GPayments
Innovate - Empower - Adapt

Authentication and Payment Solutions

Authentication

The missing element in online payment security

At a glance

This paper outlines the need for increased security, integrity and authenticity in online transactions. It briefly covers the existing standard of performing online transactions using the SSL protocol and highlights some of the shortcomings of this method. It revisits the first attempts to introduce authentication into online payments using the SET protocol and 3-D SET implementations. The focus of the paper is the new generation of authentication standards introduced in 2001 - Visa's 3-D Secure, MasterCard's Secure Payment Application (SPA) and Maestro's Online Debit Solution (SPA) - which have been designed to introduce consumer confidence while reducing fraud and chargebacks in online payment transactions. The high level operation of these new models is detailed with a brief comparative analysis.

GPayments Pty Ltd
Pittwater Business Park
Suite 8, 5 Vuko Place
Warriewood NSW 2102 Australia

Telephone: +612 9913 3088
Facsimile: +612 9913 3077
Email: info@gpayments.com
Website: www.gpayments.com

Authentication

Background

The rise of the Internet as an efficient and global communications medium opened the possibility of purchasing goods and services online. The growth in Internet usage has expanded at an exponential rate and is expected to continue for the foreseeable future. This will lead to an increase in online transactions, which are the basis for electronic commerce. As these online transactions increase further pressure will be applied to payment systems which must facilitate global business in multiple currencies across different timezones. Without payment there is no business - without ePayment there is no e-business.

Fundamental Principles

Regardless of the type of payment system the seller and buyer rely on some fundamental principles:

> **Trust.** The parties to the transaction must trust each other. The buyer must believe that the seller is legitimate and will actually deliver the goods. The buyer must believe that the goods are as represented and actually worth the price. The seller must believe that the buyer is legitimate and will provide valuable payment in exchange for the goods.
>
> **Security.** The parties need a secure environment in which to conduct the transaction. In an online payment transaction, the buyer and seller want to protect the details of the order and payment. The buyer wants to be certain that his or her account information is not stolen so that it can be inappropriately used to steal value.[1]

When people talk about payment security in electronic commerce they are really confusing a number of issues. Security, in general terms, can be broken down into:

> **Confidentiality**, in storing a payment instruction safely on a system that is connected to the Internet,
>
> **Integrity**, which is the ability to securely transmit a payment instruction from one location to another, and
>
> **Authenticity**, which is the ability to effectively verify the parties to a transaction.

When it came to making purchases over the Internet consumers immediately reached for their credit card – the same mechanism that they had used time and time again in the physical world. In the physical world when you pay with your credit card at a store your credit card provides both a means of authentication and payment. In addition to having possession of the actual credit card you provide a signature which can be compared to the signature on the back of the card. Following this authentication process the payment is made.

The rise of the Internet has lead to an increase in 'Card not present' transactions where this authentication process does not occur. While not originally designed for the Internet

[1] An Introduction to Secure Electronic Transactions April 1998 Tower Group

"Payment cards have emerged as the natural currency of the Internet and are used in over 95 per cent of on-line transactions."[2]

In today's on-line shopping environment, payment instructions containing account information are often transmitted from cardholders to merchants over open networks with no authentication. "This account information provides the key elements needed to create counterfeit cards and/or fraudulent transactions. While it is possible to obtain account information in other environments, there is a heightened concern about the ease of doing so with public network transactions. This concern reflects the potential for high-volume fraud, automated fraud (such as using filters on all messages passing over a network to extract all payment card account numbers from a data stream), and the potential for "mischievous fraud" that appears to be characteristic of some hackers."[3] In particular the Internet provides the ability for hackers to perform computerized fraud using "brute force" techniques, which were not possible, when fraud had to be laboriously performed by hand. This poses an acute problem with the rise of digital goods distribution as the incidence of payment and receipt of the goods has converged. The problem has also been exacerbated by the rise of a multitude of internet-enabled devices such as PC's, Personal Digital Assistants, wireless phones and set top boxes. It is now possible to make payments from any of these devices and these devices are predicted to become the most common access points to the Internet.

It is necessary to realize that eCommerce will continue to grow and expand regardless of the security measures involved. However, there are a number of requirements for secure eCommerce that should be introduced by the relevant organizations, which include financial institutions, card associations and merchants:

Confidentiality of payment instructions during storage

Integrity of payment instructions during transmission

Payer Authentication to increase trust between parties interacting in a virtual space

Transaction Authentication to secure a number of individual payments made during split shipments or recurring transactions

Device-Independence to support any Internet access point allowing consumers to "buy anywhere and anytime"

Interoperability to support global businesses engaging in cross-border transactions

Accountability to provide a secure audit trail which can be used as evidence in any possible dispute

While technology is responsible for driving the eCommerce revolution it must be remembered that technology itself is not a panacea. A technology solution, which addresses the issue of secure payment and authentication, must address a distinct set of requirements which are focused on solving the needs of buyers, sellers and financial institutions. These are outlined as follows:

- Fast and simple implementation by banks, merchants and customers
- Ability to leverage existing infrastructure where possible
- Seamless operation and synchronisation across multiple Internet payment devices
- Authentication of all parties to a transaction

[2] Visa Secure E-Commerce Initiative Fact Sheet, Visa EU
3 SET Secure Electronic Transaction Specification Book 1: Business Description
May 31, 1997

- Multiple encryption options based upon regional availability and requirements
- Reduction of the technology burden on buyers and sellers
- Support for future payment and authentication methods
- Reduction of the incidence of fraud and chargebacks
- Reduction in consumer and merchant fear

The major drawback with online payments is that the vast majority are not authenticated which has increased the incidence of fraud. The consumer is subject to fraud if the merchant misuses the consumer's account information or if the merchant's website is hacked. The merchant is subject to fraud where stolen card numbers are used to make purchases and the merchant is unable to receive payment for these purchases. In all card not present circumstances today it is the Merchant/Acquirer side of the business that bears the cost of fraudulent transactions and the consumer who must endure a cumbersome process for rectification. Gartner Group research indicates that online credit card payments incur twelve times more fraud than offline payments. This lack of authentication in online payment transactions has previously made the possibility of online debit payments untenable.

To add further complexity to the situation different geographical regions may require different levels of security based upon infrastructure, policies and regulations. An example is that merchants clearing credit card transactions in the U.S. market are able to check further information from the consumer than just the credit card number and expiry date using the Address Verification System. The ability to compare customer address information lessens the need for higher levels of authentication in the payment process.

