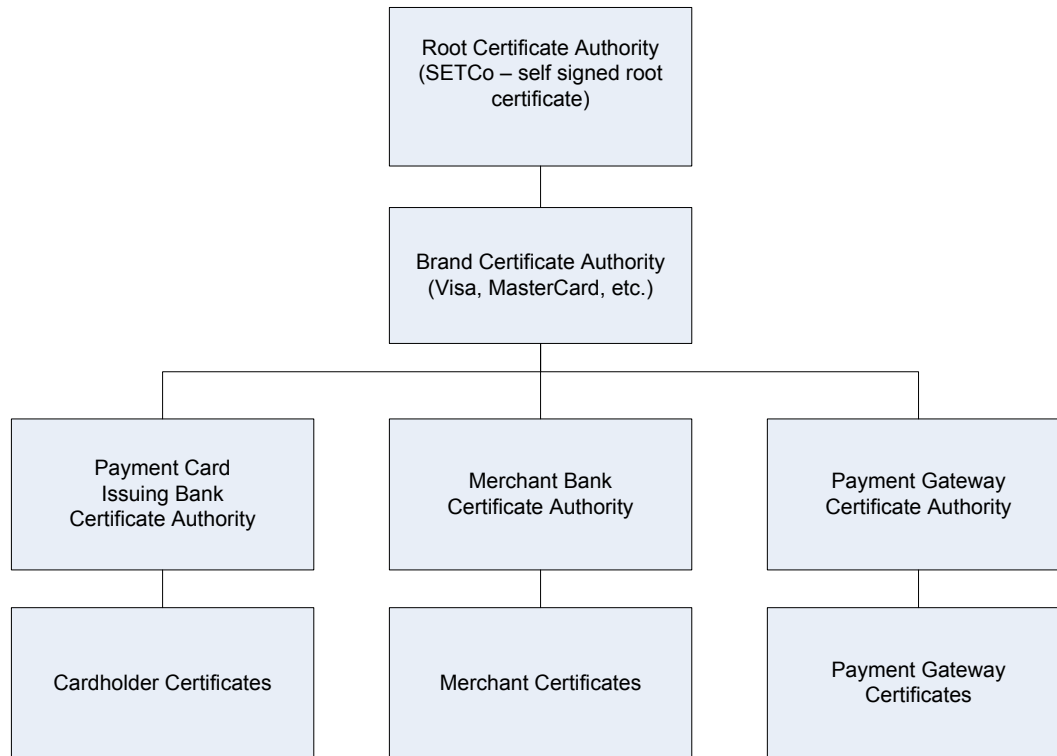


FIGURE 15 – CERTIFICATE HIERARCHY IN SET

The certificate hierarchy allows cardholders, merchants and payment gateways to present certificates in a 'certificate chain.' This allows either party to navigate the certificate chain until they have reached a common certificate authority (CA) – either at the root, brand, or bank level. The common CA can then be used to start the verification of certificates in the chain – continuing back down to the individual cardholder, merchant or payment gateway certificate. The common CA provides a verified public key, which in turn can be used for entity authentication and message-level assurances during a SET transaction.

Cardholders are expected to use their personal computers to 'register' and receive certificates from a payment-card-issuing certificate authority before being able to send SET messages to merchants (as shown in Figure 16).

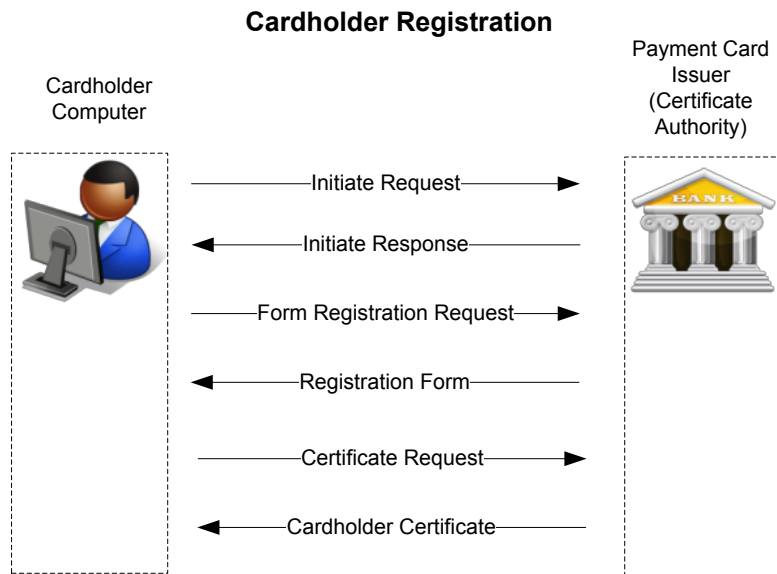


FIGURE 16 – CARDHOLDER COMPUTER REGISTRATION

In order to register, the cardholder's computer must have the SET client software installed. The cardholder initiates a registration request with its immediate CA – the payment card issuer – receiving the issuer's public key and certificates. The software on the cardholder computer navigates the certificate chain and uses the brand or root certificates to verify the issuer's certificate. With a verified issuer public key, the cardholder software generates a session key that can be used to create an encrypted form registration request. It sends this to the issuer, encrypted with the issuer's public key. The issuer returns a registration form and the cardholder software generates a private and public key pair to be used for 'signing' SET transactions. The public signature key along with cardholder details are then returned to the issuer for cardholder certificate creation. The methods of verifying the cardholder details are outside the scope of SET. If the cardholder is successfully verified, the CA returns the cardholder certificate and the cardholder is now ready to participate in SET transactions using their certified signature key pair. The cardholder software vendors are responsible for providing the 'safe storage' of cardholder certificates and key pairs (including private keys) on the cardholder computer.

Merchants and payment gateway processors are expected to perform a similar registration process – proving them with an equivalent certified signature creation key pair.

Once successfully registered with the scheme, cardholders are ready to shop at SET enabled merchant sites. Figure 17 illustrates a SET purchase request.

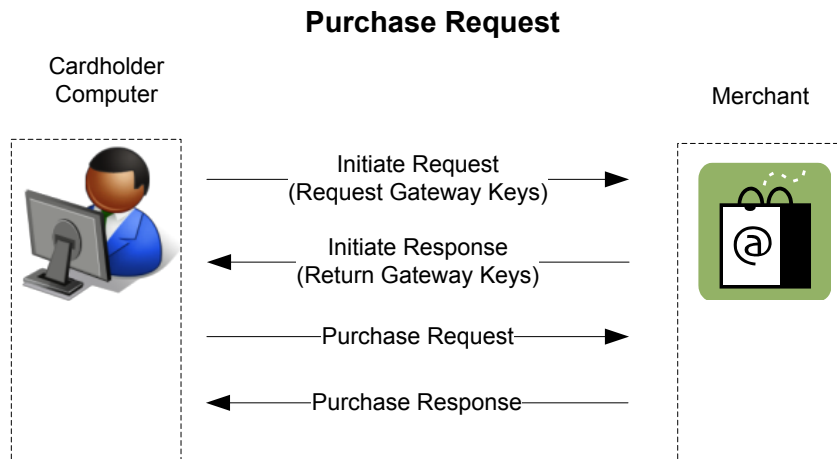


FIGURE 17 – SET PURCHASE REQUEST

The cardholder (having successfully registered with the scheme) selects goods or services from the merchant site including an agreed price and delivery options. Choosing a SET participating payment card as a payment option, will initiate a SET purchase request. This includes a request for the merchant and payment gateway certificate and public keys. The merchant replies with a signed response including the required merchant and payment gateway certificates that correspond to the payment card brand the cardholder is using. The cardholder then prepares order information (OI) and payment information (PI), and creates a 'dual signature' against digests of the OI and PI to be sent back to the merchant in the purchase request.

Dual signatures are particularly interesting, as they introduce a level of confidentiality previously unavailable to payment card users in both CP and CNP transactions. In a dual signature, the OI and PI are signed by the customer using the merchant and payment gateway public keys. In this way, only the respective parts are available to the merchant (in order to view the order information, using the merchant's private key), and the payment gateway (in order to view the payment information, using the payment gateway private key). The digest of the OI and PI is concatenated and signed by the cardholder's private key, so that the OI and PI are 'linked' to a specific order and cannot be tampered with or used separately to initiate a fraudulent transaction. In this way, payment card details of the order can be verified by the merchant and issuer, while the actual card details are kept confidential and unavailable to the merchant. This reduces the likelihood of payment card details being 'collected' and used for fraudulent purposes by the merchant or any intermediaries. Details of the order can also be kept confidential and unavailable to the payment card issuer, satisfying the requirements for optional confidentiality and privacy in the transaction (similar to the use of cash). What's more, if a dispute arises between the merchant and customer, the signed digests of the OI and PI, along with the 'known part' of either the merchant or issuer, can be used to regenerate the message digests. The transaction can thereby be verified – providing non-repudiation services [59].

2.8.2 The SET Result

SET was specifically designed to address the security requirements of Internet-based e-commerce. It provides an end-to-end message-level security system that not only satisfies our “wish-list” of requirements for payment card transactions via the Internet, but actually exceeds the services offered in ‘real world’ payment card usage. SET uniquely provides the additional feature of confidentiality – allowing payment card details to be kept from the merchant, and order information details to be kept from the card issuer. SET comes close to simulating the anonymity of a cash-like scheme, while retaining the convenience of a direct account-based cheque-like payment mechanism using traditional payment cards.

And yet despite having been designed from the ground up as a solution for secure e-commerce, SET failed to achieve implementation success. Possible reasons for failure are described in ‘*Failures of SET Implementations. What’s Amiss?*’ [60] including:

- the complexity of the scheme,
- the requirement for cardholder PC-installed software,
- possible delays in transaction processing time,
- interoperability issues,
- the costs and complexity of managing a large PKI infrastructure,
- the total cost of the investment in the scheme required by all parties.

Installing software on a cardholder’s PC in particular, introduces specific implementation difficulties. Personal computers are ‘uncontrolled’ devices and outside the scope of the scheme – susceptible to unauthorised use as well as malicious software (viruses, worms, Trojans etc.).

Also mentioned by the authors of [60] is the possible lack of end-user involvement in the development of the scheme, combined with an overestimation of end-users’ Internet skills, resulting in an ‘engineer led’ solution.

The importance of usability and the need to create user-focused task-based interfaces for security-related functions are highlighted in the seminal publication ‘*Why Johnny can’t encrypt: a usability evaluation of PGP 5.0*’ [61] and in [62,63]. Equally important is the challenge of developing and deploying security-sensitive client applications in the uncontrolled and insecure personal computer environment.

2.8.3 SET Scorecard

Here's how SET performs against our wish-list of e-commerce requirements.

SET Score Card		
Requirement	Result	Comments
Confidentiality	Good	The use of both public key cryptography and symmetric session keys provides message-level end-to-end confidentiality assurances. The use of dual signatures also provides additional confidentiality and protection – allowing only the merchant and card issuer to see their respective and relevant transaction details.
Integrity	Good	The use of a complete PKI – including signed certificates, message digests and digital signatures – provides the scheme with end-to-end message-level assurances.
Authentication	Good	The use of a complete PKI – including signed certificates, combined with mutual authentication between the customer, merchant and payment gateways – provides the scheme with entity and message authentication assurances.
Non-Repudiation	Good	The use of a complete PKI and signed certificates – including signed message digests – provides both customer and merchant non-repudiation services.
Availability	Unknown	The SET scheme is complex – requiring public key cryptographic processing capabilities for all entities in the scheme and several 'rounds' of dialogue between entities in the scheme. Software implementations on payment gateways may not have been able to cope with large volumes of SET transactions, or may have required special hardware accelerators – increasing the cost of implementation. Since SET never reached wide-scale implementation, it is unknown if availability and performance issues would have hindered the scheme – although lag times of up to 50 seconds were reported [64].
Implementation	Poor	The SET specification is complex – with close to 1,000 pages of documentation, requiring significant resources by the merchant to implement. Special software and certificates must be installed on the customer's PC and, as such, the scheme as initially presented was not portable. The protection of the certificates on the PC is also suspect since PCs are vulnerable to attack from malware (viruses, worms, Trojans) – a point which is specifically raised in Book 1 – Business Description – Scope. Mentioned as "Outside of Scope" is: " <i>[the] Security of data on cardholder, merchant, and payment gateway systems including protection from viruses, Trojan horse programs, and hackers</i> ".
Interoperability	Unknown	Although SET is a published standard, multiple SET vendors (including RSA, Terisa, GlobeSET, VeriFone, IBM, Trintech, Maithean, CyberCash, Brokat, and OpenMarket) each produced their own merchant and customer software implementations – including vendor specific e-wallets to store customer certificates. While SET customers and merchants should be able to interoperate in order to perform SET transactions, it's not clear how easy it would be for a merchant or the customer to change vendors or implementations should they wish to.
Ease of Use	Unknown	Ease of use depends to a large extent on the client software installed on the customer's PC. The authors of [60] suggest difficulty in using the client software may have impacted the adoption of SET. Since client software was produced from multiple vendors, it's reasonable to assume that some implementations may have been 'easier' to use than others.

Scheme Protection	Unknown	Since SET failed to reach wide-scale implementation, it's unclear what scheme rules or protections would have been adopted in order to protect consumers and merchants in the event of a dispute or fraudulent activity.
--------------------------	---------	--

2.8.4 SET Summary

It's interesting to note that SET and e-commerce via a web browser and SSL/TLS have achieved nearly reversed results. SET offers strong security assurances, but a failed implementation, while e-commerce via a web browser and SSL/TSL offers very little security assurances, and yet achieved wide-scale adoption because of its ease of use, ease of implementation and scheme protection.

Remarkably, it would take close to a decade after the SET initiative before another scheme designed to reduce Internet-based CNP fraud would emerge. That new scheme is known as 3-D Secure.

3. 3-D Secure

In 2001 – and after the failure of SET, Visa and MasterCard began the development of two independent schemes designed to improve the security of payment card-based e-commerce. The primary goal of both schemes was the authentication of the cardholder in order to reduce Internet-based CNP fraud. Visa introduced 3-D Secure – branded by Visa as the ‘Verified by Visa’ scheme [65] – while MasterCard introduced the Secure Payment Application (SPA). Despite initial objections to 3-D Secure [66], MasterCard eventually abandoned the full-scale implementation of SPA, and adopted 3-D Secure under the brand name of ‘MasterCard SecureCode’ [67].

3.1 Introduction

As stated above, the primary goal of 3-D Secure is to authenticate the cardholder during a payment transaction in order to reduce CNP payment card fraud. The authentication of a cardholder is what’s missing in a typical Internet-based CNP transaction (unlike the CP equivalent, where the cardholder is present with the card and can be required to perform one or more cardholder verification methods – such as signing a receipt, or entering a PIN number).

3-D Secure requires that cardholders ‘enrol’ in an issuer-managed service, either while making a purchase online, or in advance. The cardholder will typically be asked to choose a password as well as a personal assurance message. During a purchase transaction, the cardholder will be prompted to enter their 3-D Secure enrolment password in order to ‘prove’ that it is in fact the legitimate cardholder making the transaction, and not another party fraudulently using the cardholder’s details. The enrolment credentials are kept completely separate from the payment card and merchant systems and so should not be vulnerable to casual observation or collection (as is the case with the CVV2 value).

Visa refers to this process as ‘Payment Authentication’ [68], although this is technically a misnomer since the payment itself is not authorised or authenticated during cardholder authentication in 3-D Secure. Once cardholder authentication is complete, payment authorisation occurs via the normal merchant acquirer path using a payment card brand proprietary network (e.g. VisaNet or Banknet) to submit an authorisation request to the acquirer for settlement. MasterCard correctly refers to the 3-D Secure component of a payment transaction as ‘Cardholder Authentication’ [69].

The ‘3-D’ in 3-D Secure refers to the ‘Three Domain’ model of the scheme [70,69] which includes:

1. **Issuer Domain:** This domain includes the cardholder and their card issuing bank. In the issuer domain, the issuer manages the enrolment of the cardholder into the

scheme as well as the authentication of the cardholder during a purchase.

2. **The Acquirer Domain:** This domain includes the merchant and their acquiring bank. The acquirer provides transaction processing services and ensures that the merchants are operating under the agreement of the scheme.
3. **The Interoperability Domain:** This is a conceptual domain that describes the ‘interconnect’ between the issuer and acquirer domains. As we’ll see below, a unique feature of the Interoperability Domain is that it relies on the Internet in addition to the traditional and proprietary payment card networks.

Figure 18 illustrates an overview of the scheme’s architecture and components.

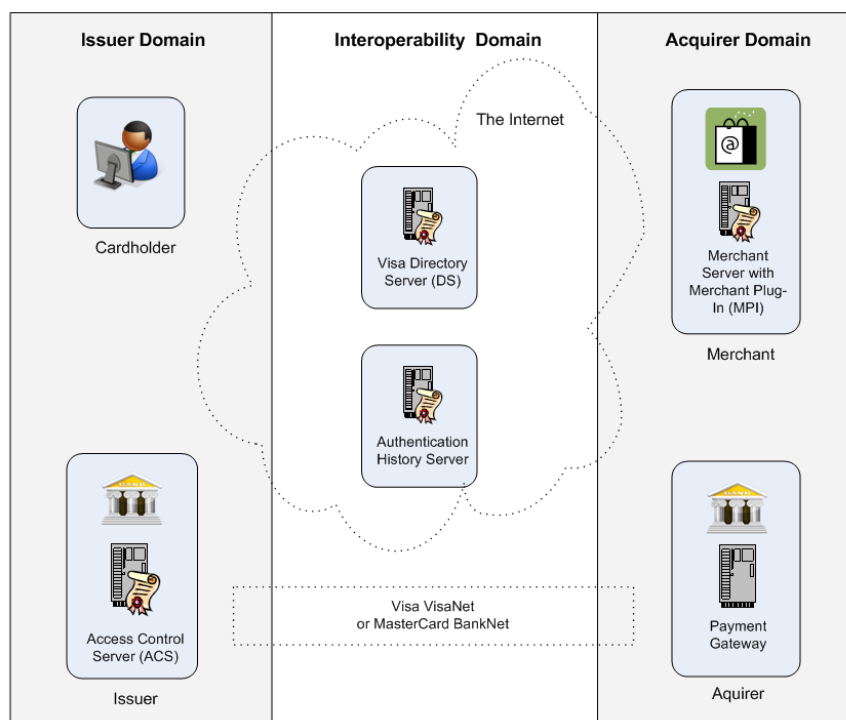


FIGURE 18 – 3-D SECURE ARCHITECTURAL OVERVIEW

There are three core requirements for the successful initiation of a 3-D Secure authentication attempt. These are:

1. The first is that the card issuer must implement an Access Control Server (ACS), including choosing an enrolment and authentication strategy. The payment card brand (Visa or MasterCard) may establish region-specific rules that require issuers to use specific authentication strategies.

2. The second is that the merchant (or services acquired by the merchant) must implement a merchant plug-in (MPI) – allowing the merchant to determine if the cardholder is enrolled in 3-D Secure, and if so, initiate the 3-D Secure cardholder authentication process.
3. The third is that the cardholder must be enrolled in 3-D Secure. Users may be asked to enrol ‘on the spot’ – in what is referred to as ‘activation during shopping’ or Activation Anytime [70] as part of the payment transaction – or they may be asked to enrol in advance at the issuer’s site. Authentication schemes include static passwords, chip and PIN (via a portable reader), and even one-time passwords (OTP) sent via SMS to the cardholder’s mobile phone.

There are two phases in the 3-D Secure authentication process. The ‘Verify Enrolment’ phase and the ‘Cardholder Authentication’ phase.

Phase 1 – Verify Enrolment

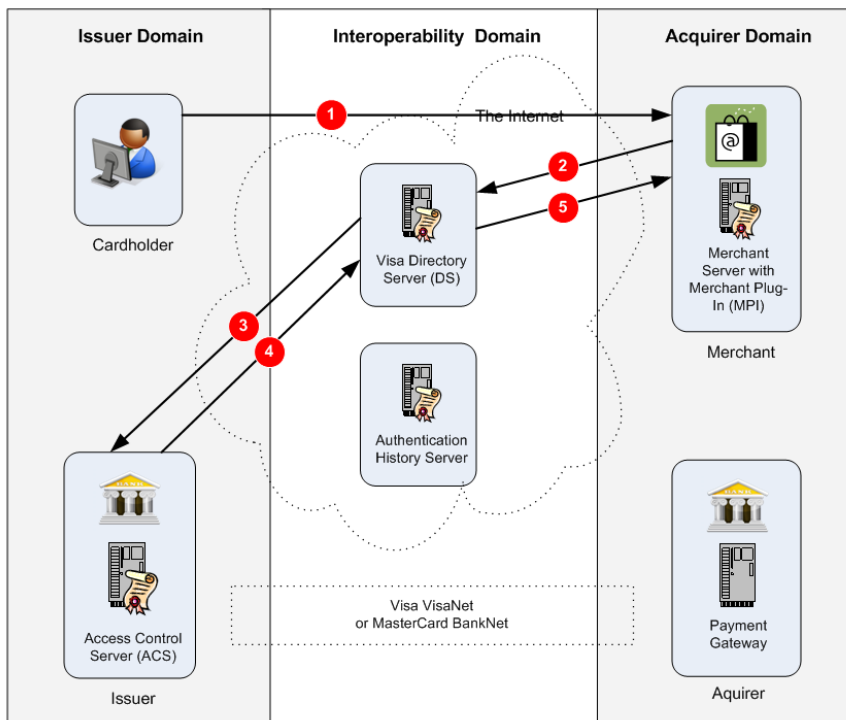


FIGURE 19 – VERIFY ENROLMENT

As illustrated in Figure 19 above, during the verify enrolment phase, the merchant will attempt to determine if the cardholder is enrolled in 3-D Secure. Steps 1-5 above are performed as follows:

1. The customer browses the merchant’s site, selecting items to purchase and then attempts to complete the purchase by beginning the ‘check-out’ or payment process. The customer selects a payment card as their payment method and enters their

payment card details.