It is in this context that we will now examine the existing methods of payment in eCommerce. This is not intended as an exhaustive analysis of existing eCommerce payment methods but rather as a brief overview of the strengths and weaknesses of certain approaches. This will provide a background for the introduction of Visa's 3-D Secure, MasterCard's SPA and Maestro's Online Debit solution, which are the online authentication standards which have been released in 2001.

A Brief History

The following is a summary of the secure online payments systems and their relative success in the market to date.

Secure Sockets Layer (SSL)

The use of SSL (secure sockets layer) provides the mechanism to securely transmit a credit card from one location to another with transactional integrity. This does not reduce intentional fraud by either the cardholder or the merchant but does protect the credit card number from hackers during transmission across the web.

SSL requires the installation of X.509 certificates from a trusted third party certificate authority on the merchant's webserver. Once this is installed the customer's browser is able to enter a secure session with the merchant's webserver and all communication over the channel is encrypted at 128 bits.

To put this in the context of a real world example

> "A SSL session, as used today, is the equivalent of using a scrambler on the telephone line to the catalog merchant." [4]

When this data arrives at the merchant's web site, all the information is decrypted and is accessible by the merchant. *The responsibility for security in storage of this information rests exclusively with the merchant*.

"The purchaser:

- Has to trust that the merchant will guard their credit card information securely and the purchaser is assuming a risk in so doing
- Has no assurance that the merchant is authorized to accept credit card payment.

In an on-line transaction the merchant also suffers a security risk, as with any mail-order or telephone-order transaction today, because he has no proof that the user is the true owner of the credit card. This is a risk that the merchant and the credit card vendor assume and factor in to their cost of doing business. This risk increases with the purchase of "soft goods", intellectual property (software, games, etc.) where the purchase is actually delivered on-line as well as being ordered on-line." [5]

In an SSL environment merchants can send payments to a payment gateway using an API model or a URL model. In an API model the merchants embed software modules in their websites which are responsible for communicating information with the acquirer's payment gateway. In an API model the merchants are responsible for building customized shopping carts for the consumer and retain the cardholder's details in a database on their own site.

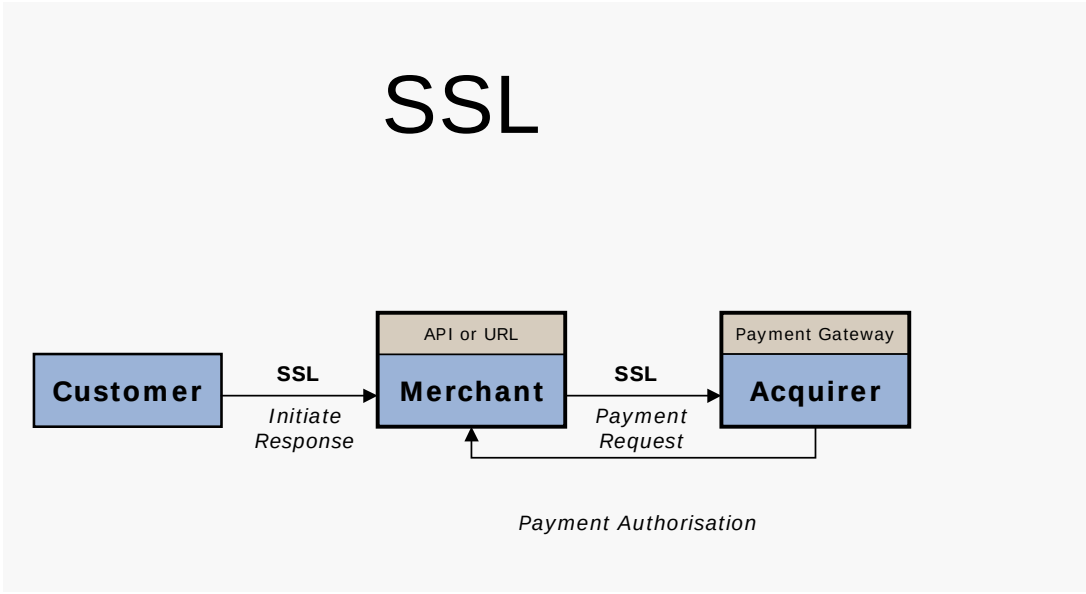
In a URL model the merchant does not embed any software in his website but instead embeds hyperlinks for each product into web pages. When a consumer clicks on one of these hyperlinks they are redirected to a payment server hosted by an acquiring institution. This payment server is responsible for providing a virtual shopping cart to the consumer.

A URL model can be employed in an SSL environment to prevent storage of cardholder details at the merchants website. This provides greater security to the consumer in that the merchant website does not store the credit card details which can then be hacked or misused. However, it does not address the issue of chargebacks from the merchant's side,

[4] SET Comparative Performance Analysis, November 2, 1998 Chris le Tocq, Steve Young, Gartner Consulting
[5] SET Comparative Performance Analysis, November 2, 1998 Chris le Tocq, Steve Young, Gartner Consulting

as the user is not authenticated in the process. This model has not been that popular with merchants who generally want to capture the client information and control the shopping cart process with the customer. In many cases individual sites have created client “wallets” in an attempt to improve customer loyalty.

SSL provides integrity and security in transferring information between the buyer and the seller but does not provide any intrinsic authentication capabilities for the customer or the merchant. Compromising the integrity of transactions during transit is a negligible problem when compared to the problems of fraudulent cardholders, fraudulent merchants and loss of data from merchant websites. Nevertheless, due to the ease of implementation SSL has gained widespread acceptance and is used for the vast majority of online purchasing today.



SET – Secure Electronic Transaction

Secure Electronic Transaction (SET) was developed by VISA and MasterCard in 1996 to add confidence to payment card transactions over the Internet. SET is a certificate-based system that utilizes digital signatures to replace the “handwritten signature” used for authentication in the physical world.

SET provides both transactional integrity and confidentiality during transmission of credit card details over the Internet. A more secure technology than SSL, “SET (Secure Electronic Transaction), not only encrypts the transaction but can ensure against fake identity"[6] as it authenticates both the cardholder and a merchant in a transaction. This authentication is achieved through the use of digital certificates, which are issued by a Certificate Authority (which may be a trusted third party) on behalf of the card-issuer. If the Certificate Authority has stringent procedures for issuing digital certificates and a SET transaction is entered into merchants are provided with the ability to pass on the liability for any fraud or chargebacks to the card-issuer. This “non-repudiation” means that the merchant can be sure that the purchaser cannot deny that they entered into the transaction. In the SET environment the merchant is also authenticated as a bona fide merchant with an acquiring institution reducing the chance of misuse of credit card details submitted by the consumer.

SET in its original incarnation was too complex requiring cardholder software and digital certificates being installed on the customers PC and major implementation issues for merchants. Issuers and acquirers were required to distribute software and manage the issuing and re-issuing of digital certificates. Due to the easier process of implementation the market adopted Secure Sockets layer (SSL)

Other weaknesses of SET were with small payments under $10 where the process of authorization and funds capture was too expensive. Portability was another problem, as the customers were required to hold a digital certificate (public key pair) on their computer. This meant they were restricted to purchasing from one computer. The rise of Internet-enabled devices made this approach redundant, as these devices, in some cases, were unable to carry the required SET certificates. SET introduced onerous certificate management and maintenance issues that were very costly for issuers and acquirers to manage.

The original objectives of SET in the Secure Electronic Transaction Specification book were to:

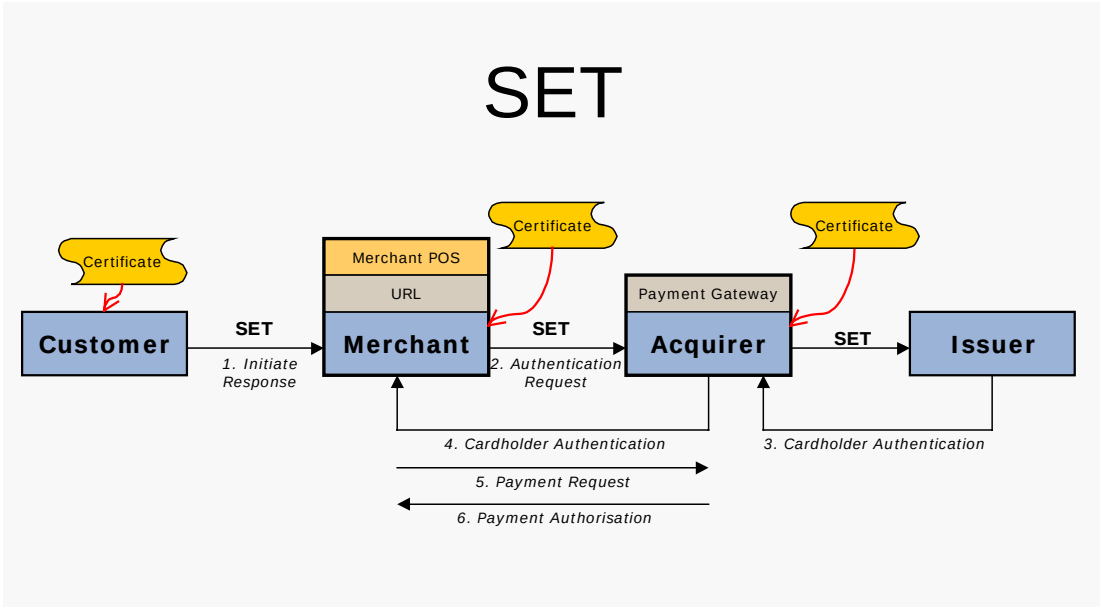
- achieve global acceptance via ease of implementation and minimal impact on merchant and cardholder end users
- allow for “bolt-on” implementation of the payment protocol to existing client applications
- minimize change to the relationship between acquirers and merchants, and cardholders and issuers
- allow for minimal impact to existing merchant, acquirer, and payment system applications and infrastructure, and provide a protocol that will be efficient for financial institutions.[7]

When held to these original objectives SET has struggled to deliver on its promises. Even as far back as 1998 there was skepticism as to the acceptance of SET by research analysts:

6 February 7, 2000, Loosen Up Rules to Boost E-Commerce, Singapore Business Times, Toh Han Shih
7 SET Secure Electronic Transaction Specification Book 1: Business Description May 31, 1997

> "Although SET is technically successful (or can be made so, with reasonable effort), the Tower Group believes that SET will have difficulty demonstrating that it offers sufficient additional value to consumers, merchants, and institutions to induce them to buy and install SET software.[8]

When eCommerce exploded onto the scene merchants were more concerned with generating volume and relied on the easier to implement SSL protocol for integrity.



8 An Introduction to Secure Electronic Transactions April 1998 Tower Group

3-D SET (Server-based SET)

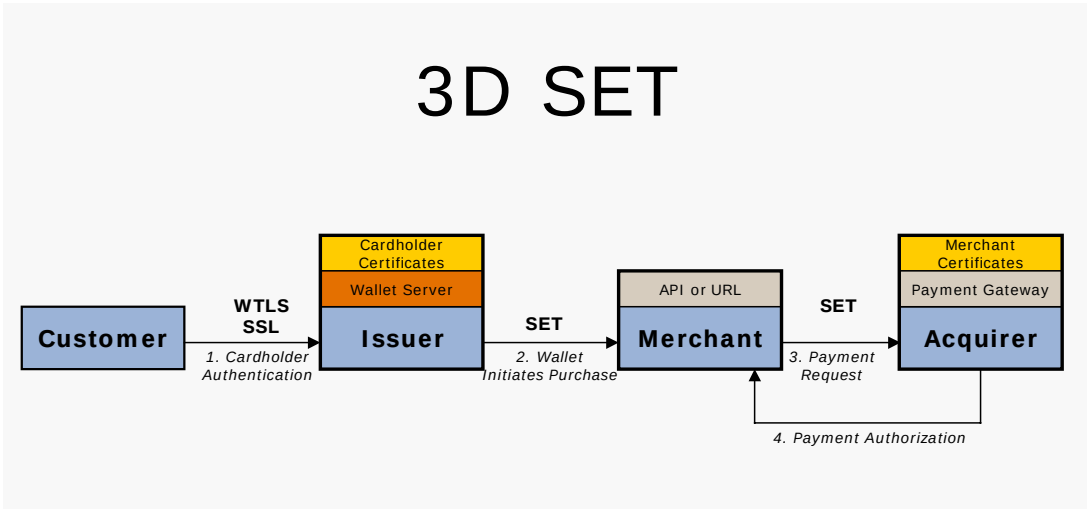
Following the resistance to the acceptance of SET in the market a number of SET vendors decided to develop server-based implementations of SET. The server-based SET model reduces the technology which has to be deployed at the merchant and customer by only requiring 'thin' modules for merchants and 'slim' digital wallets for consumers.