2. Having received payment card details, a 3-D Secure-enabled merchant will attempt to verify the enrolment of the payment card in 3-D Secure. 3-D Secure-enabled merchants will implement a merchant plug-in (MPI). The MPI may be implemented directly by the merchant, or by a payment gateway or service provider. The merchant (or service provider), using the MPI, will attempt to contact the Visa Directory Server (DS) located in the Interoperability Domain via the Internet. The MPI will send a Verifying Enrolment Request (VEReq) to the DS which includes the primary account number (PAN) of the cardholder. The MPI will be required to authenticate with the DS using certificates or a merchant ID and password. The MPI will communicate securely with the DS using SSL/TLS.
3. Based on the PAN, the DS will contact that card issuer's Access Control Server (ACS) in order to determine whether the PAN is enrolled in 3-D Secure. The DS will authenticate itself to the ACS using the scheme brand root certificate and SSL/TLS.
4. The ACS will respond to the DS, indicating whether the PAN is enrolled in the scheme.
5. The DS will respond to the MPI with a Verifying Enrolment Response (VERes) message, indicating to the MPI whether the PAN is enrolled in the scheme or not. The VERes message will also include the URL of the ACS if the cardholder is enrolled.

Phase 2 – Cardholder Authentication

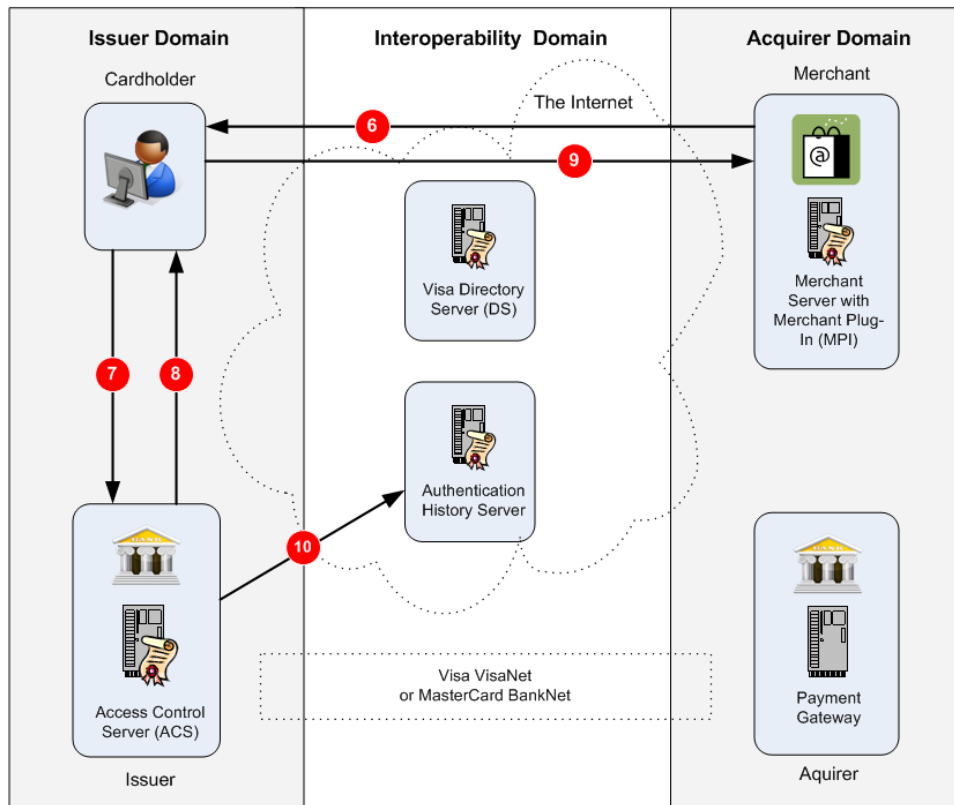


FIGURE 20 – CARDHOLDER AUTHENTICATION

As illustrated in Figure 20 above, if the cardholder's PAN is enrolled in 3-D Secure, the merchant will attempt to initiate cardholder authentication.

- Using the MPI, the merchant will create a Payer Authentication Request (PAREq). This is a signed request – including the PAN and ACS URL. The merchant will send a specially formatted web page to the customer's browser. This page will typically contain an iFrame – which is a web page within a web page that is capable of loading content from a URL that is independent of the main URL shown in the browser address bar.

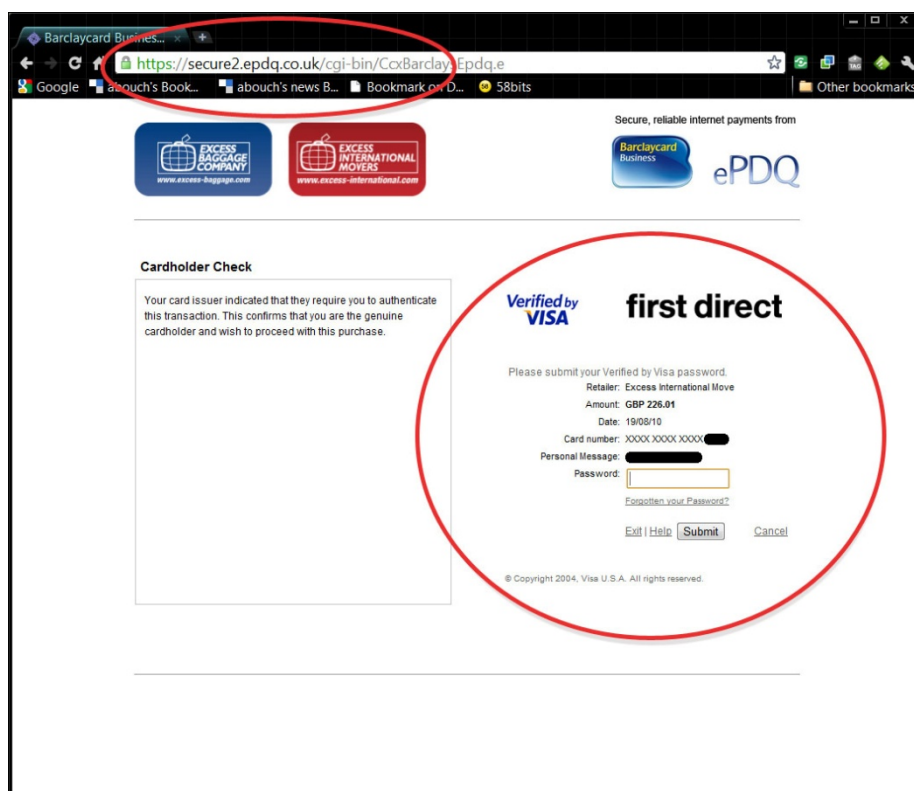


FIGURE 21 – MERCHANT WEB PAGE WITH 3-D SECURE IFRAME

Figure 21 above shows a merchant web page with an embedded iFrame, showing the 3-D Secure ACS (Verified by Visa) authentication request. In this case, the merchant (Excess International Movers) is using a payment gateway and service hosted by ePDQ from Barclaycard Business. The iFrame has been given the URL to the ACS server and is populated with the content from the ACS server of the card issuer. In this case the card issuer is First Direct – a UK Internet bank.

Early implementations of 3-D Secure used pop-up windows to show the 3-D Secure ACS authentication page, however pop-ups have now been specifically forbidden by both MasterCard and Visa [70,69].

7. The customer enters their Verified by Visa or SecureCode password and submits the form contained within the iFrame to the ACS. Both the user's credentials and the MPI PAReq are submitted to the ACS.

The personal assurance message which was chosen during enrolment is also shown on the ACS authentication page and is designed to reassure the user that the page they are looking at is in fact an authentic 3-D Secure ACS request.

8. In response to the submitted form above, the ACS prepares a Payer Authentication Response (PAREs) message which is sent back to the customer's browser.
9. The PAREs is then forwarded to the MPI via the customer's browser. The MPI verifies the signature and response of the PAREs. The transaction status of PAREs is used to determine whether the customer has successfully authenticated with 3-D Secure. A combination of the transaction status in PAREs and scheme rules will determine whether the merchant can proceed with a payment authorisation request. If the merchant proceeds with a payment authorisation request, the transaction status from PAREs will be carried forward into scheme-specific fields and included in the merchant payment authorisation request [71,69]. The transaction status results from PAREs are:
 - a. "Y" – password correct,
 - b. "N" – password incorrect
 - c. "U" – it was not possible to validate the password – for example because of a 3-D Secure system component failure.
 - d. "A" – proof that the merchant attempted to initiate an authentication attempt.
10. The ACS sends a record of the authentication attempt to the Authentication History Server.

Figure 22 shows a 3-D Secure authentication page requesting an OTP that will be sent to a user's mobile phone.

Verified by VISA

ธนาคารกรุงไทย KASIKORNBANK ธนาคารกรุงไทย

เพิ่มความปลอดภัยในการชำระเงินออนไลน์ด้วย Verified by VISA
Added Protection with Verified by Visa

โปรดตรวจสอบความถูกต้องของข้อมูลยืนยันตัวตนของท่าน จากนั้นระบุรหัสผ่าน Verified by Visa เพื่อเพิ่มความปลอดภัยในการชำระเงิน

Please verify your Personal Message and submit your Verified by Visa password.
 You need to enter your Verified by Visa password in order to complete the transaction.

Merchant: THAI AIRWAYS WEB/BAHT
Amount: 20060.00 THB
Date: 06/11/2010
Card Number: **** * * * *
Personal Message: [REDACTED]

กรุณาคlick "Request OTP" เพื่อรับรหัสรักษาความปลอดภัย SMS-OTP
 Please click "Request OTP" to receive SMS-OTP password

Ref. Code: PQPD

กรุณาระบุรหัสรักษาความปลอดภัย SMS-OTP ที่ได้รับ Request OTP

ตกลง / Submit ยกเลิก / Exit

[เปลี่ยนรหัสรักษาความปลอดภัยเป็นแบบธรรมดา](#)
 Change to static password

© Kasikornbank PCL 2010. All rights reserved.
[Terms & Conditions](#) [Privacy Policy](#)

FIGURE 22 – 3-D SECURE AUTHENTICATION USING A ONE TIME PASSWORD VIA SMS

While the objectives of 3-D Secure are clear, its impact and effectiveness in preventing CNP-based fraud might be less so.

The following is a review of 3-D Secure including advantages and disadvantages from the merchant, acquirer, issuer and cardholder perspectives.

3.2 The Merchant's Perspective

It's arguable that the entity most significantly affected by 3-D Secure is the merchant.

The overriding objective of the merchant is to successfully sell the products or services they are advertising on their website. Any process, procedure or security measure that the merchant implements must be considered within the context of this objective.

The question then is what effect does 3-D Secure have on the merchant's business?

The objective of 3-D Secure is to reduce CNP fraud. So in theory, a reduction in fraud should also mean a reduction in chargebacks to the merchant and therefore an increase in revenue (via a reduction in losses).

However, the merchant must consider several factors when deciding whether to implement 3-D Secure, including the overall cost of implementation as well as the potential for 3-D Secure to negatively impact sales. Areas that are outside the merchant's control also deserve special attention.

3.2.1 Merchant Advantages

The single greatest advantage to the merchant in implementing 3-D Secure is the policy-based reduction in chargebacks.

According to the Visa 3-D Secure Acquirer and Merchant Implementation Guide, Appendix F: Suggested Procedures for Dispute Resolution [70],

“The Visa U.S.A and Visa International Operating Regulations specify that Issuers may not charge back electronic commerce transactions under the following conditions:

The cardholder indicates that he/she did not authorize or does not recognise the purchase and the transaction involved either a 3-D Secure authentication or attempted authentication.”

This means that if the merchant has implemented 3-D Secure, and cardholder authentication was attempted via 3-D Secure, the merchant will be guaranteed the payment. The payment will not be eligible for dispute or chargeback by the cardholder via the issuer. The liability for a fraudulent transaction – where 3-D Secure authentication was either attempted, or succeeded – shifts from the merchant to the issuer.

MasterCard's liability-shift and chargeback protection policy differs from Visa's – in particular where inter-regional transactions are concerned [69]. However, for fully authenticated transactions, the same liability shift applies. The merchant will be protected from chargebacks and guaranteed the payment.

In a letter sent on April 12th, 2004 from Visa USA to all Verified by Visa merchants, Verified by Visa acquirers, and Verified by Visa merchant service providers, Visa also stated the following:

“Additionally, in August 2003, the interchange reimbursement rate for the CPS/e-commerce Preferred Retail Payment Service which includes Verified by Visa transactions became five basis points lower than the Basic or standard electronic commerce transaction rate, providing an added reason for Merchants and Acquirers to participate in the program.”

The combination of guaranteed payments and reduced interchange rates provides a powerful economic incentive for merchants to implement 3-D Secure. Chargebacks, related chargeback fines and the cost of administering and disputing chargebacks from fraud-related chargeback requests can have a substantial impact on the revenues of online merchants [72,27]. It is arguably the single greatest risk in accepting payment cards online.

Another advantage to the merchant is that the cardholder authentication details are not available to the merchant during a 3-D Secure session. These are known only to the cardholder and the issuer, and so the merchant does not have any handling or secure storage responsibilities for these credentials. This should in theory add to the overall security of the scheme since the ‘complete’ details required to initiate a payment transaction are no longer stored by a single entity or in a single place (although as we’ll see later, there is a trade-off in the separation of cardholder authentication details from the rest of the payment transaction).

3.2.2 Merchant Disadvantages

The potential disadvantages to the merchant from implementing 3-D Secure are significant and include the risk of shopping cart abandonment.

Although 3-D Secure authentication occurs ‘after’ payment card details have been received by the merchant, there is still a chance that the customer may abandon their purchase. The merchant is being asked to inject another step into the purchase transaction flow at a critical point; a step that is outside the control of the merchant – allowing the customer to be redirected to a 3-D Secure authentication page.

Reports suggest that ‘activation during shopping’ (combined with poor communication from card-issuing banks) may have surprised many users, resulting in abandoned purchases of between 6% and 60% [73,74,75,76].

North South Media is an Internet marketing company based in the UK. Figure 23, reproduced with permission from North South Media, shows the impact of 3-D Secure on one of North South Media’s clients.



FIGURE 23 – IMPACT OF 3-D SECURE ON SALES [75]:

From North South Media’s article on the effect 3-D Secure had on their client’s site [75]:

“The above image represents the timeline of when the 3-D Secure payment feature was switched on and when it was turned off. On average, day-to-day sales fell by around 60%. The traffic flow was constant during this period, and the flow charts show that the number going through the payment channels remained constant. It was when the customer was in the payment processing page they abandoned the sale.”

Other disadvantages to the merchant include:

1. The cost of implementing the MPI, including application level changes to the merchant’s website.
2. The dilution of the merchant brand through the inclusion of a prominent component in the purchase transaction, including issuer and payment card brand logos.
3. No reduction in compliance overhead. Cardholder and card details are still received, handled and processed via the conventional authorisation process and so the merchant must continue to comply with payment card and privacy-related regulations, including PCI-DSS.
4. The merchant must communicate with the DS directly, and indirectly with the ACS via the customer’s browser (which is acting as a relay) – introducing additional communication overhead and additional potential points of failure.
5. Issuer-specific enrolment, re-enrolment and authentication policies mean that the merchant site will have no way of providing any visual cues or warnings as to the experience the user is ‘about to have’ during 3-D Secure authentication and before completing the payment transaction.

3.3 The Acquirer’s Perspective

Acquirers do not directly participate in 3-D Secure. An acquirer will receive an authorisation request ‘after’ an attempted 3-D Secure authentication is complete. The acquirer will process the payment authorisation request as per the usual process via a proprietary payment card network such as VisaNet or Banknet. Payment authorisation requests that have originated

from a 3-D Secure/MPI-enabled merchant will include the 3-D Secure PAREs transaction result (converted into the appropriate authorisation request fields) [71,69]. The 3-D Secure transaction results included in the payment authorisation request will determine whether a payment is eligible for guaranteed payment and the merchant liability-shift.

If an acquirer is providing the merchant with a payment gateway or payment processing facilities then they will also implement the MPI on behalf of the merchant, passing on the cost of implementing as a service charge or an additional fee to the merchant.

Acquirers do benefit from 3-D Secure in terms of reduced interchange fees, as well as reduced administrative costs in handling disputed transactions and chargebacks where transactions have qualified as guaranteed payments – although these costs are typically passed on to the merchant.

3.4 The Issuer's Perspective

3-D Secure impacts the issuer in two distinct ways:

1. The issuer must implement the ACS. The ACS is the responsibility of the issuer. The issuer is therefore also responsible for cardholder communication, awareness and user experience as well the implementation of appropriate security controls (whether the ACS is implemented in-house or by a managed third-party service).
2. The liability for qualifying and fraudulent payment card transactions that have been authenticated via 3-D Secure shifts away from the merchant and onto the issuer. It's difficult to estimate the effect this will have on card issuers, and indirectly, on cardholders. There are concerns that if weaknesses in 3-D Secure are effectively exploited – the shift in liability, from the merchant to the issuer, will be passed on by the issuer to the cardholder [77].

3.4.1 Issuer Advantages

The most significant advantage to the issuer in the use of 3-D Secure is the protection of the 'credit card brand'. A reduction in CNP payment card fraud means that merchants will continue to accept payment cards, and cardholders will continue to use their payment cards online. Credit cards – with an annual percentage rate on unpaid balances between 16% and 20% [78,79,80] – are a valuable part of the issuer's portfolio of financial services and products.

Another significant advantage is the reduction in administrative costs for disputed transactions with the acquirer. It's unclear however if this benefit may be offset in part by administrative costs in dispute resolution with the cardholder instead.

3.4.2 Issuer Disadvantages

There are significant disadvantages to the issuer in implementing 3-D Secure which include:

1. The costs of implementing the ACS, whether through the use of managed services, or the development of in-house enrolment and ACS – including the integration with back-office systems.
2. The cost of supporting the ACS, including cardholder customer support.
3. The potential for financial losses from unmitigated security vulnerabilities in the scheme that result in issuer-liable fraudulent activity.
4. The potential for reputational damage if the scheme is not clearly communicated to cardholders.
5. The potential for reputational damage from “cardholder onerous” dispute resolution mechanisms.

3.5 The Cardholder’s Perspective

The overriding objective of the cardholder during an Internet-based CNP payment transaction is to successfully place an order for their selected products or services.

However the success of this task is dependent on several factors which include:

1. The visual interface, visual cues and metaphors that are used by the merchant’s site in order to help a user understand how to successfully place an order – including any security related cues, messages or tasks.
2. The confidence of the user in placing the order – including the submission of sensitive details like payment card information as well as name and address details.
3. Policy-based rules implemented by the merchant, acquirer or issuer that will either accept or reject a submitted order.

The security of placing an order is not the cardholder’s main objective. Cardholders would understandably like their payment details to be ‘treated securely’, however the assessment they make on the security risks associated with making a payment will be weighed against the value of their main objective – which is placing an order.

Achieving a balance between security related tasks, trust and the general usability of a system is particularly challenging for Web-based e-commerce sites, since a wide range of users and user ability must be accommodated [81].

The question then, is what effect does 3-D Secure have on the cardholder’s objective of successfully placing an order?

As described in 3.2.2, 3-D Secure authentication appears a critical point in the payment process, requiring additional steps to be taken and therefore requiring more time to complete the payment transaction. The success of this stage in the payment process will depend on several factors, including:

1. A simple cost/time calculation. A user may decide the value of their time is greater than the value in completing the additional steps required to place the order.
2. An understanding and trust of what is happening, including the perceived complexity of the task. A user may abandon the payment process if they do not understand what they are being asked to do, or if they no longer trust the payment process [82].
3. The perceived control the user has over the task – including an understanding of what will occur should they choose to proceed, or not. A user may abandon the payment process if they do not feel they have control over it [83].