Server-based SET does not store certificates at the customer device level, which opens the possibility of making SET transactions from Internet devices such as Personal Digital Assistants, Wireless Phones and set top boxes. Due to the inability for these devices to hold digital certificates it is necessary to use native security mechanisms such as SSL and WTSL for connection between these devices and a secure server responsible for holding digital certificates. The system used to manage this device-independent authentication and payment system must then be integrated with the server-based SET system.

Server-based SET, like any certificate based system, has a number of limitations in that it only caters for certificates issued by one certificate authority. This means that customers cannot use the same certificates issued from their e-banking sites or other issuers using different certificate authorities. Most customers have multiple cards from different issuers and do not want multiple digital wallets and multiple certificates. This continued to be a major impediment to the adoption of server-based SET.

Server-based SET compromises the benefit of certificate-based authentication for ease of use and freedom of access. In a client-based SET environment unauthorized access requires access to a physical device where the certificate is held. In a server-based SET environment, unauthorized access can be achieved from any Internet access device provided that a username and password are known. This actually makes the use of a digital certificate for the cardholder in server-based SET redundant.

However, the major failing of server-based SET is that it has not been interoperable with SSL websites, which are now responsible for the vast majority of eCommerce transactions. In particular merchants have been reluctant to default to SET payments and as such have provided an optional "SET button" which requires the cardholder to actively select the more secure method. Neither SET nor 3-D SET has ever gained widespread adoption and the credit card companies responsible for its introduction have now superceded it with new authentication protocols.



Visa's 3-D Secure

Visa's 3-D or Three Domain model is not a payment and authentication method or a technology implementation. It is actually a model that isolates the responsibilities of different parties within the transaction continuum. Basically speaking it identifies that card issuers have a close relationship with cardholders and merchants have a close relationship with acquirers. It also acknowledges that communication between issuers/cardholders and merchants/acquirers must occur during the course of any transaction.

The three domains referred to are:

Issuer Domain – cardholders and their bank

Acquirer Domain – merchants and their bank

Interoperability Domain – communication between issuing and acquiring organisations and Visa's infrastructure

"The Three Domain model requires banks to be capable of providing their cardholders and merchants authentication technology, but gives them a choice in selecting their preferred technology. This is made possible through an extremely flexible framework, which can embrace a variety of technical approaches."[9]

The 3-D Model was first introduced to describe server-based SET as 3-D SET. However, in reality the description of server-based SET as 3-D SET was really an issue of re-branding rather than a change in technology. 3-D was also used to describe a new version of SSL, which included payer authentication. This was originally called 3-D-SSL but has since developed into the 3-D-Secure specification.

> "*Visa is developing authenticated payment capabilities to improve transaction performance online and to accelerate the growth of electronic commerce. The objectives are to create a virtual "card present" environment online, move towards guaranteed payments, and improve transaction performance to benefit all participants. 3-D Secure is the next step in the evolution of 3-D SSL. Upon its completion, 3-D Secure will become the base standard that Visa member banks will be required to support, the singular, globally interoperable solution. Issuers and Acquirers will have the option to implement solutions in addition to 3-D Secure, but 3-D Secure will be the minimum requirement."*[10]

3-D Secure is an authenticated payment environment that requires the cardholder's issuer to be participating, the merchant to be participating and the cardholder to have registered for the process with their issuer. Under 3-D Secure there is a minimum requirement for customers to enter a username and password in the online payment process in order to verify themselves as the true owner of the credit card number they are using. Issuers have the option of authenticating users using other methods such as an e-banking authentication method, a chip card or using certificates. However, username and password is the simplest for the issuer to implement and is expected to become the most common form of authentication for credit card transactions. This promises to introduce a level of security for online credit card transactions similar to current Internet banking procedures.

In the "Issuer domain" the issuer is responsible for deploying an issuer system comprised of enrollment, receipt and access control server modules (functionally equivalent to a wallet server). The issuer system also handles communication with the 3-D Secure merchant plug-ins and a centralized Visa directory which acts as a communications intermediary between merchants and issuers. The issuer system handles all interactions with the

9 Visa Secure E-Commerce Initiative Fact Sheet, Visa EU torbits@visa.com
10 3-D Secure business requirements

customer at multiple Internet access points, which support a browser. The software deployed by the issuers needs to be integrated with their backend card systems providing access to cardholder information.

In the Acquirer domain acquirers are responsible for deploying a payment gateway and merchants install payment gateway plug-ins in exactly the same way as a typical SSL environment. Under 3-D Secure the merchant also needs to install a 3-D Secure Merchant plug-in (MPI) to handle communication with the centralized Visa directory and the customer's credit card issuer. The software implemented by each merchant needs to be integrated with their shopping cart system.

3-D Secure has minimized the requirements for cardholders mandating that they only need a browser to participate. Downloadable client software for cardholders, such as electronic wallets, is required for payments using smart cards. Electronic wallets, while not a prerequisite, can be integrated with 3-D Secure to improve the security, payment process and provide value-added services such as single login and form-filling.

3-D Secure only authenticates the customer to the merchant and does not mandate merchant authentication to the customer which makes it simpler than SET. 3-D Secure has also removed another prerequisite of SET in that it allows the merchant to store the credit card number on the merchant's server. 3-D Secure still relies on certificates, which are used by issuers and merchants. The major problem of requiring certificates for cardholders, which was the Achilles Heel for SET, has been removed.

3-D Secure introduces a large number of new messages, which have to be sent over the Internet in order to effect a transaction. 3-D Secure pilots indicate that the addition of 3-D Secure adds 10-15 seconds to the entire payment process for the customer. The large 3-D Secure XML message size originally designed with a web browser in mind created a problem for mobile Internet devices such as WAP handsets with low memory capacity. In order to address this problem 3-D Secure has introduced a second set of condensed messages for payments made from Internet-enabled devices such as mobile phones and PDA's.

In summary, the 3-D Secure model provides a workable solution to cardholder authentication which should reduce the incidence of fraud and chargeback. The security model of 3-D Secure will need to be improved to address its current vulnerability to "man-in-the-middle" attacks, which may expose the cardholder's username and password. The 3-D Secure user experience can also be improved as under the current model it requires the user to authenticate themselves for every purchase they make at different shopping sites within a single shopping session. This can be addressed by optional plug-in solutions, which only make one authentication procedure necessary.

3-D Secure requires issuers and merchants to deploy and integrate additional software in order to participate, which will require a concerted effort. However, a number of lessons have been learnt from the failure of SET and 3-D Secure is on the whole a simpler system, which should gain a higher level of acceptance in the marketplace.

3-D Secure Payment Process

1) **Customer enters details at merchant website**

2) **Merchant 3-D Secure plug-in connects to the centralized Visa Directory service to determine the network location of the issuer's server**

3) **Visa Directory validates card number participation with the Issuer**

4) **Issuer confirms card number participation in 3-D Secure**

5) **The Visa Directory service sends the Internet location of the issuer's server to the merchant plug-in**

6) **The merchant's 3-D Secure plug-in re-directs the customer to the issuer server and provides the issuer server with the transaction details**

7) **The issuer's server displays a transaction confirmation screen to the user by opening another browser window and requesting a PIN number/password**

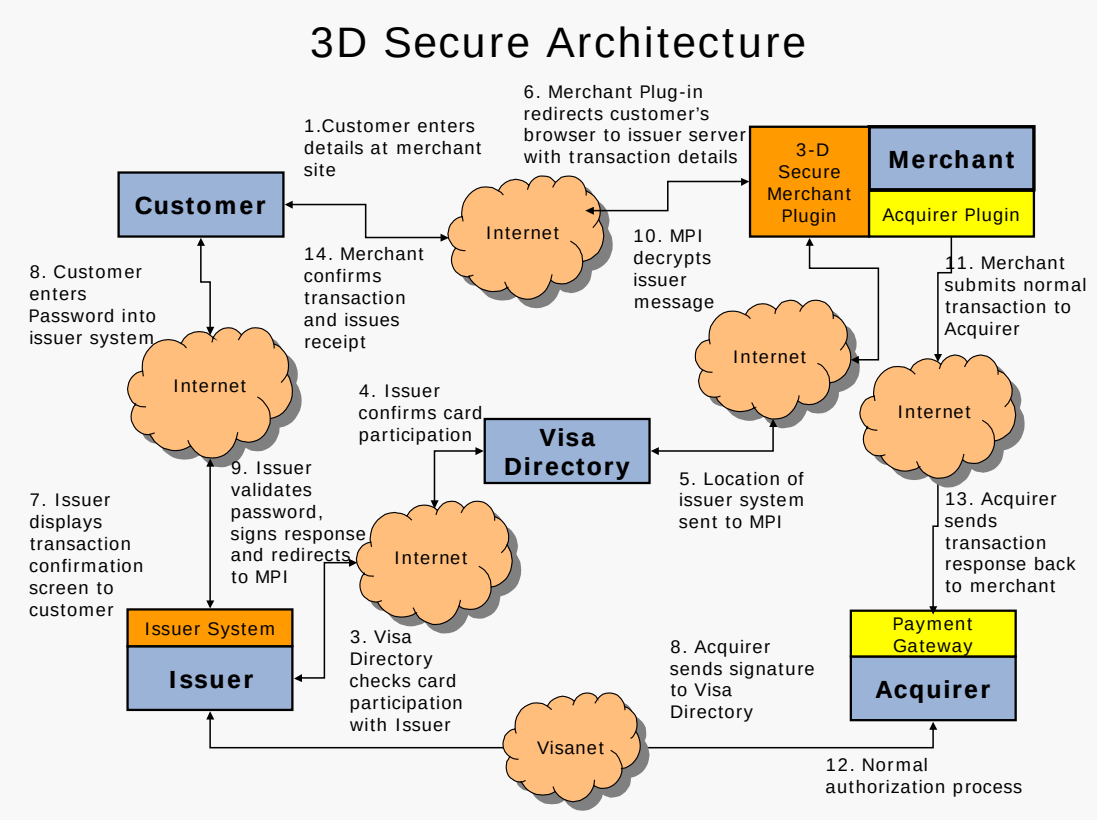
8) **The customer enters their PIN/password into this confirmation screen**

9) **The issuer's server validates the PIN/password and digitally signs the payment response**

10) **The issuer redirects the customer's browser to the 3-D Secure merchant plug-in and provides the payment response**

11) **The merchant's plug-in decrypts the payment message and extracts the status of the transaction**

12) **If the status is OK, the merchant proceeds with the normal payment authorization process**



MasterCard's Secure Payment Application (SPA)

> *"SPA is a MasterCard security solution for securing payments between Merchant and Issuer for card not present transactions via the Internet. With electronic commerce accounting for an increasing share of MasterCard and member GDV (Gross Dollar Volume), it is important to ensure that the channel is positioned to grow GDV profitably through use of security solutions designed to provide for Cardholder authentication."*[11]

SPA is an authenticated payment environment, which requires the cardholder's issuer to be participating, the merchant to be participating and the cardholder to download a client side plug-in (or a wallet application) from their issuer. Under SPA the credit card issuer is also given the flexibility of determining a suitable authentication method for their cardholders. Issuers have the option of authenticating users using SPA (username and password), biometrics, smart cards, or digital certificates. However, username and password is the simplest for the issuer to implement and is expected to become the most common form of authentication.

The issuer is required to implement a SPA compliant wallet server, which needs to be integrated with their back-end card systems providing access to cardholder information. The issuer must provide a registration process for this wallet server and distribute SPA compliant plug-ins (or electronic wallets) to their cardholders. The SPA wallet server is responsible for generating the transaction-specific security tokens, which are passed to the merchant, on to the acquirer and finally back to the issuer for transaction matching. MasterCard has decided to upgrade its proprietary Banknet as the communications backbone for this security token known as an Accountholder Authentication Value (AAV). In contrast, Visa are deploying an Internet-based Visa Directory Service and leaving Visanet untouched.

Payment Acquirers need to patch their existing payment gateways in order to accept the transaction-specific security tokens and then pass these to a new transaction field being added to MasterCard's Banknet. This will also require merchants to install a new payment gateway plug-in, which supports the passing of the security token via an extra parameter. This is a minor upgrade to the current SSL process.

The merchant will also need to upgrade their shopping cart system to carry hidden fields that hold transaction-specific information, which can be read by SPA-enabled wallets. The merchant has the option of providing a transaction reference number to the customer's SPA plug-in (or electronic wallet), which can be checked once the security token is received from the SPA wallet. This can provide extra protection against "man-in-the-middle" attacks by ensuring that the original customer is still the transactor and has not been replaced by a fraudulent imposter during the purchase process.