At the time of writing, no formal usability study of 3-D Secure could be found, however anecdotal evidence [84,73,74,75,76,85] suggests that 3-D Secure may be negatively affecting merchants, and so it can be inferred that cardholders have also been negatively affected in their attempts to place orders.

3.5.1 Survey

An informal survey was conducted in order to determine cardholder response towards 3-D Secure. The objectives of the survey were as follows:

1. To determine the level of familiarity with 3-D Secure.
2. To determine the percentage of cardholders who were aware 'before' making a payment that they would be required to enrol and/or authenticate with 3-D Secure.
3. To determine which types of authentication methods are being used.
4. To determine cardholders' general feelings and experience with 3-D Secure.

A screen-shot of the survey, including raw survey data and user comments, can be found in Appendix B.

The survey was published online at <http://www.58bits.com/survey> and was open for submissions from January 5th until January 31st 2011. Participants were invited via Twitter, Facebook and email to visit the survey site and submit their answers. The survey results were anonymous and no attempt was made to correlate visiting IP addresses or web server logs with submissions.

The following questions were asked with radio button options for answers. Question 1) and 2) were mandatory. Questions 3) to 5) including comments in 6) were optional:

1. Are you familiar with any of the following: a) 3-D Secure, b) Verified by Visa, or c) MasterCard SecureCode? a) Yes, b) No
2. Have you used Verified by Visa or MasterCard SecureCode while purchasing goods or services online? a)Yes, b) No, c) Failed to enrol or checkout

3. Were you given any warning before your purchase that you would have to enrol, or verify your details using Verified by Visa or MasterCard SecureCode? a) Yes, b) No, c) Not sure
4. When you enrolled, and then verified your details for a purchase – which of the following methods did you use? a) Password, b) Portable reader, smart card or token (OTP), c) Passcode that was sent to your mobile phone (OTP)
5. Would you describe your experience with Verified by Visa or MasterCard SecureCode as generally OK, or generally not OK? a) OK, b) Not OK
6. Do you have any comments or thoughts you would like to add concerning 3-D Secure, Verified by Visa or MasterCard SecureCode?

The survey received 222 responses. The summary results of the survey are as follows:

Question	Response			
1. Familiar with 3-D Secure, Verified by Visa or MasterCard Secure Code?	Yes	No		
	201	21		
2. Have used when purchasing?	Used	Not Used	Failed Checkout or Enrolment	
	174	39	9	
3. Knew in advance?	Knew	Did Not Know	Not Sure	NA
	67	95	56	4
4. Method of authentication?	Password	Reader or Token	OTP SMS to Phone	NA
	167	5	16	34
5. Experience with 3-D Secure.	OK	Not OK		NA
	123	71		28

TABLE 1 – 3-D SECURE SURVEY RESULTS

The following general observations can be made from the survey results:

1. 91% of users surveyed were familiar with 3-D Secure, Verified by Visa or MasterCard SecureCode. 78% of users surveyed have used 3-D Secure while making a payment. 17.6% of users have not used 3-D Secure, while 4% reported either failing to checkout or enrol. Although the survey was informal, and the number of submissions relatively low, these figures suggest broad general awareness and deployment of 3-D

Secure.

2. Only 31% of users knew in advance that they would encounter 3-D Secure during the payment process. Of those that knew in advance, 76% were generally OK with their 3-D Secure experience. Of those that did not know in advance, or were not sure whether they had been given any indication in advance that they would encounter 3-D Secure, only 47% were generally OK with their experience. This suggests that where the 'principle of least surprise' [62] is violated, users are less likely to have a favourable experience with 3-D Secure.
3. 89% of users that responded to the method of authentication question reported using passwords to authenticate with 3-D Secure – suggesting that passwords are the most widely used method of authentication.
4. Overall, 63% of users who responded to the overall experience question, were generally 'OK' with 3-D Secure, while 37% were generally 'Not OK' with their experience.

3.5.2 Cardholder Advantages

It's difficult to describe tangible advantages to the cardholder in the use of 3-D Secure. There are no direct economic benefits, and the cardholder is being asked to perform extra steps in the payment process. Until now, scheme rules and chargebacks have protected cardholders from losses where fraudulent activity has occurred. There are indirect benefits to the cardholder in the reduction of payment card fraud, such as the time saved in disputing fraudulent transactions or reissuing compromised payment cards. There is also the potential for increased confidence while shopping online, knowing that payment card details are less likely to be used fraudulently.

In terms of practical advantages, authentication using static passwords does not require any additional software or devices.

3.5.3 Cardholder Disadvantages

The disadvantages to the cardholder include the following:

1. The cardholder is being asked to perform extra steps during payment processing. The extra time to perform these steps may deter the user from continuing, especially if a 'time sensitive' order is being placed – such as an auction item, or items of limited availability or stock.
2. The cardholder may be required to authenticate 'twice' – once with the merchant application, and once with 3-D Secure.
3. The cardholder must authenticate for every transaction.

4. The cardholder must enrol for each payment card they are going to use online.
5. In the case of authentication via a static password, the cardholder must remember or safely store their 3-D Secure password for each payment card they will use online.
6. The MPI, DS, and ACS communicate via SSL and perform mutual authentication through the use of certificates that are issued and managed by the scheme root certificate authority. It is therefore arguable that cardholder authentication is the weakest link in the security of 3-D Secure – in particular where static passwords are being used (although the MPI, DS, and ACS are not immune to security vulnerabilities – such as distributed denial-of-service attacks). The scheme is vulnerable to phishing attacks, Trojans and key loggers [77,86] as well as other forms of social-engineering attacks designed to determine the cardholder's 3-D Secure password.
7. The cardholder's only defence against a fraudulent request for 3-D Secure authentication details is their personal assurance message, since they are unable to verify the URL and certificate of the ACS from within an iFrame.
8. There are anecdotal reports that users who disable JavaScript in their browser may not be able to use 3-D Secure.
9. 3-D Secure implementations by the merchant and issuer – including procedures for forgotten passwords or cancelled 3-D Secure authentication attempts – may differ from site to site and issuer to issuer, providing the cardholder with an inconsistent user experience.
10. The lack of standard enrolment, re-enrolment and authentication policies means that a user may have a different and inconsistent 3-D Secure experience for each payment card they possess.
11. 3-D Secure authentication occurs '*after*' the user has submitted their payment card details to the merchant and is 'checking out'. At this point the user may feel 'endowed' or 'committed' to a purchase and may find the disruption of a second authentication process disturbing, in particular if they were not aware that this was what was going to happen next, and at a point when alternative paths may not be clear.

3.6 3-D Secure Scorecard

3-D Secure Score Card		
Requirement	Result	Comments
Confidentiality	Poor	3-D Secure provides no additional confidentiality assurances – the merchant will be aware of both payment card and transaction details. In this respect 3-D Secure is no different from regular SSL/TLS web-based e-commerce transactions.
Integrity	Poor	There are no message-level assurances in 3-D Secure. The scheme relies on the integrity of the regular authorisation and clearing process. PAN and transaction details are not protected by message-level security mechanisms. In this respect, 3-D Secure is no different from regular SSL/TLS web-based e-commerce transactions.

Authentication	Fair	The objective of 3-D Secure is the authentication of the cardholder (and therefore the 'authority' of payment authorisation messages). Where the scheme has been clearly communicated to cardholders, the extra level of authentication provided by 3-D Secure (in particular where readers, tokens, or SMS OTPs are used) provides additional assurances that the transaction has been initiated by the cardholder. However the use of static passwords as the predominant method for authentication and the vulnerability of the scheme to phishing attacks means that authentication assurances here are considered 'fair' and not 'good'.
Non-Repudiation	Poor	There are no message- or transaction-level assurances providing non-repudiation services. In this respect, 3-D Secure is no different from regular SSL/TLS web-based e-commerce transactions.
Availability	Unknown	Anecdotal evidence suggests that 3-D Secure and its required components are highly-available. However, there is no published data concerning the availability of directory servers (DS) or authentication servers (ACS) – both of which require a connection to the Internet, and therefore may be subject to denial-of-service attacks.
Implementation	Poor	The use of iFrames and the cardholder browser to relay an authentication attempt between the merchant and the issuer represents implementation weaknesses. Variable user experience in 3-D Secure (including early implementations that used pop-ups) may be responsible for cart abandonment.
Interoperability	Good	The 3-D Secure specification along with scheme-specific MPIs means that the merchant system (via the MPI), DS, and ACS should be interoperable.
Ease of Use	Poor	Poor communication from issuers has meant that many cardholders discovered 3-D Secure for the first time while shopping – violating the security principle of least surprise. 3-D Secure requires extra steps and time be taken during the payment process. Users may be forced to authenticate twice – with the merchant application as well as with 3-D Secure. Users will have to remember a password for each payment card they use online.
Scheme Protection	Unknown	Payment cards have previously received good scheme and legal protection when used online. The shift in liability from the merchant to the issuer, combined with the vulnerability of the scheme to phishing attacks, raises questions about scheme protection and dispute resolution mechanisms between the issuer and cardholder.

3.7 3-D Secure Further Analysis

At this point in the report, we've examined the history of payment cards, including their rise as the predominate method of payment in e-commerce via a web browser using SSL/TLS.

We've also considered the EMV standard, including the properties of smart cards that can be used to provide message-level assurances for authentication, confidentiality and non-repudiation.

We then briefly examined the failed SET standard – an early attempt at securing payment card-based e-commerce which like EMV, provided comprehensive end-to-end message-level assurances, including authentication, confidentiality and non-repudiation.

We've also described the difficulty of establishing trust in e-commerce (and over an insecure and open network such as the Internet) – in particular between two parties previously unknown to one another and with no prior trust relationship.

What's more, we've established that – like the Internet itself – payment cards are being used in a way never intended by their inventors.

If it weren't for all of the above, it would be tempting to deride Visa's 3-D Secure initiative as complex and of questionable value.

3-D Secure justifiably attempts to correct one of the major deficiencies in the use of payment cards online – the problem of cardholder authentication. And it attempts to do this without requiring any additional software to be installed by the cardholder.

That said, there are valid architectural and security-related questions that can be asked about the way in which the scheme has been implemented. It would appear that one of the scheme's greatest failings to-date has been a lack of communication from card issuers, with a significant percentage of cardholders unaware that they would be required to enrol and authenticate with 3-D Secure.

First Direct is a well known Internet bank in the UK (a division of HSBC). It provides Verified by Visa enrolment and authentication services for its customers. It also provides an information page under the payment card section of its website concerning online security, in which it describes its membership in the Verified by Visa programme [87]. Links are provided for 'further information'. Clicking on these links displays a pop-up warning message as shown in Figure 24:

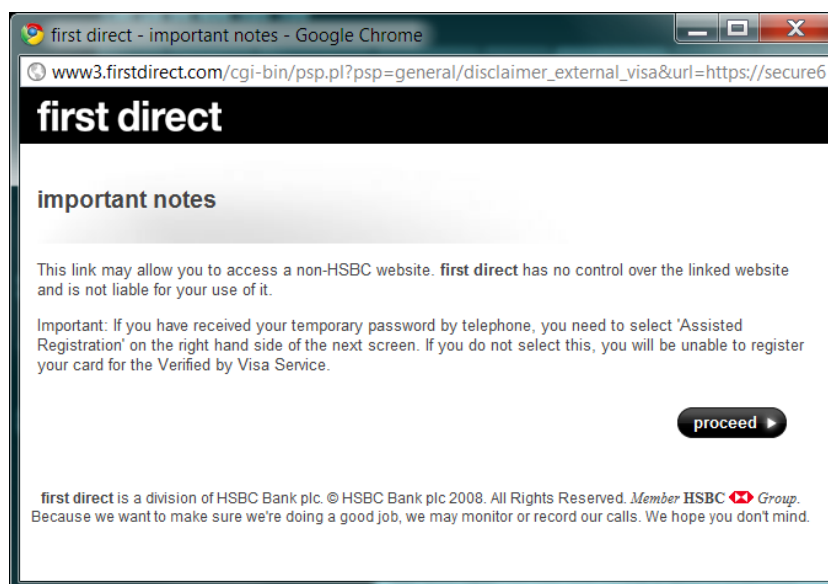


FIGURE 24 – FIRST DIRECT'S WARNING MESSAGE BEFORE VISITING ITS VERIFIED BY VISA PAGES (SOURCE [87])

The warning in the first paragraph states,

“This link may allow you to access a non-HSBC website. First Direct has no control over the linked website and is not liable for your use of it.”

Clicking ‘proceed’ repopulates the pop-up with a ‘partially viewable’ window, containing First Direct’s managed services for Verified by Visa – run by Arcot Systems Inc (shown in Figure 25).

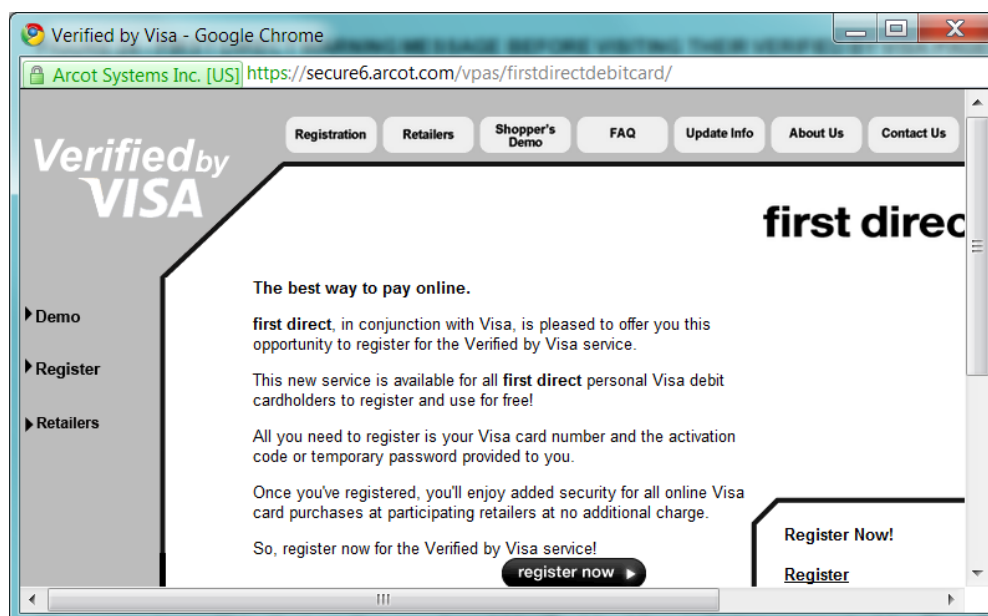


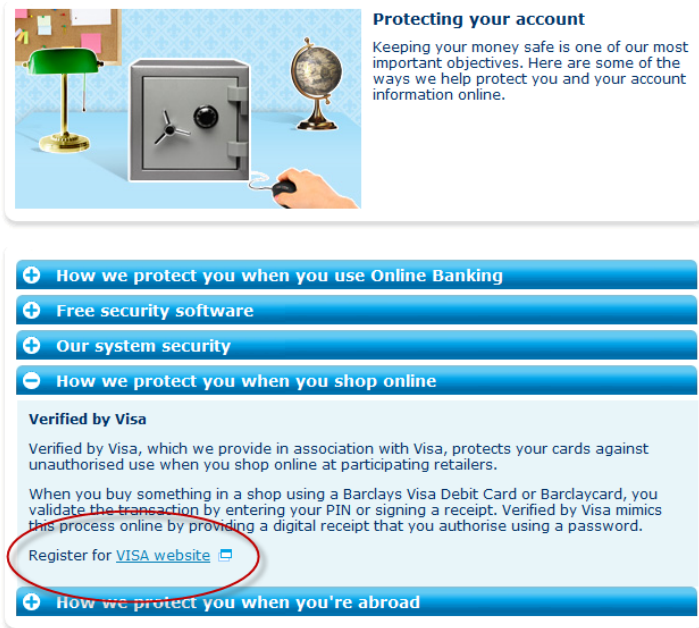
FIGURE 25 – FIRST DIRECT’S MANAGED VERIFIED BY VISA SERVICES WINDOW

It’s remarkable that on the one hand Verified by Visa is being promoted by First Direct as an online card security measure, while on the other (and before visiting a page that will allow us to register and/or change our Verified by Visa details) we are being given the warning that “First Direct has no control over the linked website and is not liable for your use of it”.

These are extremely confusing messages. Not least of which is due to the fact that the ‘Arcot Systems’ certificate and URL – on a page containing text that appears to belong to First Direct – looks remarkably like the type of site users are warned against as a potential phishing attack.

Barclays Bank PLC is major high-street bank in the UK. Barclays’ website contains a helpful and educational section on banking security and how users can protect themselves from threats online. Verified by Visa is also mentioned under a subsection, shown in Figure 26, that contains two paragraphs and a sentence that directs the visitor to an external link with the text “Register for VISA website”.

What we're doing to protect you



Protecting your account
 Keeping your money safe is one of our most important objectives. Here are some of the ways we help protect you and your account information online.

- How we protect you when you use Online Banking
- Free security software
- Our system security
- How we protect you when you shop online**

Verified by Visa
 Verified by Visa, which we provide in association with Visa, protects your cards against unauthorised use when you shop online at participating retailers.

When you buy something in a shop using a Barclays Visa Debit Card or Barclaycard, you validate the transaction by entering your PIN or signing a receipt. Verified by Visa mimics this process online by providing a digital receipt that you authorise using a password.

[Register for VISA website](#)

- How we protect you when you're abroad

FIGURE 26 - BARCLAYS BANK INFORMATION ON VERIFIED BY VISA (SOURCE HTTP://WWW.BARCLAYS.CO.UK)

Clicking on the nonsensical link to “Register for VISA website” results in a pop-up window as shown in Figure 27:

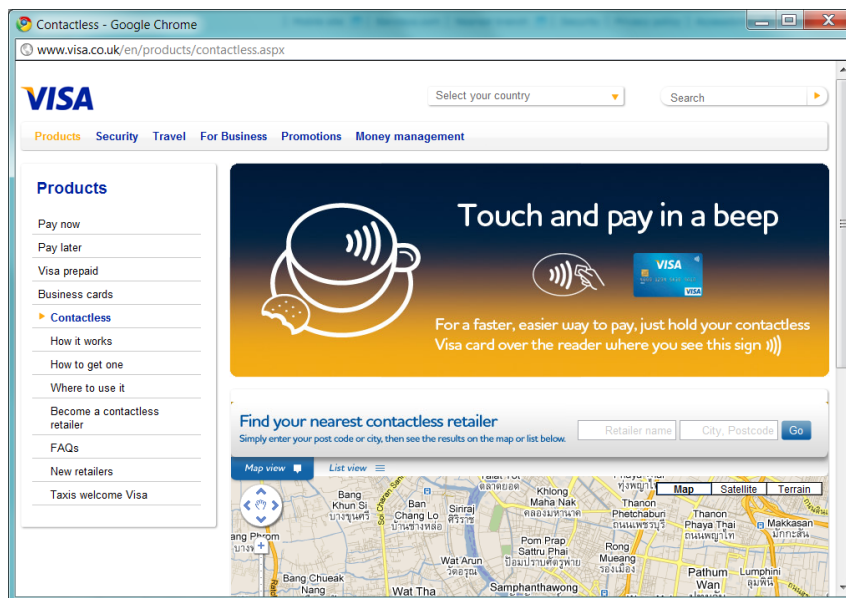


FIGURE 27 - THE POP-UP WINDOW SHOWN AFTER FOLLOWING BARCLAYS VERIFIED BY VISA LINK (SOURCE HTTP://WWW.BARCLAYS.CO.UK)

It's unclear what “Touch and pay in a beep” has to do with Verified by Visa.

Poor ownership and communication with little or no attempt at creating cardholder awareness by card issuers has almost certainly contributed to the reputational damage of 3-D Secure.

Poor communication from issuers to cardholders might also have been partly responsible for reports of shopping cart abandonment.

The use of passwords as the predominant authentication method has also raised questions about the effectiveness and security practises of the scheme. Passwords are vulnerable to collection from key logging, phishing attacks and other socially engineered attacks. There is also very little guidance and support provided to cardholders on the choice and safe storage of passwords. Issuers may have chosen passwords as an authentication method for cost savings and convenience since there are equipment-, logistical- and support-related costs associated with the use of readers and tokens (which have their own usability and convenience related advantages and disadvantages [88]). Anecdotal reports suggest that in certain regions, such as the Nordics, authentication with static passwords will eventually be phased out.

The use of onetime passwords (OTPs) sent to a user's mobile phone appears to strike a good balance between usability, convenience and security. However the short messaging service (SMS) was not designed as a reliable messaging protocol and there is no guarantee that messages will arrive in a timely manner [89]. Figure 22 shows an optional fall-back to static passwords should the SMS OTP fail to arrive in time. There are also mobile-network-operator costs associated with SMS messages.