The cardholders are required to download and install browser plug-ins or an electronic wallet under the SPA system. These "lean" plug-ins do not carry certificates like the "fat" SET wallets of the past, which should result in acceptable download times. Under SPA the purchasing process begins with the user logging into their plug-in (or electronic wallet) when shopping at a merchant site. The plug-in (or electronic wallet) is designed to wake-up when a SPA-compatible payment page is encountered. This allows issuers to provide a range of value-added services such as form filling which expedite the payment process and reduce shopping cart abandonment by the user.

In summary, the SPA model is focused around cardholder authentication and requires the use of plug-in software or an electronic wallet by cardholders. Issuer's can introduce business rules which mandate that all online transactions must use the SPA plug-in (or electronic wallet), which reduces the risk of, unauthenticated online purchases.

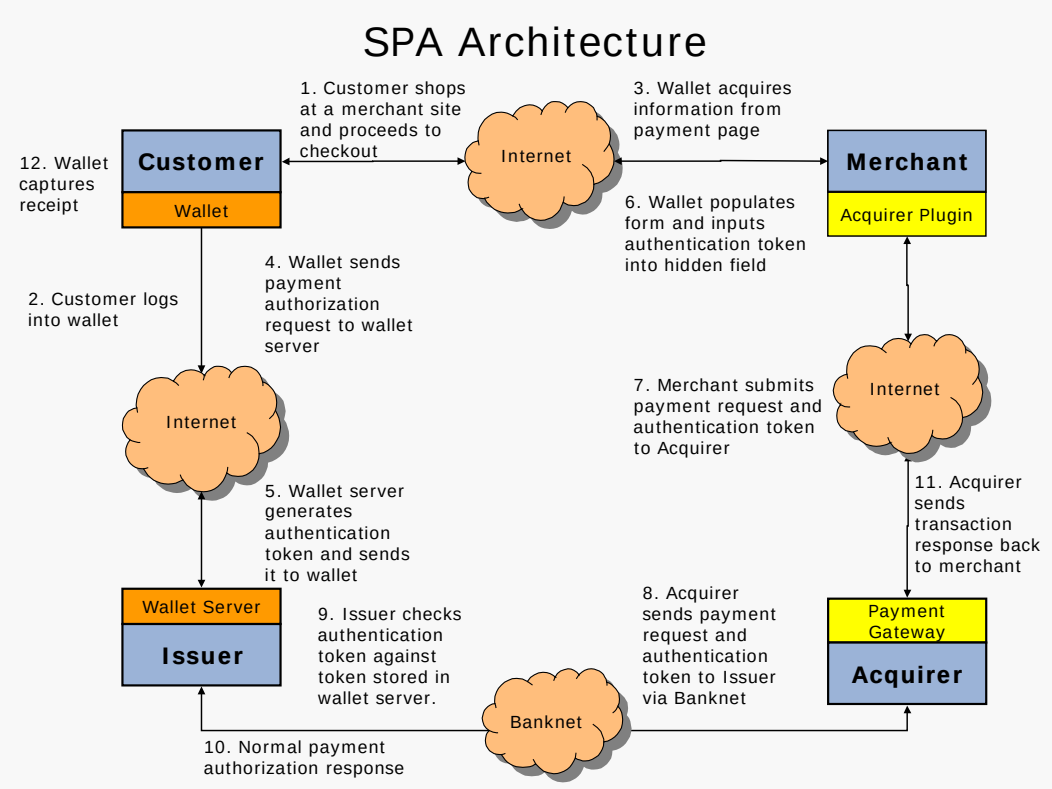
11 SPA and UCAF Functional Specification 1.0, MasterCard

The major advantages of SPA are that it has a simple but elegant architecture. It has a straightforward message flow and does not require additional software implementation by the merchant.

SPA requires one authentication of the cardholder for multiple purchases across different merchants in a single shopping session and the use of a cardholder plug-in or an electronic wallet has mitigated the risk of exposing cardholder's username and password in a "man-in-the-middle" attack.

MasterCard SPA payment process

1) **Customer shops at a merchant site and proceeds to checkout**
2) **Customer logs into electronic wallet**
3) **Wallet reads information from payment page at merchant's site**
4) **Wallet sends payment authorization request to wallet server**
5) **Wallet server generates authentication token and sends it to wallet**
6) **Wallet populates merchant payment form and inputs authentication token into hidden field**
7) **Merchant submits payment request and authentication token to acquirer**
8) **Acquirer sends payment request and authentication token to issuer via MasterCard's Banknet**
9) **Issuer checks authentication token against token stored in wallet server**
10) **Normal payment authorization response**
11) **Acquirer sends transaction response back to merchant**
12) **Wallet captures receipt**



Maestro's Online Debit Solution

> *"The e-commerce strategy, defined by the Maestro International Board and supported by several Member banks' committees of MasterCard International and Europay International, aims at ensuring the rapid, convenient and secure acceptance of Maestro branded cards for Internet purchase transactions."*[12]

Maestro's Online Debit Solution provides a framework for authenticated Internet payment transactions which supports MasterCard's SPA. The global standard for online card payments is a 16-digit PAN and a 4-digit Expiry Date which has posed a problem in the past for Maestro debit cards which do not have a 16 digit account number. Maestro has addressed this problem by endorsing the use of a "static" credit card number, similar to a virtual card number, which is a 16 digit number designed to represent the cardholders' debit account during Internet transactions.[13]

An electronic wallet forms the necessary consumer purchasing platform (CPP) for Maestro cards to be accepted securely and profitably on the Internet. Maestro has introduced the option of using the merchant's expiry date fields (mmyy) as a unique transaction identifier rather than an actual expiry date. This is designed to replace the transaction-specific security token utilized by MasterCard's SPA. The cardholder's electronic wallet is responsible for generating this unique number for entry into the merchant's 4 digit expiry date fields.

The advantage of this approach is that it minimizes the changes, which need to be made to existing merchant websites in order to accept online debit transactions. In contrast to the slightly more onerous requirements of MasterCard SPA, it is not mandatory for acquirers to alter the online merchant interface to their payment gateway to accept a transaction-specific security token. Maestro, however, is leveraging the use of the same hidden fields used by MasterCard in the merchant website for transaction matching purposes.

Maestro's Online Debit solution requires the cardholder's issuer to be participating, the merchant to be participating and the cardholder to download a client-side plug-in or electronic wallet application from their issuer. The Maestro issuer is also given the flexibility of determining a suitable authentication method for their cardholders in a similar manner to SPA and 3-D Secure. Maestro issuers have the option of authenticating users using username and password, biometrics, smart cards, or digital certificates. However, username and password is the simplest for the issuer to implement and is expected to become the most common form of authentication. Some issuers may choose to supplement username and password with an additional level of customer authentication at the moment of transaction.

The Maestro issuer is required to implement a wallet server, which needs to be integrated with the Maestro issuers back-end card systems providing access to cardholder information. The issuer must provide a registration process for this wallet server and distribute Maestro compliant electronic wallets to their cardholders. The Maestro wallet server is responsible for performing matching of transaction details retrieved by the wallet with transaction details received from acquirer Which requires a realtime connection to the issuer's back-end system. The importance of this matching process is elevated in the Maestro solution as it is used to ensure that a transaction was initiated by an authenticated Maestro customer rather than relying on the transaction-specific security token used by MasterCard SPA. Additionally, the Maestro wallet server is responsible for replacing the static card number with the original Maestro debit number, expiry date and track 2 data for transmission to legacy systems.

Payment Acquirers do not need to make major changes to their existing payment gateways to support Maestro's online debit solution. The use of a static card number and dynamically

12 Maestro MIG

13 Maestro has forbidden the use of dynamic pseudo card numbers for online debit transactions due to the complexities of customer support when the card number changes for every online transaction.

generated expiry date allows the Maestro transaction to pass transparently through their existing infrastructure. This also reduces the impact on merchants, as they are not required to change their acquiring process to support the passing of the accountholder authentication value (AAV) security token. The merchant interface to the acquirer is kept intact except for an identifier indicating Maestro transactions.

The merchant accepting Maestro will need to upgrade their shopping cart system to carry hidden fields that hold transaction-specific information, which can be read by SPA compliant plug-ins or electronic wallets. The merchant may also be required to introduce functionality communicated through hidden fields to notify the cardholder's electronic wallet of recurring transactions. Maestro has also made support for partial deliveries or split shipments mandatory which will require the merchant to cater for this functionality in their website if this is their common business practice. Maestro has gone beyond the simple payer authentication provided by protocols such as Visa's 3-D Secure and has introduced an additional level of "transaction authentication". In contrast to payer authentication, which provides protection to the merchant that the customer is bona fide, transaction authentication can provide protection for the customer against merchant initiated fraud during a split shipment. If a merchant is unable to fulfil an order for a number of items it often ships the items in stock and charges the cardholder for the items shipped. When the remaining items are shipped an additional charge is made against the cardholder's account. Maestro's online debit solution will ensure that the original transaction amount authorized by the customer is not exceeded in these additional charges applied to the Maestro account. This is an additional benefit of Maestro's focus on transaction matching within the Issuer's wallet server and provides a mechanism for eliminating chargeback disputes based upon split shipments.

The cardholders are required to download and install electronic wallets under the Maestro solution similar to MasterCard SPA. These can be "lean" browser plug-ins rather than stand-alone windows applications and as such will not require the user to go through an installation process. Under Maestro's solution the purchasing process begins with the user logging into their electronic wallet when shopping at a merchant site. The wallet is designed to wake-up when a Maestro payment option is detected/selected on a SPA-compatible payment page. Additional services such as form-filling, which expedite the payment process, can be provided to reduce shopping cart abandonment by the user.

Maestro have also provided a model which is open to multiple access devices including mobile commerce channels. This should ensure that secure online debit payments can be initiated from PC's at home, at work or in an Internet café as well as new payment devices such as PDA's and mobile phones. This provides the opportunity for the Maestro issuer to provide convenience for cardholder payments initiated from multiple devices without compromising transactional security.

In summary, the Maestro Online Debit solution provides both payer authentication and also introduces effective transaction authentication. It requires the use of an electronic wallet by cardholders and leverages MasterCard's SPA through compatibility with hidden fields on merchants' websites. It has simplified the implementation of online debit solutions through the use of a 16 digit static card number and reduces the changes required to the merchant acquiring process. Maestro have, for the first time, made Internet debit transactions as simple as an authenticated Internet credit card transaction. This should accelerate the adoption of online debit payments as an alternative to credit transactions.

Maestro Online Debit Solution Payment Process

1) **Customer shops at a merchant site and proceeds to checkout**

2) **Customer logs into electronic wallet**

3) **Wallet reads information from payment page at merchant's site**

4) **Wallet sends payment authorization request to wallet server**

5) **Wallet server sends virtual card number, unique transaction identifier for expiry date field (and optional AAV data field) to wallet**

6) **Wallet populates merchant payment form with virtual card number transaction identifier for expiry date field (and optional AAV authentication data field)**

7) **Merchant submits payment request to acquirer**

8) **Acquirer sends payment request to issuer via MasterCard's Banknet**

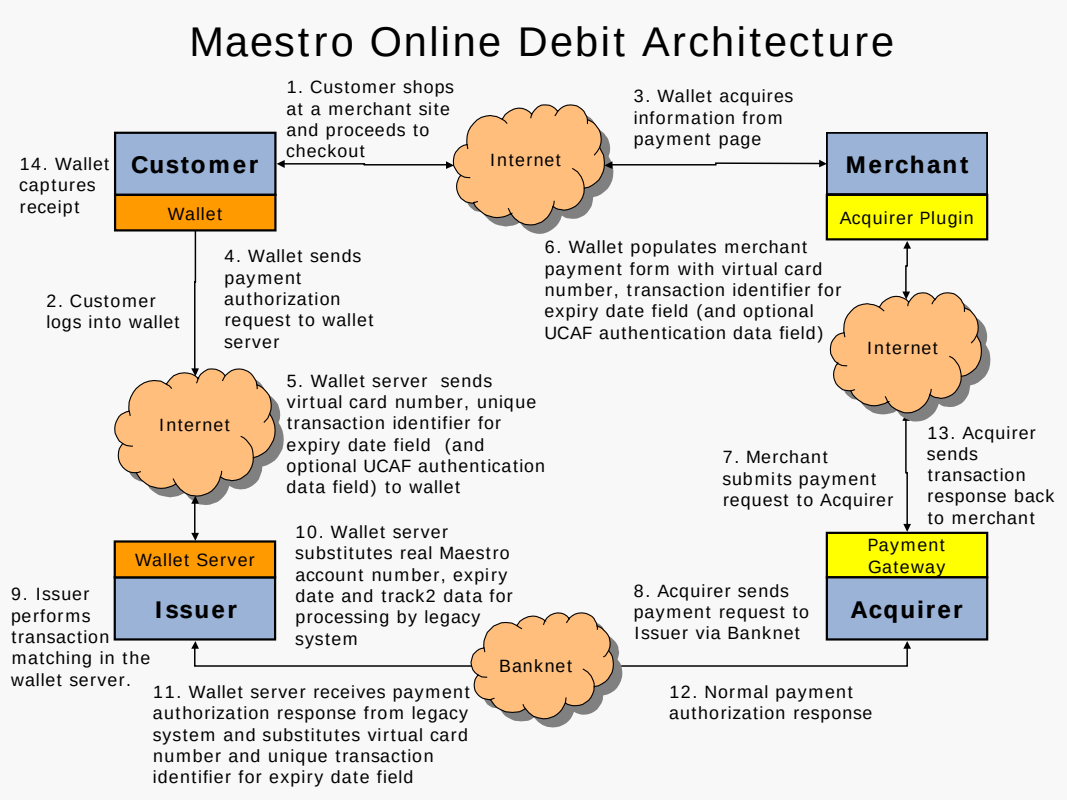
9) **Issuer performs transaction matching in wallet server**