It also seems unfortunate that – while the merchant continues to assume responsibility for the safe handling of payment transaction details, including PAN and CVV2 values (under strict scheme and regulatory supervision) – they could not also have assumed responsibility for handling and forwarding the 3-D Secure password.

Had this been possible, the complexity of the scheme would have been significantly reduced. The merchant or payment gateway services would have been able to communicate directly with the ACS via the MPI. The merchant would then have complete control over the user's experience – including any warnings, visual cues, and alternative paths provided to the cardholder.

As mentioned in the 3.2.1, the separation of 3-D Secure credentials from the rest of the payment details may be considered an advantage to the merchant – with less risk associated in handling all of the details required to initiate a transaction. However, this separation comes with the tradeoffs in complexity and usability noted above, and points to a fundamental difference between 3-D Secure and the two schemes we've looked at previously.

The use of iFrames (as opposed to a full URL redirection to the ACS) also raises questions about usability and security practises. The 'hiding' of the source URL of the contents of the iFrame means that the cardholder has no way of verifying the origin of the iFrame contents. The cardholder must rely on their personal assurance message in order to verify that they are about to enter their credentials into a valid ACS authentication form. If the user's payment

card details have been compromised, then it is trivially easy to collect their personal assurance message by masquerading as the cardholder at a valid MPI-enabled site.

According to our requirements scorecard the security of 3-D Secure is about the same as regular web-based SSL/TLS transactions, with the added feature of cardholder authentication. It offers no greater security because it does not provide message-level assurances.

Message-level assurances are an important component in end-to-end secure communication since they can provide entity authentication, data origin authentication, confidentiality, and non-repudiation services. However these services rely on shared or agreed keys as well as cryptographic processing capabilities at both ends of a communication channel. The EMV standard achieves this through the use of issuer-distributed smart cards. The SET standard attempted to achieve this through the use of customer-installed SET wallets and customer-issued certificates.

The lack of message-level assurances in 3-D Secure means that it is vulnerable to man-in-the-middle attacks, even if an OTP device is being used (although this would require an 'active attack' against a single payment transaction). What's more, the lack of message-level assurance means that some of the more interesting features of SET – such as confidentiality via dual signatures – cannot be implemented via 3-D Secure. It is for this reason too that allowing the merchant to collect the 3-D Secure authentication credentials might be perceived as risky. The merchant would again have access to all of the details required to complete the transaction – increasing the attractiveness of the merchant as a target for attack.

As previously stated, the security of any system represents a balance between security and usability. 3-D Secure has attempted to achieve that balance by adding a single and critically missing component to Internet-based CNP transactions – cardholder authentication. It has not attempted to provide a complete end-to-end message-level solution. It could be argued then that the infrastructure and components required to support 3-D Secure appear larger and more complex than one would think would be necessary to support the extra assurances provided.

The following chart shows the levels of Internet-based CNP fraud in the UK from 2000 to 2009 [25]:

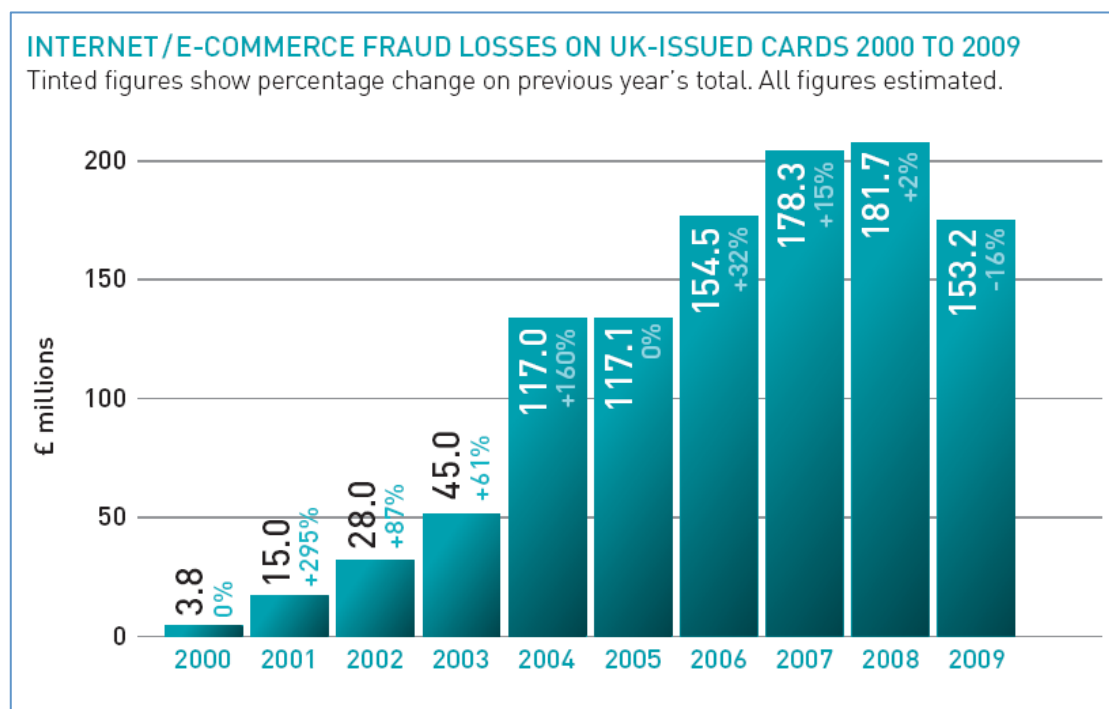


FIGURE 28 – INTERNET / E-COMMERCE FRAUD LOSSES IN THE UK [27]

The dramatic increase in Internet-based payment card fraud from 2000-2008 is an indication of the size of the problem. Also noteworthy is the decrease in fraud for 2009. Financial Fraud Action UK in [27] has the following to say:

“The reasons behind the decrease include the increasing use of sophisticated fraud screening detection tools by retailers and banks, as well as the continuing growth in the use of cardholder authentication processes such as MasterCard SecureCode and Verified by Visa”

What the authors of [27] do not include in their analysis is the overall reception of 3-D Secure, including its cost as well as its impact on merchants and the cardholder shopping experience. Nor do the figures appear to be weighed against seasonal or economic factors – including the financial crisis of 2008/09.

3.8 3-D Secure Summary

In summary, powerful economic levers are being used to force merchants to implement a scheme that implies a much greater level of security than is really provided. Poor communication and ownership from issuers combined with an overreliance on ‘activation during shopping’ may have also contributed to merchant losses and scheme reputational damage. Preliminary data suggests that the scheme may be reducing levels of Internet-based

fraud. Future analysis, combined with reported levels of fraudulent 3-D Secure activity (including cardholder dispute resolution mechanisms) will determine whether the scheme can be considered a success or not.

4. Alternatives

In this section we examine two alternatives to traditional payment card-based e-commerce.

The alternatives described below were chosen for both their relevance in e-commerce today, as well as for representative examples of payment models that differ from traditional payment card-based solutions. The first – PayPal, was chosen as an example of a three-party model designed to illustrate the advantages and disadvantages of such schemes. The second – iDEAL, was chosen as an interesting example of a four-party indirect push account-based scheme started by the banking community in the Netherlands. Both schemes also benefit from development as ‘e-commerce-only’ solutions, without the need to integrate or support a prior ‘real world’ payment system.

4.1 PayPal

4.1.1 Introduction

PayPal was created in 1999 by Max Levchin and Peter Thiel under a company named Confinity. PayPal, along with a system previously design by Levchin and Thiel called Field Link – was targeted at transferring money between wireless devices such as mobile phones and PDAs. Neither Field Link nor the first incarnation of PayPal were successful commercially. After two false starts, Levchin and Thiel recognised the potential for an e-commerce-based payment system, and PayPal was re-designed and re-launched specifically for the World Wide Web [90,91].

PayPal acts as an intermediary payment transfer service between two parties. In the case of the merchant, PayPal removes the need to implement traditional card payment gateway or payment processing services. PayPal also removes the need for the merchant to employ the services of an acquiring bank since ‘settlement’ is performed by the PayPal transfer. PayPal can be integrated into the regular check-out process of the merchant’s website.

PayPal can also be used to make personal transfers of money between PayPal members using the PayPal system alone.

The service that PayPal provides is a three-party system using an indirect push payment model to transfer payments from a buyer to a seller. ‘Real’ funds enter the system by linking PayPal accounts with credit or debit cards as well as regular bank accounts. PayPal accounts can also hold a credit balance which can be used to make payments. The ‘bank-like’ features of PayPal caused initial concern amongst regulatory authorities resulting in some states in the USA temporarily banning PayPal [91] before regulatory concerns were addressed.

eBay was the major contributor to PayPal’s success as it became the favoured method of settling payment for auctions – outperforming eBay’s own in-house payment system, Billpoint [91].

PayPal became a public company after an initial public offering (IPO) in 2002. In the same year the company was purchased by eBay for \$1.4 billion in stocks [90].

PayPal makes its money from transaction fees. For purchases from registered merchants – PayPal charges between 1.4% and 3.4% of the total transaction value plus a flat fee of £0.20 GBP [92]. Personal transfers between members are free when the accounts are linked directly to a bank account. Personal transfers via PayPal using debit or credit cards incur a transaction fee of 3.4% plus a flat fee of £0.20 GBP [92].

The steps required in a PayPal e-commerce transaction as illustrated in Figure 29 are as follows [93]:

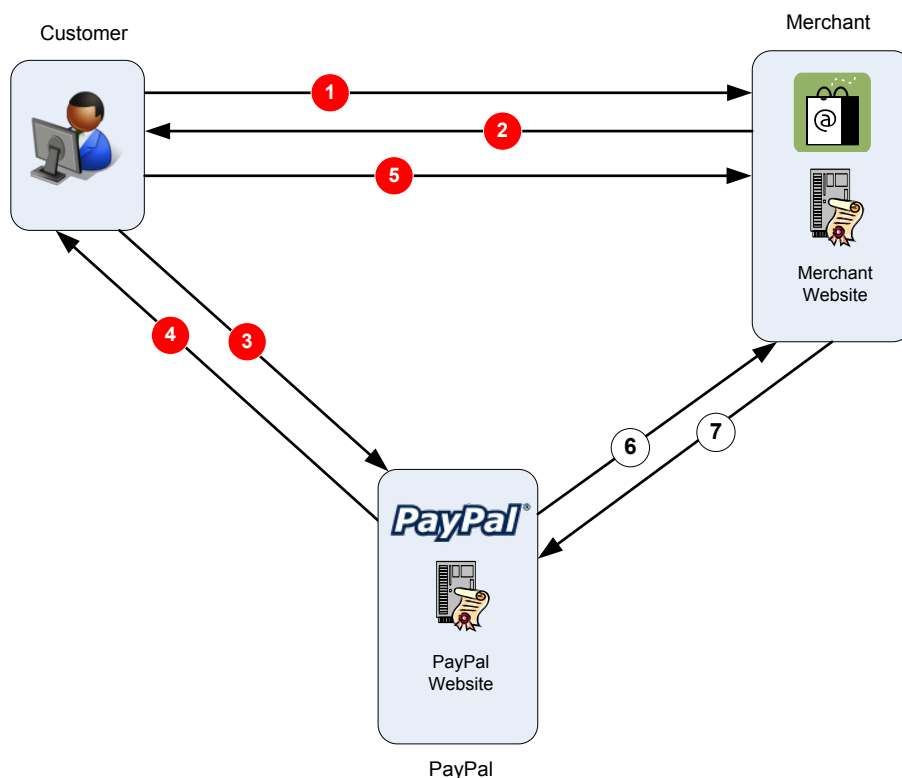


FIGURE 29 – PAYPAL TRANSACTION FLOW

1. The customer browses the merchant's site, selecting products or services to purchase. The customer selects PayPal as their method of payment.
2. The merchant's website responds with a specially crafted redirection URL that contains the purchase amount, merchant's details, as well as success and failure return URLs.
3. The customer is redirected to the PayPal website where the transaction amount and merchant's details are displayed. The connection to PayPal is secured via SSL/TLS. The customer will rely on the high-assurance PayPal certificate and URL address to ensure that they have in fact been redirected to PayPal and not a malicious site. The

customer authenticates with PayPal – either using their username and password, or using PayPal's Security Key two-factor authentication system [92]. After authentication with PayPal, the customer then authorizes the payment to the merchant.

4. Having completed the payment transaction, the customer is shown a payment summary page containing the merchant's return URL (as received by PayPal in 2. above).
5. The customer returns to the merchant's website for optional order completion information.
6. The merchant can optionally receive an instant payment notification (IPN) [93]. The merchant registers an IPN URL with their PayPal account and after any successful payment into their PayPal account, an HTTP POST message is sent to this URL. The merchant responds by simply echoing back the contents of the POST'd message. IPN's are useful when the customer and merchant need immediate notification of the success or failure of payment – as in the case of an instant download or other digital purchases. Without an IPN the merchant can either wait for an email notification from PayPal, or check their PayPal account, reconciling the order with payment information. The merchant would then fulfill the order. The customer typically receives confirmation emails – both from PayPal and the merchant.
7. If IPN is implemented – the merchant echoes back the IPN message.

4.1.2 PayPal Advantages

There are several advantages in the use of PayPal for both the merchant and the customer. These include:

1. The merchant does not require any additional payment processing, payment gateway, or acquirer services.
2. Since the merchant is not handling any payment information – there are no sensitive data handling or compliance-related requirements and costs. This also reduces the 'attractiveness' of the merchant system as a target for attack since customer payment details are not available to the merchant.
3. Although the merchant must still allow the customer to be fully redirected to an external site, that site is always PayPal. The merchant is therefore able to provide helpful information to the customer, advising them on the next steps as well as providing alternative paths.
4. The customer is being fully redirected to PayPal – a payment system they control with clear alternative paths.
5. Visiting a familiar URL and payment processor like PayPal also improves the customer's chances of correctly following security advice in identifying the PayPal URL and SSL certificate, helping to protect the customer against phishing attacks.

6. Customers may also use PayPal's Secure Key two-factor authentication scheme – improving the strength of their authentication with PayPal, and therefore further reducing the risk that their account will be compromised.
7. The separation of payment and order details also offers the customer a degree of confidentiality, with neither the merchant or PayPal in possession of the combined order and payment details.

4.1.3 PayPal Disadvantages

There are also disadvantages to the merchant and customer. These include:

1. PayPal is only available to buyers and sellers in certain countries.
2. Merchants must still modify their applications in order to integrate with PayPal – including IPN support if required.
3. The use of PayPal concentrates risk into a single and attractive entity for attack. There have been numerous reported incidents of phishing attacks [94,95,96,97], at least one successful cross-site-scripting attack (XSS) [98] as well as the recent distributed denial of service attack (DDoS) by the 'Anonymous' group [99]. PayPal also appears at the top of the 'most phished brands' in multiple reports [100,101].
4. Buyers may not be eligible for the same degree of protection from purchases made using PayPal as they would paying the merchant directly with a payment card. For example, in order to qualify for chargeback protection when using a payment card, a buyer may need to take extra steps – ensuring that the amount loaded into their PayPal account and subsequently debited for the payment are the same [102].

4.1.4 PayPal Scorecard

PayPal Score Card		
Requirement	Result	Comments
Confidentiality	Fair	The separation of payment and order information means that neither PayPal nor the merchant have the complete order details.
Integrity	Fair	The integrity of the payment instructions rests within PayPal's system since no payment details are transmitted to the merchant.
Authentication	Fair	Authentication of the buyer is handled by PayPal and while passwords are vulnerable to phishing and other social engineering attacks – dealing with a single authenticating entity helps to reduce the risk of account compromise. The use of PayPal Secure Key also increases the strength of authentication. Merchant authentication is dependent on URL recognition, SLL certificates and other 'branding' or trust-related cues on the merchant site as with regular SSL/TLS transactions.
Non-Repudiation	Fair	The PayPal transaction record can be used as evidence for the sending and receipt of payment. However the buyer must still rely on other consumer protection measures for non-delivery, or the delivery of faulty goods and services, in order to settle disputes.
Availability	Good	For countries where PayPal is available – anecdotal evidence suggests that PayPal and its required components show good levels of availability.

Implementation	Fair	The merchant application must still be modified in order to support PayPal integration. However the integration is performed by standard HTTP-based URL redirection, requiring no additional software or plug-ins. The customer requires no additional software.
Interoperability	Good	PayPal is not required to integrate with any other system or API. URL redirection and IPN are performed using the HTTP and URL standards.
Ease of Use	Fair	Ease of use will depend on both the user's experience at the merchant's site as well as the user's experience with PayPal. Redirecting to PayPal should provide a consistent and familiar payment experience with good user control, including clear alternative paths. However the user will still be expected to successfully navigate and complete tasks on two separate systems, as opposed to a single integrated solution. Ease of use is considered 'fair' as a result.
Scheme Protection	Fair	Scheme protection including merchant chargebacks may be available to buyers when using PayPal – however care must be taken to ensure that scheme rules are followed in order to qualify for protection.

4.1.5 PayPal Further Analysis

PayPal offers significant advantages over traditional payment cards for use in e-commerce. The separation of payment and order details reduces the burden of payment infrastructure, security and compliance-related activities for the merchant. The customer is presented with a consistent and familiar payment experience. Customers that are both Internet and PayPal savvy may also feel that their payment details are more secure with PayPal acting as a single trusted entity from which to authorize payment.

However the three-party model employed by PayPal may suffer from scalability issues. The concentration of a payment system into a single entity not only increases the attractiveness of PayPal as a target for attack, but also introduces other logistical and service-related challenges [103].

PayPal has achieved relatively low levels of fraud [104] through an active seller and buyer fraud-management system. However, early reports suggest that PayPal's efforts may have lead to the implementation of overzealous fraud measures, resulting in honest accounts being frozen. Once frozen, the measures required to 'reactivate' an account are significant [104,105] including the submission of identifying documents such as a passport, driver's license and bank statements. During the 'reactivation' process a seller or buyer may be denied access to their PayPal credit balance. It's been this author's own experience – after using PayPal to make a payment while abroad, that all of the documents described above were required in order to re-activate an account with PayPal.

Three-party model scalability issues, availability in other countries, as well as competition from traditional and alternative payment schemes might explain why – despite seemingly good financial results – PayPal represents a small percentage of the overall activity in the payment industry [106].

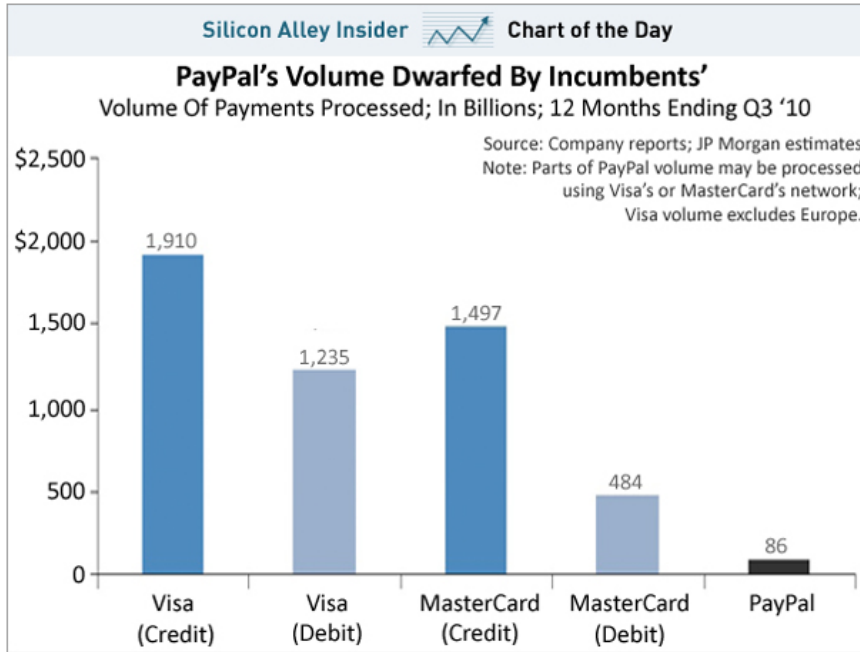


FIGURE 30 – PAYPAL'S PAYMENT PROCESSING FIGURES [106]

4.1.6 PayPal Summary

In summary, PayPal scores fairly well as an e-commerce payment mechanism. However, PayPal's adoption is likely to be limited by three-party model scalability issues, as well as competition from traditional and alternative payment schemes.

4.2 iDEAL

4.2.1 Introduction

iDEAL is an e-commerce payment system developed by the Dutch banking community [107]. It has 'PayPal-like' features, but has been implemented as a four-party indirect push payment model. iDEAL leverages Internet banking facilities to provide customers and merchants with a scheme that allows them to transfer funds directly between banks. Traditional payment cards are not required in iDEAL.

iDEAL is owned and operated by Currence, a not-for-profit payment product company in the Netherlands whose purpose is to oversee national payment schemes [108]. Currence was founded in 2005 by eight banks from within the Dutch banking community. iDEAL is funded via joining fees as well as annual product fees from member banks [108]. Merchants are not required to pay any scheme related fees, although customer and merchant banks will agree interchange fees for the transfer of funds between banks that will form part of the cost of each transaction.

A description of the iDEAL architecture and transaction sequence was obtained from the iDEAL website at www.ideal.nl, as well as from a telephone interview with an iDEAL product manager at Currence on the 15th of February 2011.

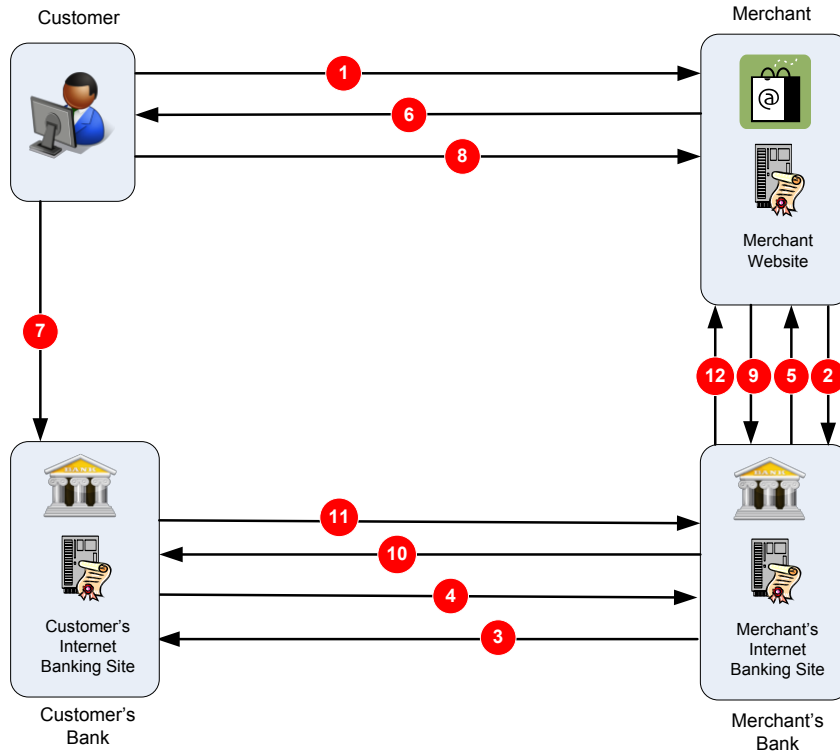


FIGURE 31 – IDEAL TRANSACTION FLOW

The iDEAL transaction flow, as illustrated in Figure 31, proceeds as follows:

1. The customer browses the merchant's website, selecting products and services for purchase. At checkout, the customer selects iDEAL as their payment method. The merchant displays a list of customer banks accessible through the merchant's bank. The most recent customer bank list is retrieved periodically by the merchant using a 'directory protocol'. The customer selects the bank with which they have an Internet banking relationship.
2. The merchant sends a transaction request – including order ID, amount, and merchant return URL – to the merchant bank to initiate the payment transaction.
3. The merchant's bank forwards the transaction request to the customer's bank.
4. The customer's bank sends a message back to the merchant's bank containing a URL to which the customer must be redirected. Included in the URL is a transaction identifier that allows the customer to 'join' the merchant-initiated transaction at the customer's bank.
5. The merchant's bank returns the URL to the merchant.

6. The merchant redirects the customer to the supplied URL received from the customer's bank via the merchant bank.
7. The customer authenticates with their Internet banking facility and authorizes the transaction.
8. The customer returns to the merchant's site via a merchant return URL and views order completion information at the merchant site.
9. The merchant issues a payment status request – sent to the merchant's bank
10. The merchant's bank forwards the payment status request to the customer's bank.
11. The customer's bank returns the payment status to the merchant's bank.
12. The merchant's bank returns the payment status to the merchant. Payment status is received within seconds and is usually fast enough to show the result of the payment to the customer when they return to the merchant's website. If approved, a payment status message signed by the merchant's banks acts as the payment 'guarantee' – allowing the merchant to proceed with order processing. Actual payment and receipt of funds by the merchant's bank may take up to 2-3 working days.

4.2.2 iDEAL Advantages

There are several advantages to both the customer and the merchant in the iDEAL system.

1. Like 3-D Secure, payments made using iDEAL are guaranteed and cannot be reversed. The merchant will therefore be protected from fraud-related chargebacks.
2. Like PayPal – the customer benefits from a consistent and familiar experience in the authorisation of payment through the use of their existing Internet banking facilities.
3. All of the iDEAL member banks implement either token based, SMS OTP or Transaction Authentication Number (TAN) lists for authentication between the customer and their Internet banking facilities. The use of a familiar and secure Internet banking site combined with two-factor authentication reduces the risk to the customer from account compromise via malware or phishing attacks.
4. In order for banks to participate in iDEAL, they must agree to the iDEAL terms and conditions which include minimum levels of system availability. These are described as standard prime time (7 am to 1 am) with a guaranteed availability of 99,0% and standard non-prime time (1 am to 7 am) with a guaranteed availability of 93,5% [107].
5. iDEAL is a four-party distributed model that allows both the customer and merchant to choose their own banks with whom to form their own trust relationships. This helps to spread the risk of attack amongst a network of banks as opposed to concentrating that risk into a single entity – as in the case with PayPal.
6. The merchant is required to communicate only with the customer and their merchant bank – reducing the dependency on other communication points.

7. Since the payment process is handled by the customer's bank, the merchant will not have any compliance or sensitive data-handling responsibilities for payment information.
8. The customer does not require a payment card.

4.2.3 iDEAL Disadvantages

1. The merchant must integrate their application with iDEAL.
2. The merchant must still perform a full browser redirect – giving up control of the customer while sending them to their Internet banking facilities.
3. The merchant (via the merchant bank) must communicate twice with the customer's bank, in order to both initiate as well as request status of the payment transaction.
4. The customer must have Internet banking facilities.
5. The lack of message-level assurances means that it is still theoretically possible for the customer to be subject to a phishing or man-in-the-middle attack – even with the use of two-factor authentication although this would require an active attack against the customer.
6. iDEAL is only available within the Dutch banking community. International customers and merchants will have to use alternative payment systems.

4.2.4 iDEAL Scorecard

iDEAL Score Card		
Requirement	Result	Comments
Confidentiality	Fair	The separation of payment and order information means that neither the bank nor the merchant have the complete order and payment details.
Integrity	Fair	The integrity of the payment instructions rest within the Internet banking system, since no payment details are transmitted to the merchant.
Authentication	Fair	As with PayPal, authentication of the customer is handled by a single authenticating entity – helping to reduce the risk of account compromise. Two-factor authentication by the customer provides additional authentication assurances. Merchant authentication is dependent on URL recognition, SLL certificates and other 'branding' or trust-related cues on the merchant site as with regular SSL/TLS transactions.
Non-Repudiation	Fair	The Internet banking transaction record can be used as evidence for the sending and receipt of payment. However the lack of chargeback mechanisms means that the customer must rely on other consumer protection measures for non-delivery, or the delivery of faulty goods and services in order to settle disputes.
Availability	Good	Guaranteed minimum service levels by member banks ensure that the system has good availability.
Implementation	Fair	As with PayPal, the merchant application must still be modified in order to support iDEAL integration. However the integration is performed via standard HTTP-based URL redirection requiring no additional software or plug-ins. The customer requires no additional

		software.
Interoperability	Good	Scheme rules and implementation standards ensure good interoperability between merchants and banks.
Ease of Use	Fair	Ease of use will depend on the customer's experience at the merchant site and the customer's Internet banking facilities. The customer will need to have Internet banking facilities. However these facilities should provide a consistent and familiar payment experience with good user control, including clear alternative paths
Scheme Protection	Fair	The merchant is protected from fraud through guaranteed payments. The user's protection will depend on Internet banking fraud and dispute resolution mechanisms, as well as consumer protection legislation.

4.2.5 IDEAL Further Analysis

The iDEAL scheme is similar to 3-D Secure in that it requires the customer to interact directly with their own financial institution during a payment transaction. In the case of 3-D Secure this is the card issuer (although the user may not be aware that they are communicating directly with their issuer because of the use of iFrames). iDEAL differs from 3-D Secure in that the customer is fully redirected to their Internet banking facilities, and their interaction with the bank includes both customer authentication **and** payment authorisation. Complete redirection should make it clear to the customer that they are visiting their Internet banking site and they can follow general security advice in verifying the site URL and certificates.

iDEAL has seen significant growth within its market. The figure below shows the growth of iDEAL from its launch in October 2005 to more than 7 million transactions in the month of October 2010.

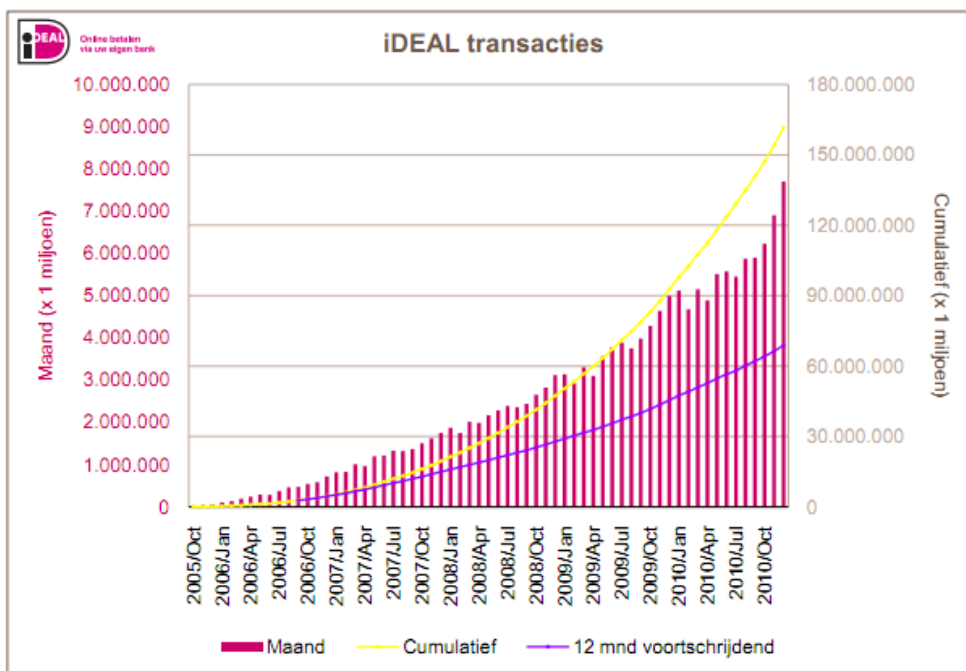


FIGURE 32 – IDEAL TRANSACTION GROWTH (Source: Currence [108])

Currence also reports that the total transaction value of sales made with iDEAL in 2010 amounted to more than €5.2 billion.

According to the Currence website [108]:

“No other European country has such a successful online banking based payment system. iDEAL has provided a major impulse to the e-commerce market in the Netherlands. Once a system like iDEAL is adopted by banks in other countries it could also help to increase the growth of e-commerce, which is in line with the aims of the European Commission.”

iDEAL's success in the Netherlands may be attributed to several factors. The first is that in the Netherlands credit cards are not as widely used as in other countries [109,110] and so there is less competition from an incumbent payment card-based solution. The second is that Internet banking facilities in the Netherlands are mature, with most using two-factor authentication schemes. Thirdly, within a relatively small geographic area the establishment of consumer protection organisations like the Home Shopping Organization [111] increases the likelihood of the customer being able to determine the 'trustworthiness' of the merchant. The trustworthiness of the merchant is particularly important in iDEAL since payments made using iDEAL are authorised 'before' delivery and do not receive the same degree of protection as traditional payment card-based schemes. For example, the customer cannot initiate a 'chargeback' for non-delivery. Merchants and customers participating in iDEAL must also have a bank account in the Netherlands. Account vetting and opening procedures for merchants may help to attribute trustworthiness to the merchant.

4.2.6 iDEAL Summary

In summary, guaranteed payments combined with reduced compliance overhead provide a strong incentive for merchants to offer iDEAL as a payment option. The customer's bank is motivated to provide a good user experience and a secure service since Internet banking forms part of the bank's regular portfolio of customer services. The customer and merchant are also free to choose between competing Internet banking and merchant services with which they can form their own trust relationships.

5. The Future

5.1 Activity in E-commerce

5.1.1 Trends

The convergence of technology in smart cards, near field computing (NFC), mobile computing, and the Internet is creating remarkable opportunities for new and innovative payment schemes.

In 2010, the retail payment sector saw announcements from both major and minor players in the payment industry, including [112,113,114,115,116,117,118,119] to name a few.

Development activity in e-commerce also continues to offer alternatives to traditional payment card-based schemes including services from Amazon Payments [120], Google Checkout [121] and even 'social network'-based schemes like Facebook Credits [122] and Twitpay [123].

The Apple iPhone phenomena – with its integrated iTunes and App Store [124,125] – is a noteworthy example of a system that has succeeded in creating a nearly 'frictionless' shopping and payment experience. However Apple has achieved this at the expense of consumer and merchant choice – creating a completely closed and proprietary environment.

While the schemes noted above fall into several different categories and models, they are an indication of the dynamic and evolving nature of payments systems in general. They are also an indication of the opportunities that exist for merchants and consumers to migrate from traditional payment card-based schemes.

5.1.2 Regulatory Environment

Changes in the regulatory environment – in particular in Europe – are also likely to have an impact on the development of alternatives to payment card-based e-commerce solutions. The European Payments Council (EPC) and the Single Euro Payments Area (SEPA) initiative [126] aims to standardize and simplify payment systems in Europe. SEPA allows national and all cross-border payments within Europe – to effectively be treated as domestic payments. SEPA has defined both a SEPA Credit Transfer Scheme (SCT) and the SEPA Direct Debit Scheme (SDD) [127], and there is even a proposal for a pan-European SEPA based general purpose payment card [128].

The Directive on Payment Services (PSD) will also facilitate payment systems across Europe and between member nations as well as provide opportunities for other non-bank-based payment organizations to enter the payment market [129].

The International Council of Payment Network Operators (ICPNO) [130] was formed specifically to facilitate growth in Internet banking-based schemes (such as iDEAL), and

seeks to create a framework that will allow global interoperability between national Internet banking networks and merchants [131].

SEPA, PSD and ICPNO represent interesting opportunities for the development of new and alternative e-commerce systems.

5.1.3 Security

From a security perspective, 3-D Secure represents the payment card industry's largest 'implemented' effort to-date to tackle the problem of CNP fraud in e-commerce.

UK and European banking communities are also investing in two-factor authentication schemes based on EMV infrastructure, allowing a cardholder to use an EMV card to authenticate with Internet banking facilities as well as 3-D Secure. The scheme is referred to as The Chip Authentication Program (CAP) and major retail banks in the UK have issued un-connected CAP card readers that allow EMV chip cards to be read and used to authenticate cardholders online [132,133]. The cardholder inserts their card into a reader and enters their PIN. In response to a correct PIN entry, the chip on the card generates a time-sensitive OTP that can be used to authenticate the user. The correct entry of a PIN (something known) and the generation of the passcode by the card (something in the cardholder's possession) provide the two factors of authentication. However, as previously noted, one-time passwords are still vulnerable to an active man-in-the-middle attack. What's more, the author's of [134] have identified several weaknesses in the implementation of CAP readers. Noteworthy amongst their criticisms is the risk to the cardholder from a physical attack in which the cardholder is forced to enter their PIN into a portable reader as the 'verification' of PIN and card details before theft. The risk of physical attack and theft are not unique to individuals carrying CAP readers; however, a cardholder typically enters their PIN at 'relatively' safe locations like an ATM machine or at a retail POS counter. Being able to 'verify' a cardholder's PIN using a card reader on-the-spot, and in a private location, makes the extraction of a PIN number from a cardholder a little more convenient for the criminal – and is an interesting example of the sometimes 'unintended' consequences of an overlooked implementation detail when building secure systems.

While CAP is being implemented by major UK banks in order to improve the security of Internet banking, our 3-D Secure survey, as well as the registration procedures of at least two major UK banks, – indicate that static passwords are currently the predominate method of authentication for 3-D Secure.

Also noteworthy in [134] is the reference to message-level transaction authentication (via an electronic signature device). This report has previously referred to the value of message-level assurances that provide entity as well as data origin authentication, confidentiality and non-repudiation services. However, as also previously noted, the fundamental challenge in

implementing such services is the distribution and safe storage of verifiable keys to both ends of a communicating channel.

From a personal computing perspective, an obstacle to the safe distribution and usage of keys required for message-level assurances comes from the scale of the malware problem that affects personal computers. As uncontrolled and unconstrained devices, personal computers are vulnerable to viruses, Trojans, key-loggers and other forms of malware spread via malicious software and websites [100,101,135,136], as well as from shared devices such as USB drives [137,138]. It becomes extremely difficult to 'attest' to the authenticity of a transaction in such an environment, where any attempt at the distribution and use of secret or public keys may be compromised by malware.

One attempt at creating verifiable cryptographic keys, while simultaneously countering the 'omnipresent threat' of malware, is described in [139]. The scheme is based on a lightweight client-side enrolment and certification process that relies on the presence of a trusted platform module (TPM). The TPM is an embedded security token and is part of the Trusted Computing Group's initiative to provide a secure platform for personal computers, laptops and mobile devices [140]. The scheme described in [139] relies on a manufacturer-created key pair that ships with every TPM – called an endorsement key (EK). The EK can be used to create additional key pairs known as attestation keys (AK), which would then be sent to a scheme manager, or card issuer for certification. The authors of [139] describe such keys as suitable for both mutual authentication in SSL as well as user authentication in 3-D Secure. User-friendly client software would be required in order to communicate with the TPM and scheme manager during the creation and certification of such keys. There are also noted privacy concerns in [139] associated with the use of the platform-specific EK (even if only in the certification process of other key pairs) – with the potential to create a traceable 'super cookie' linking AKs to the EK of a specific device or platform.

Smart cards, with their previously noted security- and convenience related-properties, represent an attractive security platform. Multi-application smart cards in particular [141] offer remarkable opportunities for convenient and secure application development on a single token or card. Contactless smart cards [142], as well as NFC technology [143] combined with mobile handsets will allow a future generation of mobile telephones to act as contactless tokens, or as a reader for other contactless tokens. Imagine a mobile telephone as a remote POS system. A user may simply hold their contactless payment card close to their mobile phone, authenticate via PIN and then authorise a payment transaction for the intended recipient. Smart cards and tokens alone, however, do not solve all of the problems related to building secure systems – as Ross Anderson and his colleagues at Cambridge University, as well as other information security groups around the world, have repeatedly demonstrated. That said, a standards-based and securely evaluated smart card or token, combined with a well implemented scheme, is an attractive alternative to the 'uncontrolled' environment of personal computers for security sensitive functions.

An interesting question to ask at this point – is: what would a smart card or token based scheme for e-commerce look like with today's available technology? Or more interestingly: – what would a scheme look like if it was able to exploit new technology and was driven solely by customer and merchant requirements?

5.2 A Hypothetical E-commerce System

This section describes a hypothetical e-commerce system. System design is driven primarily by customer and merchant requirements. The scheme is naïve in so far as it depends on an imaginary token-containing mobile handset. However, the purpose of this hypothetical system is to illustrate the potential benefits of a scheme that offers message-level assurances and has been designed from a customer and merchant point of view. From a regulatory and geographic perspective, we'll also assume that this scheme falls under a SEPA-like agreement in which inter-bank transfers can be made easily and affordably. We'll call our scheme e-REP (for Really Easy Payments).

The following describes the customer and merchant requirements for the scheme.

5.2.1 Customer Requirements

1. The customer would like to pay quickly and easily with as few intermediary steps as possible.
2. The customer would like to deal only with the merchant.
3. The customer does not want any passwords to remember.
4. The customer would like to be able to shop and pay using any computer or mobile device.
5. The customer would like to be able to shop confidentially, and without the fear of sensitive details like account and payment information being used maliciously by a third-party.
6. The customer would like to be able to choose which, if any, personal details they give to the merchant.
7. The customer would like to be able to choose from whichever financial organisation they feel will give them the best service and support for the given payment scheme.

5.2.2 Merchant Requirements

1. The merchant would like control over the complete shopping and payment experience – without having to redirect the customer to any other entity during the payment process.
2. The merchant would like to receive payment authorization from the customer with as few intermediary steps as possible.
3. The merchant would like to offer a payment option that can be easily and affordably integrated into their existing merchant application.

- The merchant does not want any compliance or regulatory overhead associated with the payment scheme.

5.2.3 Scheme Architecture and Transaction Sequence

Based on the requirements above, Figure 33 illustrates a direct account based 'cheque-like' scheme in which the customer is able to send a secure payment-authorisation message to the merchant.