11) **Wallet server substitutes real Maestro account number, expiry date and track2 data for processing by legacy system. Wallet server receives payment authorization response from legacy system and substitutes virtual card number and unique transaction identifier for expiry date field**

12) **Normal payment authorization response to issuer**

13) **Acquirer sends transaction response back to merchant**

14) **Wallet captures receipt**



Conclusion

The Internet will continue to grow as a medium for commerce and this will necessitate the need for security, integrity and authenticity in online transactions. A plurality of payment and authentication methods have arisen and will continue to arise serving the diverse needs of the online economy.

The use of SSL to simply provide transactional integrity will not address the issue of fraud and chargeback for online transactions. A widely deployed authentication system is necessary to reduce the costs to merchants, acquirers and issuers currently experienced. A common authentication system also promises to mitigate the consumers' fears of using their credit card to make online purchases, which should increase the adoption of eCommerce.

The SET protocol was an overly complex system and expensive for all parties to implement. It was also costly to maintain due to the reliance on digital certificates. While it was good to see Visa and MasterCard collaborating on the protocol it never gained widespread acceptance and the 3-D SET implementations arrived too late and delivered too little to change the market's negative sentiment toward SET.

3-D Secure is the first of the new authentication methods to market and has the support of a number of industry vendors. While it adds 10-15 seconds to the purchasing process and requires a separate authentication for every purchase it does have a first mover advantage and is being pushed by the world's largest credit card organisation. 3-D Secure is likely to gain high levels of penetration by 2003 and Visa is attempting to make its installation mandatory for credit card issuers.

MasterCard SPA is a technically elegant solution to online credit card authentication. It promises easier integration for the merchant but does require the cardholder to install a "lean" client plug-in (or an electronic wallet). The benefit of the electronic wallet is that value-added services such as form filling can be provided to the customer. MasterCard have committed to upgrading their Banknet to support SPA and have delivered a solution which requires less messages to be sent over the Internet which should result in greater efficiency.

Maestro could have delivered their own authentication solution to the market for online debit transactions, as there is plenty of demand from consumers to expand the range of online payment methods available. By delivering a standard, which is compatible with MasterCard SPA, yet is even easier for merchants and acquirers to implement, they have made online debit transactions a very achievable outcome for Maestro Issuers. Maestro and MasterCard will be able to exploit the synergies of a combined rollout and issuers will be able to leverage a common infrastructure for both solutions. Online debit transactions, which have not had the same take-up as online credit card transactions to date, are now poised for rapid growth.

Both 3-D Secure and SPA deliver a solution to an existing problem in online credit card transactions – a lack of authentication. Both solutions will gain traction in the marketplace in the coming years. After the failure of SET these credit card organizations need to be successful in promoting this round of authentication protocols.

The online economy would benefit from one standard for online authentication rather than different standards from Visa, MasterCard and Maestro. However, GPayments has been quick to realize that all three standards can be supported in a single solution, which simplifies the decision-making, implementation and maintenance process for financial institutions. The real question is how quickly these cardholder authentication solutions can be implemented in the market leading to a ubiquitous authentication standard for all online transactions.

Glossary

AAV Accountholder Authentication Value. A transaction-specific security token generated from hidden UCAF fields on a SPA compatible website, which is passed through the UCAF field on MasterCard's Banknet for transaction matching at the issuer's wallet server.

Acquirer A Financial Institution (or its agent) which acquires from the card acceptor the data relating to the transaction and initiates that data into an interchange system.

API Application Programming Interface

Authentication This is the process of verifying that a party is really who it claims to be.

Cardholder A customer associated with an account, requesting the transaction from a card acceptor.

Certificate Authority A trusted third party that authenticates a user and provides them with a certificate (public key)

Electronic Wallet A software application that stores purchasing information for the Internet. Such information includes the cardholder's name, mailing address, billing address, credit card number, and often some security information.[14]

Issuer A Financial Institution (or its agent) which issues the financial transaction card to the cardholder.

Merchant A merchant offers goods for sale or provides services in exchange for payment. A merchant that accepts payment cards must have a relationship with an Acquirer.

Payment Gateway A payment gateway is a device operated by an Acquirer or a designated third party that processes merchant payment messages, including payment instructions from cardholders.

PAN Primary Account Number. This refers to the 16 digit number appearing on a credit card.

PDA Personal Digital Assistant. A small handheld device or computer.

SET Secure Electronic Transaction. A certificate based payment and authentication standard.

SPA Secure Payment Application. Authentication standard developed by MasterCard

SSL Secure Sockets Layer. A data transfer protocol.

3-D Secure Authentication standard developed by Visa

URL Uniform Resource Locator. A unique address of a resource on the World Wide Web

UCAF Universal Cardholder Authentication Field This is a hidden field provided by the merchant on the order confirmation page. UCAF is used for transaction matching at the issuer's wallet server.

WAP Wireless Applications Protocol. A communications standard for mobile devices.

WTLS WAP Transport Security Layer

X.509 The most widely used standard for defining digital certificates.

XML Extensible Markup Language. A data description language designed for interoperability between disparate systems

14 Electronic Wallets: The Conceptual Framework October 1999 Theodore Lacobuzio The Tower Group