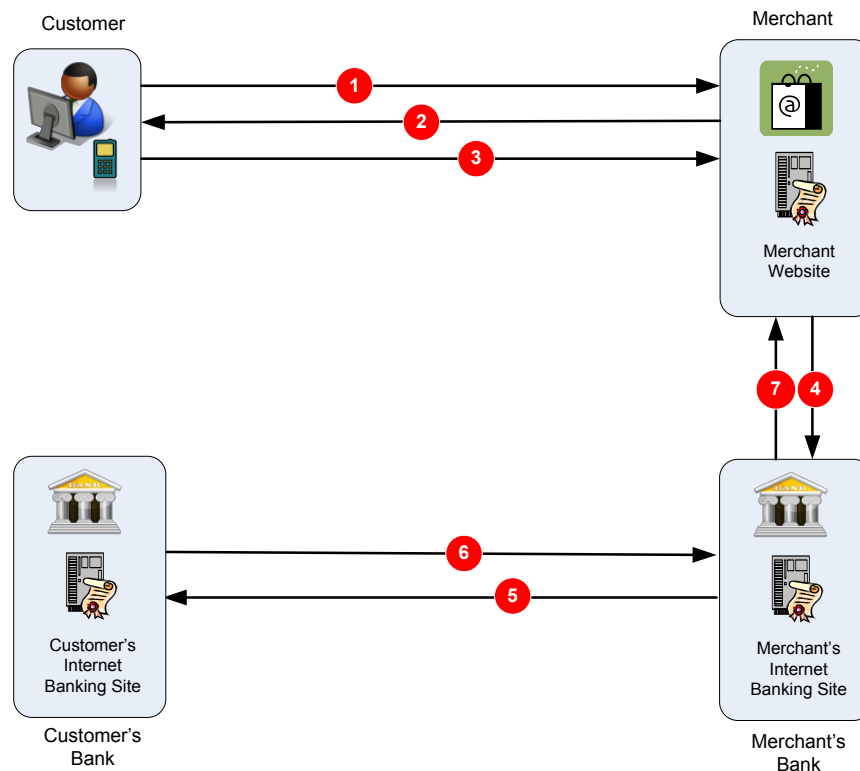


FIGURE 33 - A HYPOTHETICAL TOKEN BASED E-COMMERCE SYSTEM

The transaction sequence for e-REP is as follows:

- As with previous schemes, the customer browses for goods and services at the merchant's website, and then during 'check-out' chooses the e-REP payment method.
- The merchant responds with a specially created e-REP page containing summary order information, payment information as well as an e-REP order number and routing code. The payment details, including e-REP information, are also displayed as a QR code [144], as shown in the figure below.

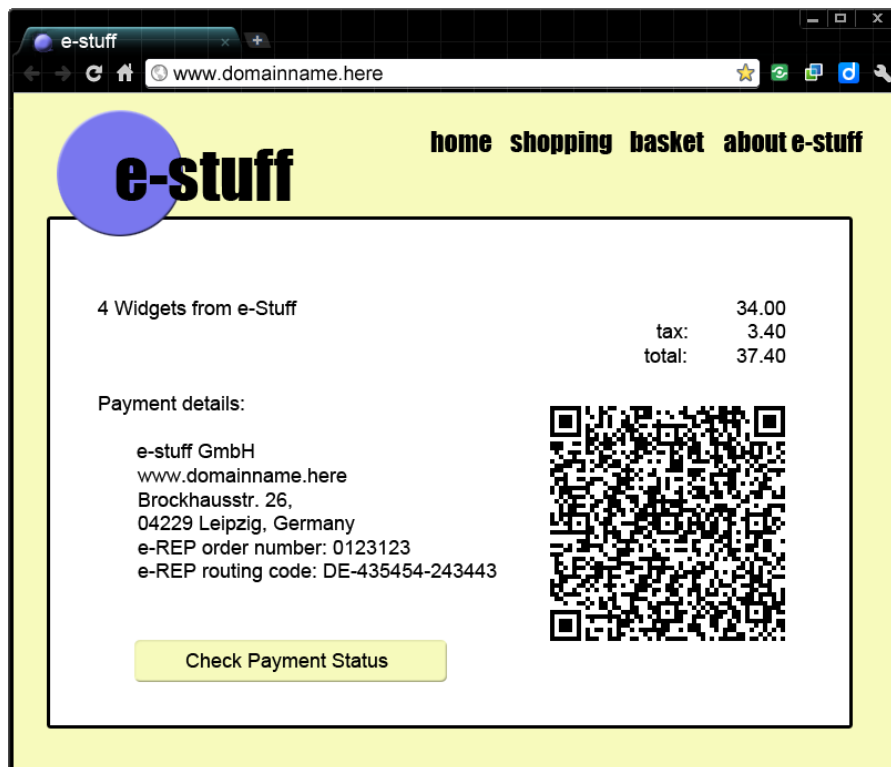


FIGURE 34 - AN E-REP CHECKOUT PAGE WITH QR CODE

3. The customer has a mobile handset equipped with a camera, QR code decoding software, and an issuer-managed secure token containing a shared secret key. The customer holds their mobile handset close to their computer screen and using the camera in their handset – decodes the above QR code. The QR code contains all of the e-REP information required to initiate the payment and is identical to the information displayed to the left of the QR code. The customer authenticates with the e-REP application contained within the handset (via the issuer token) using a PIN and generates an e-REP payment-authorisation message. The token-generated message contains the encrypted payment details (for the beneficiary) as well as encrypted customer details including account name and routing code. The message also contains a public customer-routing code that can be read by the merchant and acquirer. Upon confirmation from the customer, the mobile device transmits the e-REP message via the Internet to the merchant – using the merchant URL and an e-REP application MIME type. The e-REP message is effectively a SEPA-like one-off direct-debit payment authorisation. The e-REP message could also be sent via other means, such as an email attachment, since it is not bound to a particular communication protocol.
4. The merchant forwards the message to their acquiring bank for settlement.
5. Based on the public customer-routing code the merchant's bank forwards the message to the customer's bank.

6. The customer's bank verifies the encrypted e-REP message using the key shared with the token issued to the customer. If verified (and assuming the customer has the required funds or credit balance), the customer's bank will return a payment authorisation result to the merchant's bank, as well as initiate a payment transfer to the merchant's bank.
7. The merchant's bank forwards the payment-authorisation result to the merchant for order completion. Actual payment is credited to the merchant's account via bank transfer from the customer's account in 2-3 days.

5.2.4 E-REP Advantages

The advantages of our (albeit contrived) scheme are:

1. The use of a cryptographic token to create a payment-authorisation message that is bound to both the customer and the beneficiary is both efficient and secure. Such a scheme would be resistant to 'man-in-the-middle' attacks since the digitally encrypted and tamper-resistant message would be worthless to any other party.
2. The scheme requires a minimum number of 'rounds' of communication, so it represents an efficient use of communication channels.
3. The use of a QR code provides an 'air gap' between the un-trusted environment of a personal computer and the trusted token-containing mobile device.
4. The scheme is an improvement over EMV, in so far as the 'terminal' or PIN entry device is under the control of the customer – reducing the risk of PIN compromise.
5. Via the 'application' functions of the token, the scheme offers the potential for additional EMV-like management and risk based functions as well as novel methods of payment instructions. These could include setting purchase limits for authorisation messages, or even the use of 'delegated' authorisation messages that could be given to another party in order to make a payment on behalf of the e-REP token holder (for example in the case of a gift, or gift voucher).

5.2.5 E-REP Disadvantages

1. The first and most obvious disadvantage is that an extra device is required in order to decode the QR code, as well as generate an encrypted and signed e-REP message. This has both cost and usability implications. Customers without mobile handsets could in theory log-in to their Internet banking facilities (like iDEAL) in a separate browser window and initiate an e-REP payment using the order number and routing code above. Those without Internet banking facilities could call their bank, or financial institution and – using an automated menu system – initiate an e-REP payment by entering the order number and routing code above. In both cases, these would be equivalent to a SEPA credit-transfer (or indirect account push-based payment). However, both of these options require non-integrated steps to complete the payment

- including the ‘re-keying’ of routing and order details. And both of these options violate the customer requirement of having to only deal with the merchant.
2. The second disadvantage is that, even with such a device, the scheme has not described the enrolment process for the customer in order to receive the issuer controlled security token. There would be administrative and infrastructure-related costs in deploying such tokens and applications securely.
 3. The customer must also rely on regular URL, certification, and reputational-related factors in order to establish trust with the merchant since the merchant is not explicitly authenticated in the scheme.
 4. The payment-authorisation result messages – sent from the customer’s bank, to the merchant’s bank and then to the merchant – will need to be protected from tampering. This requires the additional cost of either a scheme-based PKI and CA, or the use of public keys and certificates provided via commercial CAs.

5.2.6 E-REP Summary

Since this is a contrived example, we’ll not create an e-REP scorecard as the values here would be equally contrived. The scheme does however demonstrate the potential for providing convenient and extremely efficient message-level assurances via an issuer-managed security token.

An obvious question to ask is why don’t schemes like e-REP exist today? As described above, the first obstacle is the cost and availability of mobile devices capable of hosting secure tokens.

However, there is another factor that may have had a significant impact on the development of such devices. In Europe, it is common practise to tie the subsidised price of a mobile handset to a mobile-telephone-operator contract – effectively locking a customer into an agreement with a particular mobile operator for the term of the contract. The advantage to the customer is that they receive an otherwise expensive handset at a significantly reduced price. The advantage to the mobile network operator is that they receive guaranteed payments for the term of the contract. More importantly, however, mobile network operators have tried (mostly unsuccessfully) to leverage their existing network infrastructure including customer and billing systems – into providing value-added services. These services included alternative payment schemes. A notable example is Vodafone’s Mpay programme, as well as a recent announcement from AT&T, Verizon, and T-Mobile [116].

The effects of subsidising handsets through mobile-operator contracts, as well as mobile operator attempts to leverage their existing network and infrastructure to provide alternative payment schemes – mean that mobile operators have had an enormous influence over the choice, and even design, of mobile handsets. It was simply not in the mobile operator’s interest to offer handsets with advanced features, including support for technology that would have allowed customers access to non-mobile operator-based payment schemes.

In summary, our e-REP scheme was intended to demonstrate the potential of a message-level secure token-based scheme. And that the use of an issuer-managed security token can enhance both the security and efficiency of a payment scheme as well as satisfying the major requirements of both the customer and merchant. However, the cost of such a scheme – as well as potentially negative pressures on mobile handset innovation – has meant that such schemes have not yet seen wide-scale development or deployment.

6. Conclusion

The historical context presented earlier in this report makes clear that both the Internet and e-commerce have developed in ways that were unanticipated by their creators. And that this unanticipated growth was driven by novel methods of communication and trade. However inherent weaknesses in security, combined with the fundamental challenges of establishing trust and identity, meant that growth on the Internet, was followed closely by increasing levels of malicious and criminal activities online.

Our brief history of payment cards describes the arrival and social acceptance of credit cards (and later debit cards) as a convenient and well understood mechanism for making payments in the 'real' world. The growth of the payment card industry as a whole was facilitated by banking communities and the formation of a four-party system linked together by branded payment card networks such as Visa and MasterCard.

As e-commerce developed – and despite attempts to develop alternative and arguably more suitable schemes for making payments online – payment cards became the predominate method for making payments in web based e-commerce.

This report also makes clear that the use of payment cards in e-commerce resulted in yet another set of challenges (and an entire industry) related to the protection of card and cardholder data. In fact, the threat of theft and the fraudulent use of card and cardholder data was so great that scheme rules designed to protect cardholders from fraudulent transactions were introduced in the form of 'chargebacks'. Chargebacks have protected cardholders – allowing them to shop online without fear of suffering a financial loss from fraudulent transactions. And yet chargebacks also arguably dumped the risk of accepting such transactions onto merchants.

In 1994 work began on the EMV standard – a standard designed to reduce the level of fraud in 'card present' transactions. The scheme has been credited with a significant reduction in card present fraud and is an example of the effective use of smart cards in a financial application. However, as EMV reached wide-scale deployment, CNP fraud continued to rise dramatically online. The success of EMV itself was credited in part for the shift in criminal activity to a method of payment that was now seen as the 'softer' target in the payment card industry.

In 1996, Visa and MasterCard began working on SET – a comprehensive and secure scheme for e-commerce. Despite the scheme's security features, SET failed to achieve commercial success.

In 2001, Visa (and later MasterCard) began work on 3-D Secure: another attempt at introducing security features designed to reduce CNP fraud online.

What's interesting about this short history of payment card systems and security is that it highlights the fact that it has taken more than eight years for a scheme designed to combat CNP fraud to become widely implemented. And that, having finally reached wider-scale implementation, there have been questions raised about the scheme's design, as well as the negative impact it may have had on merchants in the form of shopping card abandonment.

The objectives of this report include a technical review of 3-D Secure. It also includes an attempt to answer questions about 3-D Secure's suitability as a method for preventing CNP fraud and whether 3-D Secure represents good security practises, or not.

From an architectural point of view, 3-D Secure appears split between two models. By 'reaching out' and contacting the issuer for authentication, almost all of the required infrastructure has been put into place to enable an indirect push model that includes payment authorisation and the crediting of the merchant's account. And yet, the model still operates as a direct account-based cheque-like scheme where the merchant is given payment authorisation instructions for settlement via the regular acquirer/issuer route. The separation of authentication and authorisation channels in this way represents additional communication overhead.

In attempting to conclude whether 3-D Secure represents good security practises – it is this author's opinion that 3-D Secure neither espouses nor represents best practises in information security: has failings in ownership, communication, usability, and security while simultaneously burdens cardholders with yet another password-based scheme. What's more, 3-D Secure does nothing to reduce compliance-related costs associated with the handling of payment card data. Nor does it address the fundamental problem of using payment cards in a way never indented – including the repeated transmission of sensitive card and cardholder data to every merchant for every transaction.

While it would be fair to say that 3-D Secure was not designed to correct the fundamental weaknesses associated with the use of payment cards in e-commerce, it is also this author's opinion that – given the magnitude of CNP-related losses in the UK alone – 3-D Secure demonstrates a lack of innovation and progress within the payment card industry as a whole. From 2000 to 2009, a total of 993.3 million pounds sterling were attributed to Internet and e-commerce fraud losses in the UK [27]. It's likely that a large percentage of these losses were born by merchants in the form of fraud-related 'chargebacks'. What percentage of these losses, on a global scale, would have been required to invest in a scheme that radically improved the security of e-commerce?

Another stated objectives of this report, is an attempt to answer the question of:

“...whether given the current ‘state of affairs’ of e-commerce and online payments systems, 3-D Secure was the right thing to do given all of the above, or whether alternative solutions would have been more appropriate.”

The simple answer is that there did not appear to be any other choice. Without evidence of any alternative solution in development, and in the face of the continued rise of CNP fraud, 3-D Secure was the only scheme available to the payment card industry.

MasterCard in 2006 [145], and Visa in 2008 [146] underwent corporate restructuring and – in the USA – are now both publicly listed companies. An analysis of the impact of this restructuring is outside of the scope of this paper; however, it would be correct to say that MasterCard and Visa now have an obligation to their shareholders, as well as their scheme members.

Concerns have, however, been expressed about the influence the ‘Visa / MasterCard duopoly’ may be having in Europe and, in particular, over the SEPA initiative [147].

Perhaps conflicting obligations, combined with the luxury of market dominance, have contributed to the slow pace of innovation in traditional payment card-based e-commerce. Or perhaps, the largest factor in the lack of progress is one of liability. What would the world of e-commerce look like today if the scheme operators themselves, namely Visa and MasterCard, had been forced to accept the liability for the fraudulent use of their own payment instruments – instead of handing the bulk of that liability to merchants?

Looking to the future, it seems unlikely that 3-D Secure will remain in its present form for long. At some point the changes required to address the fundamental weaknesses of using payment card data online will be made. Perhaps EMV will be fully extended to support remote tokens and devices, allowing cardholders to authenticate and authorise a payment transaction via a more efficient and secure message-level-based scheme.

In the meantime, alternatives to traditional payment card-based schemes will continue to emerge, with e-commerce as a whole likely to see dramatic changes over the coming years as the potential for integrating smart cards and tokens with mobile devices is fully realised.

What remains to be seen, however, is whether any scheme that achieves wide-scale implementation and commercial success does so because of merits in customer and merchant usability, convenience and security – or because of the influence and leverage of ‘other vested interests’.

Bibliography

- [1] Internet Usage Statistics, 2010. Internet World Stats.
<http://www.internetworldstats.com/stats.htm> (accessed Sept 28, 2010).
- [2] Internet Access, 2010. Office For National Statistics.
<http://www.statistics.gov.uk/cci/nugget.asp?id=8> (accessed Sept 28, 2010).
- [3] A Brief History of the Internet. <http://www.isoc.org/internet/history/brief.shtml> (accessed Nov 04, 2010).
- [4] 15 ways the Internet is changing the world. <http://www.telenor.com/en/news-and-media/articles/2010/15-ways-the-internet-is-changing-the-world> (accessed Sept 28, 2010).
- [5] IC3 2009 Annual Report on Internet Crime Released, 2010. IC3.
<http://www.ic3.gov/media/2010/100312.aspx> (accessed Aug 12, 2010).
- [6] New figures show cyber crime on the rise, 2009. Guardian.co.uk.
<http://www.guardian.co.uk/technology/2009/mar/30/internet-cyber-crime> (accessed Aug 12, 2010).
- [7] Plastic Fraud Figures (2009).
[http://www.theukcardsassociation.org.uk/view_point_and_publications/facts_and_figures/plastic_fraud_figures_\(2009\)/](http://www.theukcardsassociation.org.uk/view_point_and_publications/facts_and_figures/plastic_fraud_figures_(2009)/) (accessed Sept 15, 2010).
- [8] How Cybercriminals Steal Money. http://www.neildaswani.com/?page_id=7 (accessed Sept 28, 2010).
- [9] Information Management: A Proposal. <http://www.w3.org/History/1989/proposal.html> (accessed Oct 19, 2010).
- [10] A Little History of the World Wide Web. <http://www.w3.org/History.html> (accessed Oct 19, 2010).
- [11] Transport Layer Security. http://en.wikipedia.org/wiki/Secure_Sockets_Layer (accessed Oct 19, 2010).
- [12] Boston Consulting Group Report. <http://www.connectedkingdom.co.uk/the-report/> (accessed Nov 02, 2010).
- [13] O. E. Akindemowo, The Fading Rustle, Chink and Jingle: Electronic Value and the Concept of Money, *University of New South Wales Law Journal* **1998**, 24 (21)(20).
- [14] C. European Parliament, *Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions*; Eu, 2009.
- [15] R. Weber, *Chablis - Market Analysis of Digital Payment Systems (TUM-I9819)*; Institute for Information The Technical University of Munich, 1999.
- [16] L. Peiro, N. Asokan, M. Steiner, and M. Waidner, Designing a generic payment service, *IBM Systems Journal* **1998**, 37 (1), 72-88.
- [17] B. Valerie-Anne, L. Van Hove, and M. Hartmann, *Classifying Payment Instruments - A Matryoshka Approach*; European Central Bank, 2009.

- [18] R. Boer, C. Hensen, and A. Screpnic, *Online Payments 2010*; Innopay BV, 2010.
- [19] D. Chaum, A. Fiat, and M. Naor, Untraceable Electronic Cash, *CRYPTO '88 Proceedings on Advances in cryptology*, 1990; pp 319-327.
- [20] Mondex. <http://www.mondex.com/> (accessed Dec 05, 2010).
- [21] S. Glassman, M. Manasse, M. Abadi, P. Gauthier, and P. Sobalvarro. The Millicent Protocol for Inexpensive Electronic Commerce. <http://www.w3.org/Conferences/WWW4/Papers/246/> (accessed Dec 05, 2010).
- [22] E. Gerson and B. Woolsey. The History of Credit Cards, 2009. <http://www.creditcards.com>. <http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php> (accessed Nov 22, 2010).
- [23] J. Nocera. *A Piece of the Action: How the Middle Class Joined the Money Class*; Touchstone, 1995.
- [24] Company Milestones. http://www.mastercard.com/us/company/en/ourcompany/company_milestones.html (accessed March 04, 2011).
- [25] *Benefits of Open Payment Systems and the Role of Interchange*; MasterCard Worldwide, 2009.
- [26] *Visa U.S.A. Consumer Credit - Interchange Reimbursement Fees*; Visa Inc, 2010.
- [27] *FRAUD The Facts - 2010 - The Definitive Overview of Payment Industry Fraud and Measures to Improve it.*; Financial Fraud Action UK, 2010.
- [28] Payment Cards. <http://www.interpol.int/Public/CreditCards/Default.asp> (accessed Dec 06, 2010).
- [29] K. E. Mayes and K. Markantonakis. Smart Cards for Banking and Finance. In *Smart Cards, Tokens, Security and Applications*; Springer, 2008; p 117.
- [30] ISO/IEC 7811-2:2001. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31440 (accessed Jan 29, 2011).
- [31] Magnetic Stripe. <http://cobweb.ecn.purdue.edu/~tanchoco/MHE/ADC-is/Magnetic/main.shtml> (accessed Jan 29, 2011).
- [32] About EMV. http://www.emvco.com/about_emv.aspx (accessed Dec 07, 2010).
- [33] ISO/IEC 7816-1:1998. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29257 (accessed Dec 14, 2010).
- [34] K. E. Mayes and K. Markantonakis. An Introduction to Smart Card. In *Smart Cards, Tokens, Security and Applications*; Springer, 2008; pp 1-25.
- [35] The Common Criteria. <http://www.commoncriteriaportal.org/cc/> (accessed Dec 15, 2010).
- [36] EMV Books 1-4 Version 4.2 2008. <http://www.emvco.com/specifications.aspx> (accessed Dec 12, 2010).

- [37] H. X. Mel and D. M. Baker. *Cryptography Decrypted*; Addison-Wesley Professional, 2000.
- [38] R. J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*; Wiley, 2008.
- [39] F. Piper. *Cryptography: A Very Short Introduction*; Oxford University Press, 2002.
- [40] R. Anderson, M. Bond, and S. Murdoch, *Chip and Spin*; Computer Labaoratory, University of Cambridge, 2005.
- [41] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond. EMV PIN verification “wedge” vulnerability. <http://www.cl.cam.ac.uk/research/security/banking/nopin/> (accessed Dec 13, 2010).
- [42] P. Gutmann, PKI: it's not dead, just resting, *Computer* **2002**, 35 (8).
- [43] D. Saar and S. J. Murdoch. Tamper resistance of Chip & PIN (EMV) terminals. <http://www.cl.cam.ac.uk/research/security/banking/tamper/> (accessed Dec 13, 2010).
- [44] S. Drimer and S. J. Murdoch. Chip & PIN (EMV) relay attacks. <http://www.cl.cam.ac.uk/research/security/banking/relay/> (accessed Dec 13, 2010).
- [45] Banking Code Standards Board. <http://www.bankingcode.org.uk/> (accessed Dec 13, 2010).
- [46] HSBC Merchant Services – Card not present fraud. <http://www.hsbc.co.uk/1/2/business/info/card-fraud/card-not-present> (accessed Dec 17, 2010).
- [47] Card-not-present sales. http://www.visaeurope.com/en/businesses_retailers/retailers_and_merchants/security/handling_visa_payments/card-not-present_sales.aspx (accessed Dec 16, 2010).
- [48] Your rights when paying by credit card. <http://www.which.co.uk/consumer-rights/sale-of-goods/your-rights-when-paying-by-credit-card/> (accessed Feb 11, 2011).
- [49] Cartoon Captures Spirit of the Internet. <http://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html> (accessed Oct 19, 2010).
- [50] On the Internet, nobody knows you're a dog. http://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you're_a_dog (accessed Oct 19, 2010).
- [51] R. Rasmussen and G. Aaron, *Global Phishing Survey: Trends and Domain Name Use 1H2010*; APWG, 2010.
- [52] Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce. http://www.gartner.com/press_releases/asset_129754_11.html (accessed Dec 07, 2010).
- [53] *RSA Monthly Online Fraud Report - January 2011*; RSA, 2011.
- [54] *Phishing Activity Trends Report - 1st Quarter 2010*; APWG, 2010.

- [55] PCI Security Standards Council.
https://www.pcisecuritystandards.org/organization_info/index.php (accessed Dec 6, 2010).
- [56] MasterCard warns of massive credit-card breach.
<http://www.securityfocus.com/news/11219> (accessed Feb 19, 2011).
- [57] Cost of PCI Compliance.
http://blog.elementps.com/element_payment_solutions/2009/02/pci-compliance-costs.html (accessed March 03, 2011).
- [58] C. Albrecht, L. Bombard, B. He, and S. Malone, Building Trust for Electronic Commerce — An evaluation of SSL and SET, *Capstone Papers* **2006**.
- [59] W. Stallings. Secure Electronic Transaction (SET). In *Network Security Essentials: Applications and Standards (4th Edition)*; Prentice Hall, 2010; pp 223-234.
- [60] P. Jarupunphol and C. Mitchell, Failures of SET implementation - What is amiss?, *7th Asia-Pacific Decision Sciences Institute Conference*, Bangkok, 2002.
- [61] A. Whitten and J. Tygar, Why Johnny can't encrypt: a usability evaluation of PGP 5.0, *SSYM'99 Proceedings of the 8th conference on USENIX Security Symposium*, 1999.
- [62] S. L. Garfinkel, *Design Principles and Patterns for Computer Systems That are Simultaneously Secure and Usable*; Doctor of Philosophy in Computer Science and Engineering; Massachusetts Institute of Technology, 2005.
- [63] A "change in user behavior". <http://www.identityblog.com/?p=1166> (accessed March 04, 2011).
- [64] G. Agnew. Secure Electronic Transactions: Overview, Capabilities, and Current Status. In *Payment Technologies for E-commerce*; Springer, 2003; pp 211 - 226.
- [65] Verified by Visa. <https://usa.visa.com/personal/security/vbv/index.jsp> (accessed March 04, 2011).
- [66] M. Merkow. Mastercard's Response to the Online Payments Quandary, 2002. ECommerce-Guide. <http://www.ecommerce-guide.com/news/trends/article.php/952181> (accessed Jan 04, 2011).
- [67] MasterCard SecureCode.
http://www.mastercard.com/in/merchant/en/security/what_can_do/SecureCode/index.html (accessed March 04, 2011).
- [68] *Verified by Visa System Overview External Version 1.0.2*; Visa International Services Association, 2006.
- [69] *The SecureCode Merchant Implementation Guide*; MasterCard International, 2005.
- [70] *3-D Secure Acquirer and Merchant Implementation Guide*; Visa U.S.A Inc, 2004.
- [71] *3-D Secure Protocol Specification - Core Functions*; Visa International, 2002.
- [72] *Seventh Annual UK Online Fraud Report - 2011 Edition*; CyberSource Ltd, 2011.
- [73] Verified by Visa: a conversion rate killer? <http://econsultancy.com/uk/blog/3887-verified-by-visa-a-conversion-rate-killer> (accessed Jan 25, 2011).

- [74] Q&A: Ethical Superstore CEO Andy Redfern. <http://econsultancy.com/uk/blog/3865-qa-ethical-superstore-ceo-andy-redfern> (accessed Jan 25, 2011).
- [75] 3D Secure Might Bust Your Conversions. <http://www.northsouthmedia.co.uk/blog/3d-secure-might-bust-your-conversions/> (accessed Jan 25, 2011).
- [76] What do people think about 3-D Secure - Verified by Visa or MasterCard SecureCode? <http://www.quora.com/E-Commerce/What-do-people-think-about-3-D-Secure-Verified-by-Visa-or-MasterCard-SecureCode> (accessed Dec 12, 2010).
- [77] S. J. Murdoch and R. Anderson, Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication, *Financial Cryptography and Data Security 2010*, Tenerife, 2010.
- [78] Credit Cards. <http://www2.firstdirect.com/1/2/creditcards> (accessed Jan 31, 2011).
- [79] Credit Cards. <http://www.barclays.co.uk/Creditcards/P1242557963445> (accessed Jan 31, 2011).
- [80] Credit Cards. <http://www.hsbc.co.uk/1/2/personal/credit-cards> (accessed Jan 31, 2011).
- [81] C.-M. Karat, C. Brodie, and J. Karat. Usability Design and Evaluation for Privacy and Security Solutions. In *Security and Usability*; L. F. Cranor and S. Garfinkel, Eds.; O'Reilly Media, Inc., 2005; pp 47-74.
- [82] A. S. Patrick, P. Briggs, and S. Marsh. Designing Systems That People Will Trust. In *Security and Usability*; L. F. Cranor and S. Garfinkel, Eds.; O'Reilly Media, Inc., 2005; pp 75-99.
- [83] Y. Ka-Ping. Guidelines and Strategies for Secure Interaction Design. In *Security and Usability*; L. F. Cranor and S. Garfinkel, Eds.; O'Reilly Media, Inc., 2005; pp 247-273.
- [84] 3D Secure or not? <http://www.foviance.com/what-we-think/3d-secure-or-not/> (accessed Jan 31, 2011).
- [85] Who benefits from 3-D Secure? <http://www.quora.com/E-Commerce/Who-benefits-from-3-D-Secure> (accessed Feb 18, 2011).
- [86] Verified by Visa security program used as bait in phishing scams. <http://www.internetretailer.com/2005/01/06/verified-by-visa-security-program-used-as-bait-in-phishing-scams> (accessed Jan 30, 2011).
- [87] Online Card Security. <http://www1.firstdirect.com/1/2/creditcards/online-card-security> (accessed March 11, 2011).
- [88] U. Piazzalunga, P. Salvaneschi, and P. Coffetti. The Usability of Security Devices. In *Security and Usability*; L. F. Cranor and S. Garfinkel, Eds.; O'Reilly Media, Inc, 2005; pp 221-242.
- [89] *Two-Factor Authentication: An essential guide in the fight against Internet fraud*; GPayments, 2006.
- [90] PayPal Inc - History. <http://www.fundinguniverse.com/company-histories/PayPal-Inc-Company-History.html> (accessed Feb 05, 2011).
- [91] How PayPal Works. <http://money.howstuffworks.com/paypal3.htm> (accessed Feb 05,

- 2011).
- [92] PayPal. <https://www.paypal.co.uk/> (accessed Feb 06, 2011).
- [93] Integrating PayPal Payments into E-Commerce Applications with ASP.NET. <http://www.west-wind.com/presentations/PayPalIntegration/PayPalIntegration.asp> (accessed Feb 09, 2011).
- [94] Paypal phishing emails - scam attacks with actual examples. http://www.webdevelopersnotes.com/articles/paypal_phishing_scam_email_attacks.php (accessed Feb 07, 2011).
- [95] New Technique [against] PayPal. <http://securitylabs.websense.com/content/Alerts/704.aspx> (accessed Feb 07, 2011).
- [96] 419 Scams go Phishing. <http://community.websense.com/blogs/securitylabs/archive/2010/08/09/nigerian-scams-meet-phishing.aspx> (accessed Feb 07, 2011).
- [97] PayPal Phishing Attack. http://www.us-cert.gov/current/archive/2008/04/08/archive.html#paypal_phishing_attack (accessed Feb 07, 2011).
- [98] PayPal Security Flaw allows Identity Theft. http://news.netcraft.com/archives/2006/06/16/paypal_security_flaw_allows_identity_theft.html (accessed Feb 07, 2011).
- [99] Tis the Season of DDoS – WikiLeaks Edition. <http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-edition/> (accessed Feb 07, 2011).
- [100] Monthly Malware Statistics, January 2011. http://www.securelist.com/en/analysis/204792159/Monthly_Malware_Statistics_January_2011 (accessed Feb 21, 2011).
- [101] Phishing, Spam and Malware Statistics for December 2010. <http://techblog.avira.com/2011/01/21/phishing-spam-and-malware-statistics-for-december-2010/en/> (accessed Feb 21, 2011).
- [102] Chargeback on credit and debit cards. <http://www.which.co.uk/consumer-rights/sale-of-goods/your-rights-when-paying-by-credit-card/chargeback-on-credit-and-debit-cards/> (accessed Feb 07, 2011).
- [103] PayPal.com and payment APIs hit by performance issues. <http://news.netcraft.com/archives/2011/02/18/paypal-com-and-payment-apis-hit-by-performance-issues.html> (accessed Feb 20, 2011).
- [104] Assessing Criticism of PayPal. http://www.wilsonweb.com/wct5/paypal_assess.htm (accessed Feb 07, 2011).
- [105] The Problem with Paypal. <http://www.kudzuworld.com/blogs/tech/paypal.en.aspx> (accessed Feb 07, 2011).
- [106] PayPal Is Still A "Drop In the Bucket". <http://www.businessinsider.com/chart-of-the-day-paypal-volume-2011-1> (accessed Feb 07, 2011).
- [107] iDEAL - Home. <http://www.ideal.nl/> (accessed Feb 07, 2011).

- [108] Currence. <http://www.currence.nl> (accessed Feb 12, 2011).
- [109] Banking Services - Netherlands.
<http://www.justlanded.com/english/Netherlands/Netherlands-Guide/Money/Banking-Services> (accessed Feb 16, 2011).
- [110] Debit Cards - The Netherlands.
http://en.wikipedia.org/wiki/Debit_card#The_Netherlands (accessed Feb 16, 2011).
- [111] Thuiswinkel Waarborg (The Home Shopping Organisation). <http://www.thuiswinkel.org/> (accessed Feb 16, 2011).
- [112] Barclaycard and Orange unwrap contactless credit card. [16](#) (accessed 2011 02, 2011).
- [113] 125 million iOS devices morph into credit card terminals.
<http://www.zdnet.com/blog/apple/125-million-ios-devices-morph-into-credit-card-terminals/8665> (accessed Feb 16, 2011).
- [114] Start Accepting Credit Cards on your iPhone. (accessed Feb 16, 2011).
- [115] Subway to use FaceCash mobile payments.
<http://www.finextra.com/News/Announcement.aspx?pressreleaseid=36710> (accessed Feb 16, 2011).
- [116] AT&T, Verizon, and T-Mobile make plans to replace credit cards with smartphones.
<http://venturebeat.com/2010/08/02/att-verizon-and-t-mobile-make-plans-to-replace-credit-cards-with-smartphones/> (accessed Feb 16, 2011).
- [117] Visa officially announces their case that turns your iPhone into a credit card.
<http://www.mobilecrunch.com/2010/05/17/visa-officially-announces-their-case-that-turns-your-iphone-into-a-credit-card-and-weve-got-pics/> (accessed Feb 16, 2011).
- [118] DeviceFideleity Announces Mobile Contactless Payment Solution for iPhone.
<http://corporate.visa.com/media-center/press-releases/press1018.jsp> (accessed Feb 16, 2011).
- [119] Citi Begins Offering Customers Contactless-Payment Stickers.
<http://www.paymentsource.com/news/citi-begins-offering-contactless-payment-stickers-3002023-1.html> (accessed Feb 16, 2011).
- [120] Amazon Payments. <http://payments.amazon.com/sdui/sdui/home> (accessed Feb 20, 2011).
- [121] Google Checkout. <http://www.google.com/checkout/> (accessed Feb 20, 2011).
- [122] Facebook Credits. <http://www.facebook.com/credits/> (accessed Feb 20, 2011).
- [123] Twitpay. <http://twitpay.com/> (accessed Feb 20, 2011).
- [124] iTunes. <http://www.apple.com/itunes/> (accessed Feb 16, 2011).
- [125] Apps for iPhone. <http://www.apple.com/iphone/apps-for-iphone/> (accessed Feb 16, 2011).
- [126] SEPA - Single Euro Payments Area.
<http://www.ecb.europa.eu/paym/sepa/html/index.en.html> (accessed Feb 20, 2011).

- [127] SEPA Vision and Goals.
http://www.europeanpaymentscouncil.eu/content.cfm?page=sepa_vision_and_goals
(accessed March 05, 2011).
- [128] SEPA for Cards.
http://www.europeanpaymentscouncil.eu/content.cfm?page=sepa_vision_for_cards
(accessed March 05, 2011).
- [129] Payment Services Directive (PSD).
http://ec.europa.eu/internal_market/payments/framework/psd_en.htm (accessed Feb 11, 2011).
- [130] ICPNO. <http://www.icpno.org/index.asp> (accessed Feb 16, 2011).
- [131] ICPNO wants simplified online payment rules by 2010.
<http://www.telecompaper.com/news/icpno-wants-simplified-online-payment-rules-by-2010> (accessed Feb 11, 2011).
- [132] About the PINsentry card reader.
<http://www.barclays.co.uk/Helpsupport/AboutthePINsentrycardreader/P1242560253440> (accessed Feb 21, 2011).
- [133] Card-Reader. <http://www.natwest.com/personal/online-banking/g1/banking-safely-online/card-reader.ashx> (accessed Feb 21, 2011).
- [134] S. Drimer, S. J. Murdoch, and R. Anderson, Optimised to Fail: Card Readers for Online Banking, *Financial Cryptography and Data Security '09*, 2009.
- [135] All Your iFrame Are Point to Us. <http://googleonlinesecurity.blogspot.com/2008/02/all-your-iframe-are-point-to-us.html> (accessed Feb 21, 2011).
- [136] Internet Security Threat Report: Mid-Term Report.
<http://www.symantec.com/business/theme.jsp?themeid=threatreport> (accessed Feb 21, 2011).
- [137] Majority of Malware Attacks are Triggered by USB Enabled Drives.
<http://www.dngnet.com/2011/01/majority-of-malware-attacks-are-triggered-by-usb-enabled-drives/> (accessed Feb 21, 2011).
- [138] One in eight malware attacks come via USB.
<http://www.itworld.com/security/126540/usb-devices-play-part-one-out-every-eight-attacks> (accessed Feb 21, 2011).
- [139] S. Balfe and K. G. Paterson, Augmenting Internet-based Card Not Present Transactions with Trusted Computing, *Financial Cryptography 2008, Lecture Notes in Computer Science Vol. 5143*, 171-175.
- [140] Trusted Platform Module.
<http://www.trustedcomputinggroup.org/solutions/authentication> (accessed Feb 22, 2011).
- [141] K. Markantonakis. Multi Application Smart Card Platforms and Operating Systems. In *Smart Cards, Tokens, Security Applications*; K. Mayes and K. Markantonakis, Eds.; Springer, 2008; pp 51-83.
- [142] ISO/IEC 14443-1:2008.
http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber

[=39693](#) (accessed Feb 23, 2011).

[143] NFC Forum. <http://www.nfc-forum.org/home/> (accessed Feb 23, 2011).

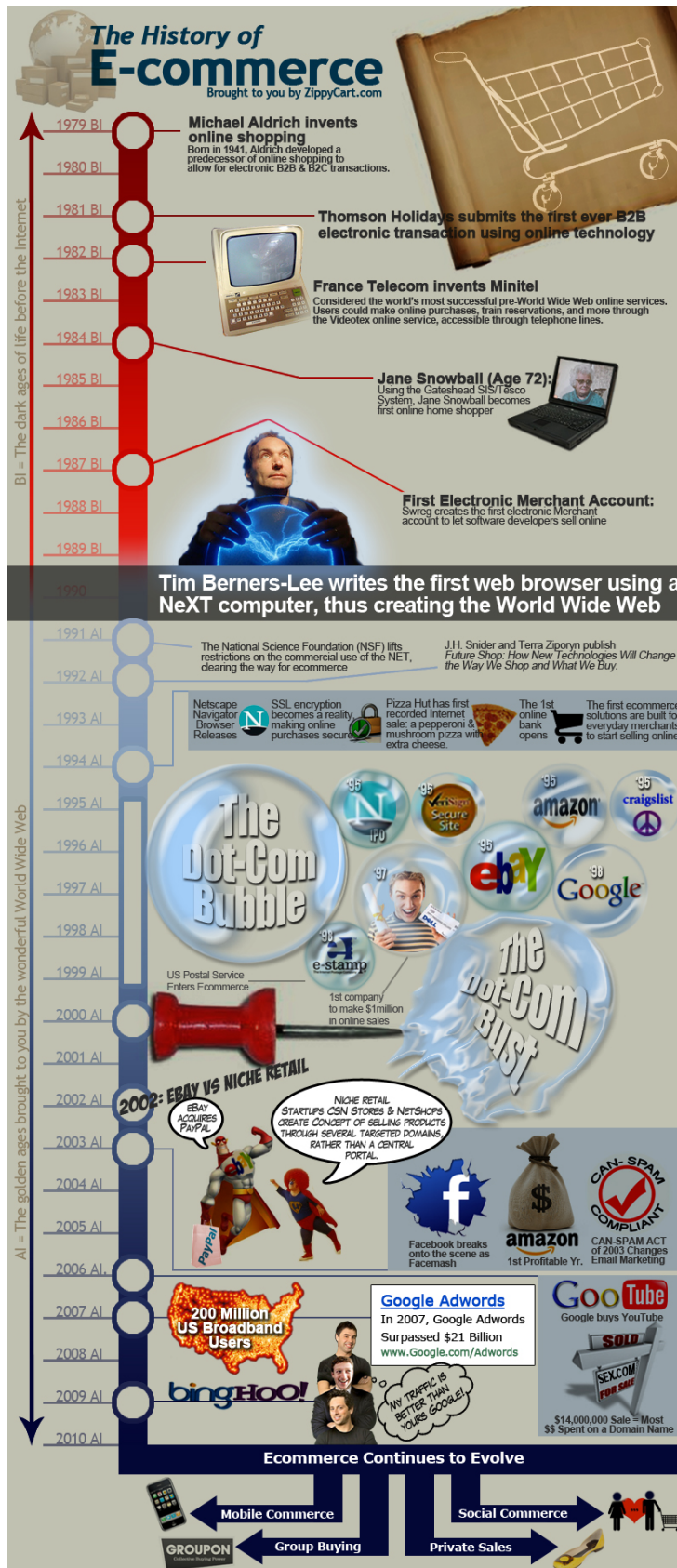
[144] About 2D Code. <http://www.denso-wave.com/qrcode/aboutqr-e.html> (accessed Feb 25, 2011).

[145] Corporate Report. <http://www.mastercard.com/us/company/en/corporate/letter.html> (accessed March 02, 2011).

[146] *Visa Inc. Corporate Overview*; Corporate Report; Visa Inc., 2009.

[147] Concerns about domination Visa and MasterCard in Europe.
<http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/1800653/2010/12/09/Zorgen-over-dominantie-Visa-en-Mastercard-in-Europa.dhtml> (accessed March 02, 2011).

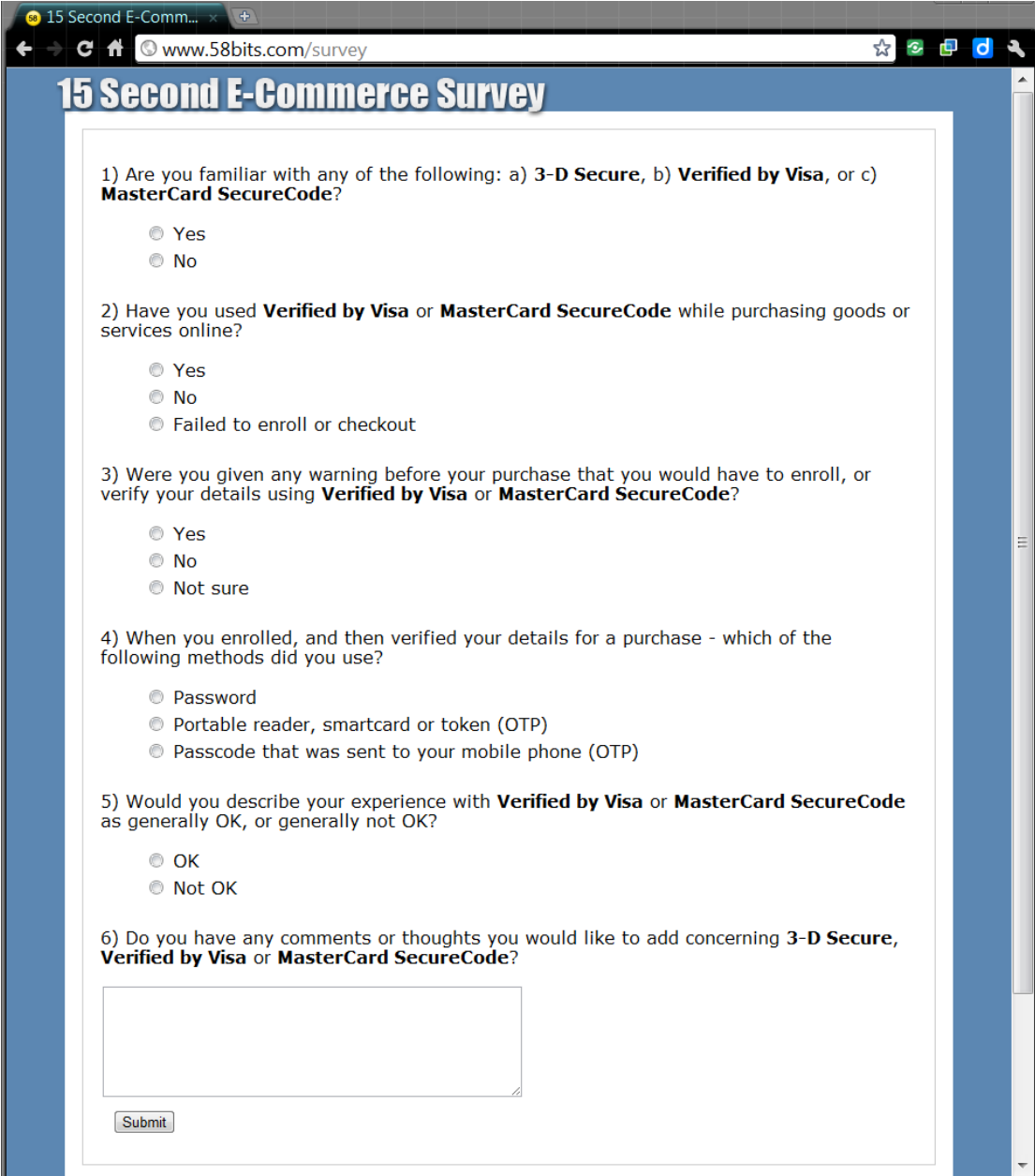
Appendix A – The History of E-commerce



(Source: <http://zippycart.com/infographics/e-commerce-history.html> used with permission under the Creative Commons Attribution-NoDerivs 3.0 Unported License)

Appendix B – Survey

1. Survey Screenshot



15 Second E-Commerce Survey

1) Are you familiar with any of the following: a) **3-D Secure**, b) **Verified by Visa**, or c) **MasterCard SecureCode**?

Yes
 No

2) Have you used **Verified by Visa** or **MasterCard SecureCode** while purchasing goods or services online?

Yes
 No
 Failed to enroll or checkout

3) Were you given any warning before your purchase that you would have to enroll, or verify your details using **Verified by Visa** or **MasterCard SecureCode**?

Yes
 No
 Not sure

4) When you enrolled, and then verified your details for a purchase - which of the following methods did you use?

Password
 Portable reader, smartcard or token (OTP)
 Passcode that was sent to your mobile phone (OTP)

5) Would you describe your experience with **Verified by Visa** or **MasterCard SecureCode** as generally OK, or generally not OK?

OK
 Not OK

6) Do you have any comments or thoughts you would like to add concerning **3-D Secure**, **Verified by Visa** or **MasterCard SecureCode**?

2. Survey Data

1) Have Heard Of	2) Have Used	3) Knew Beforehand	4) Authentication Method	5) OK/ NOT OK	6) Comments
YES	YES	NOT SURE	PASSWORD	NOT OK	Apparently verified by visa has some password size limit (which is too small) so confirming my password works but authenticating with it fails. :-) So to authenticate I end up entering my credit card confirmation details which is close to what I enter in my order already so it's no more secure and just wastes my time.
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	OTP SMS	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	I'm not entirely sure why it's beneficial – it's very light on explaining how it improves security.
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	Uneven implementation by merchant websites. One website forced Verified by Visa, while it was optional at another merchant. No perceivable value. Hard to "opt-out" of the program. Eventually stopped shopping at the merchant site.
YES	YES	NOT SURE	OTP SMS	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	NO	NOT SURE	PASSWORD	OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	NO	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	NO	NOT SURE	NULL	NULL	NULL
YES	YES	KNEW	READER OR TOKEN	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	NOT SURE	READER OR TOKEN	OK	One name would be better. Why three?
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	NO	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
NO	YES	KNEW	PASSWORD	NOT OK	Too complicated, difficult to memorise the password/password code, mobile phone OTP is not realtime (instant) when oversea.
YES	YES	KNEW	PASSWORD	OK	Security is iffy, the bank's policies assume no one is going to try to spoof them.
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL

YES	YES	DID NOT KNOW	PASSWORD	OK	I like this service. It has always concerned me how easy it is to buy items online. I wish that this was used everywhere.
YES	NO	DID NOT KNOW	PASSWORD	NULL	NULL
YES	YES	KNEW	PASSWORD	NOT OK	Confusing to customer
YES	YES	NOT SURE	PASSWORD	OK	Knowing a bit about this. Its really a scheme to protect the merchant not the customer. Does it help cut fraud, well yes as its more information someone has to gain and fraudsters like an easy target
YES	YES	KNEW	PASSWORD	OK	NULL
YES	NO	NOT SURE	NULL	NULL	Don't buy online except for plane tickets.
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	OTP SMS	OK	I'm less happy receiving codes OTA (over the air) to my cellphone since the recent demonstrations of how easy it is to hack cellphone communications (reduced to script kiddie level now) due to the weaknesses in a5/1
YES	NO	NOT SURE	OTP SMS	OK	NULL
NO	NO	DID NOT KNOW	NULL	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	Password scheme too fussy
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	Make the process of 3DSecure seamless for the end user...
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	it is extra security level, I would encourage it.
YES	YES	KNEW	PASSWORD	NOT OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	A pin in the b@d
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	NO	DID NOT KNOW	NULL	NULL	I just use MBNET (Virtual Credit Cards with limited lifetime and value).
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	Its been a long time since I did it – but I have a vague recollection that the VbV password reset process used was very weak. (that might be deperent on the bank rather than the scheme)
YES	NO	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
NO	NO	NULL	NULL	NULL	NULL
YES	YES	NOT SURE	READER OR TOKEN	NOT OK	NULL

YES	YES	KNEW	PASSWORD	OK	I think theMC solutionis the one use topay for downloads from HNV
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	FAILED	DID NOT KNOW	PASSWORD	NOT OK	Well, paying by creditcard but still having to use a password or other verification methods nullifies the idea of paying with creditcard.
YES	YES	NOT SURE	PASSWORD	NOT OK	I never remember the password, and therefore have to reset it every time, making it very annoying.
YES	YES	NOT SURE	PASSWORD	NOT OK	It wasn't integrated well with the web site. I think I cancelled the purchase. I don't want to use it again.
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	I think the process varies wildly from website to website. Also as an e-commerce retailer, I find customer awareness really low. And we haven't implemented it. As a customer, there's been no communication introducing me to the scheme. Overall, I think it's a shambles.
YES	YES	KNEW	PASSWORD	NOT OK	Horrible to use, especially on a mobile browser
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	NOT OK	I turn it off at every given opportunity. What I lose in revenue in chargebacks is miniscule in comparison to what I would lose by having them active in my checkout.
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	Incredibly frustrating. Doesn't update (welcome message) and doesn't recognise password. Password restrictions (7–10 letters) too restrictive for people to remember don't character limit.
NO	NO	DID NOT KNOW	PASSWORD	NOT OK	I have no idea what these are.
YES	YES	DID NOT KNOW	PASSWORD	OK	None really other than it seemed to take a few frustrating tel calls to get a new card enrolled, as online registration didn't work properly.
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	can be a real pain if you have a joint account. partner and you have to agree on password, and both remember it and not reset it without telling partner
YES	FAILED	DID NOT KNOW	NULL	NOT OK	I refuse to make purchases with these systems. Banks aren't interested in user experience the way merchants are. Being redirected to a website you weren't expecting – and which isn't your own bank – is a terrible experience. And I'm no more protected with these systems either.
YES	YES	NOT SURE	PASSWORD	NOT OK	generally poorly implemented by

					everyone. BTW. I even worked with Mastercard on their mobile version and they didn't seem 100% on how to make it good.
YES	YES	KNEW	PASSWORD	OK	No, my experiences are good.
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	I wish the experience could be more integrated into the checkout process so that it doesn't break the workflow. I guess that's partially the vendor's fault though.
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	I HATE Verified by Visa – it's an unwanted speedbump and a distraction from my goal of shopping/paying for things online.
YES	YES	KNEW	PASSWORD	NOT OK	Verified by Visa on my Lloyds TSB account has pathetic password requirements: eg, only alphanumeric characters. My facebook account has a more secure password. Given this is my financial security at stake, I'm pretty angry about this easily-fixable problem.
YES	YES	DID NOT KNOW	PASSWORD	OK	Having used Verified by Visa with password authentication I did get the impression that the overall security of the transaction increased. However, having to remember yet another password doesn't seem very efficient. I would much prefer one OTP or smart card device to be used for credit card transactions.
YES	YES	NOT SURE	OTP SMS	OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	It's a bit of hassle, but I appreciate why it's there. One thing I always think, is that it seems very easy to reset the password, and I've always wondered if it's too easy.
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	NO	DID NOT KNOW	PASSWORD	NOT OK	These verified scenarios are a complete pain. I understand that it's more secure, and it's generally a good idea, but it makes the process so painful that I would just refuse to use a site that requires it. Nowadays, I just use my Amex for most everything, and let them monitor and catch fraud on the other end, it's much more convenient and just as secure.
YES	YES	KNEW	PASSWORD	OK	NULL
YES	NO	NULL	NULL	NULL	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	NOT OK	Integration feels awkward, unpleasant and almost like someone has hijacked my buying process. First experience with Verified by Visa almost felt like a

					phishing scheme. They really, REALLY need to improve their user experience.
NO	NO	DID NOT KNOW	NULL	NULL	NULL
YES	FAILED	DID NOT KNOW	NULL	NULL	NULL
YES	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	NOT SURE	READER OR TOKEN	OK	Impractical for corporate credit cards where a token is not available.
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	does it really make the transaction more secure?
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	I've always had problems with the Visa one because it's used so infrequently that I can't remember the password, which has to be complicated and can't be one which you've used before.
YES	NO	NOT SURE	PASSWORD	NOT OK	Have never used it, didn't seem worth the additional headaches.
YES	YES	NOT SURE	PASSWORD	NOT OK	I think credit cards and their verification system is basically broken. You can reset 3-D secure using basic details and an email account, this renders it useless. I don't understand why credit card payment essentially boils down to giving the code to your vault to a 3rd party and trusting they will only take out the amount of money agreed. You also trust they won't give it to anyone else. It would be better if the physical card was used to generate some form of digital signature to verify an agreed transaction.
YES	YES	KNEW	PASSWORD	OK	NULL
YES	NO	NOT SURE	PASSWORD	NOT OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	NOT SURE	PASSWORD	NOT OK	Terrible. Never remember my password always have to get reminder. Ruins shopping
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	I keep forgetting my passwords, but the refresh process is easy. I think these schemes are a reasonable compromise between alternatives (SET) and nothing at all!!
YES	NO	NOT SURE	PASSWORD	NOT OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	Doesn't seem particularly helpful (i.e. doesn't increase my assurance of the security of the checkout process)
YES	YES	NOT SURE	PASSWORD	NOT OK	I dislike it and everyone I know dislikes it. That includes users and implementors :)

YES	YES	NOT SURE	OTP SMS	OK	NULL
YES	YES	NOT SURE	OTP SMS	OK	NULL
YES	YES	NOT SURE	OTP SMS	OK	NULL
YES	YES	NOT SURE	OTP SMS	OK	NULL
YES	YES	NOT SURE	OTP SMS	OK	Nope
YES	YES	NOT SURE	OTP SMS	OK	Nope
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	no
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	KNEW	PASSWORD	NOT OK	I was somehow suprised, and a little bit afraid on the upcoming security dialog first time I saw it. I was just shopping on a known online shop whereas this form just broke my well known experience for this particular shop.
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	Implementation was clumsy. Think it was like tigerdirect.
YES	YES	KNEW	PASSWORD	NOT OK	Too much of a barrier to a smooth checkout. Implementations tend to be clunky and slow. Always approach the experience with dread. Do not feel it offers me any significant additional security.
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	I hate Verified by Visa...slows me down and one more thing to remember.
YES	YES	NULL	PASSWORD	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	its better to have a token than a regular password.
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	KNEW	PASSWORD	NOT OK	A disposable one time virtual Visa card number derived from the parent one would be a more workable solution.
NO	NO	NOT SURE	NULL	NULL	NULL
NO	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	KNEW	PASSWORD	NOT OK	Lack of universal adoption makes this useless.
YES	YES	KNEW	PASSWORD	OK	NULL
YES	FAILED	NOT SURE	NULL	NOT OK	NULL
YES	YES	KNEW	OTP SMS	OK	NULL
NO	NO	DID NOT KNOW	PASSWORD	NOT OK	good
NO	NO	DID NOT KNOW	NULL	NULL	NULL
NO	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
NO	NO	DID NOT KNOW	PASSWORD	NULL	NULL
YES	YES	KNEW	PASSWORD	NOT OK	NULL
NO	FAILED	NOT SURE	NULL	OK	NULL

YES	YES	KNEW	PASSWORD	OK	Good in principle. I find that it is so rarely used, I have to look up my password each time.
YES	YES	KNEW	NULL	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	NO	DID NOT KNOW	NULL	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
NO	NO	NULL	NULL	NULL	NULL
NO	NO	NOT SURE	NULL	NULL	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
NO	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	KNEW	READER OR TOKEN	NOT OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	* seems to break, especially if I'm using noscript, so purchases don't go through. * I'm never quite sure if I should re-send a transaction if it pauses for ages. Don't want to pay twice. * hate embedding another site in a frame. * it makes me feel nervous about security – but I don't really know why. Maybe because I'm not sure where I'm being redirected to (no URL in address bar, or HTTPS info in browser?)
YES	YES	NOT SURE	NULL	NULL	NULL
YES	YES	KNEW	PASSWORD	OK	I normally integrate using the help of the payment provider. I have only integrated through XML once and it was unnecessarily difficult. Would be nice to have better documentation for verified by visa/3D secure.
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	OTP SMS	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	NO	NOT SURE	NULL	NULL	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	It's badly, badly designed.
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	KNEW	OTP SMS	OK	NULL
YES	FAILED	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	Notes 1. Sometimes the transaction is refused for no apparent reason. 2. Sometimes the transaction claims to be covered by VfV or MC SC, but no actual authentication is subsequently performed.

YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	NOT SURE	PASSWORD	OK	MasterCard SecureCode doesn't integrate nicely with the visual aspect of a website, but it's great service, never have any complaints...
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	Use of these services should be mandatory – sites like Amazon really should implement more secure payment processing methods. Similarly, standards for security before and after 3-D Secure, VbV and MCSC should be set – sites like 24studio.co.uk have "holes" that can allow security breaches.
YES	YES	DID NOT KNOW	PASSWORD	OK	No
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	eCommerce sites need to be sensitive to how long the enrollment process can take people (session related issues) and also warn if quick selling stock is not allocated until after payment.
YES	YES	DID NOT KNOW	OTP SMS	OK	I have been stuck sometimes when the bank, without my knowledge, changed my credit card They called it 'upgrading', though I don't remember asking for it and the VbV then failed whilst I was abroad.
YES	FAILED	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	NOT SURE	PASSWORD	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	Terrible service. Can never remember my password, is a real blocker to purchasing.
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	It was a bitch to use first time but now i'm used to it, it's fine
YES	YES	KNEW	OTP SMS	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	Looks like a phishing site. It's v annoying.
NO	FAILED	NOT SURE	NULL	NOT OK	NULL
YES	YES	KNEW	PASSWORD	OK	I experienced this (Verified by Visa) when I lived in the UK (I left in Dec 2008). I live in the US now and I have not experienced this here with my new credit card. You would expect the VISA brand to be the same everywhere and the push for security to be uniform across the continents. In my opinion credit card security is very lax here. My husband and I share our cards all the time. We use

					them in stores, restaurants etc and no one ever questions this – even when the signature is different. Leticia
YES	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	NOT SURE	PASSWORD	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
NO	NO	NOT SURE	NULL	NULL	NULL
NO	NO	NOT SURE	NULL	NULL	NULL
NO	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	KNEW	PASSWORD	NOT OK	I don't trust it. It is badly put together. It is often badly integrated into websites. It frequently breaks leaving me to phone my bank to find out if funds were actually taken or not. And on a mobile phone (I've tried on iPhone and Android 2.1/2.2) and it is even less stable on those platforms.
YES	YES	NOT SURE	PASSWORD	NOT OK	VbV sucks! I hate it, I don't know anyone who likes it!
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	Generally think it makes online purchases more secure. As Craig pointed out with so many sites now using it, it seems crazy that Amazon aren't
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	NOT SURE	PASSWORD	NOT OK	To easy to potentially fake a page and phish a password from me.
YES	NO	NOT SURE	NULL	NULL	NULL
YES	YES	KNEW	PASSWORD	OK	Very pleased with the service.
YES	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	KNEW	PASSWORD	NOT OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	To avoid finding out after I have committed to purchase that I need to use one of these systems, it would be better to be told during the checkout process. I think it should be mandatory to state during the checkout that "payments will be validated by 3-D SECURE, VERIFIED BY VISA or MasterCard SecureCode" Etc..
YES	YES	KNEW	PASSWORD	OK	Better than the non–security on AMEX cards (mine has been cloned online twice now) but laughably insecure due to only needing to know my DOB to bypass it – more companies should be using smart card readers or SMS validation rather than simple password.
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL

YES	YES	DID NOT KNOW	PASSWORD	NOT OK	Always concerns me, looks like a doggy site wanting you banking password.
NO	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	NOT SURE	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	KNEW	PASSWORD	OK	NULL
YES	YES	DID NOT KNOW	PASSWORD	OK	NULL
YES	FAILED	DID NOT KNOW	NULL	NOT OK	Poorly implemented. Adds no security to process. Terms and conditions reduce the rights of the cardholder, signup sites for both of my cards look like phishing.
NO	NO	DID NOT KNOW	NULL	NULL	NULL
YES	YES	DID NOT KNOW	PASSWORD	NOT OK	Just adding another stage of authentication by password is not a smart ID solution and invariably leads to a denial of service