



GPayments
Innovate - Empower - Adapt

Authentication and Payment Solutions

Visa 3-D Secure vs. MasterCard SPA

A comparison of online authentication standards

At a glance

This paper is designed to provide a comparative analysis of the the new generation of authentication standards - Visa 3-D Secure (VbV) and MasterCard's Secure Payment Application (SPA). It is written from the perspective of a software company which has developed and implemented issuer, cardholder, acquirer and merchant products for secure electronic commerce payments. It draws upon experiences as an early developer and implementer of SET, a founding member of the Visa 3-D Secure Forum, a developer of a 3-D Secure Access Control Server, a developer of a 3-D Secure Merchant Plug-in, a participant in the 3-D Secure compliance testing process, a supplier of 3-D Secure products and services to Visa and a provider of a 3-D Secure test environment to merchants. It also draws upon experiences as a developer of a SPA cardholder applet, a developer of a server-based electronic wallet, a MasterCard SPA draft specification reviewer, a licenced MasterCard SPA implementer, a Maestro MIGS draft specification reviewer and a supplier of demonstration SPA software to MasterCard. This whitepaper is designed to convey the first-hand experience of working with these standards. It also seeks to bring clarity to the strengths and weaknesses of each standard while maintaining an independent perspective.

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.au
Website: www.gpayments.com

Copyright © 2002 by GPayments - This work is copyright. Other than as permitted by law, no part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any process without prior written permission.

While GPayments has taken all reasonable care in preparing this whitepaper, the information, figures and details contained within are presented in good faith. No warranty or guarantee (express or implied) is given by GPayments as to the completeness or accuracy of the whitepaper or any information provided in connection with it.

Contents

Background.....	3
Visa 3-D Secure Overview.....	4
MasterCard SPA Overview.....	8
A Comparison of the Cardholder Experience under Visa 3-D Secure and MasterCard SPA.....	10
CARDHOLDER EXPERIENCE.....	10
Initial Registration Experience.....	10
Purchasing Experience.....	11
Multiple Location Purchasing.....	15
Additional Services.....	16
A Comparison of the Issuer Experience under Visa 3-D Secure and MasterCard SPA.....	17
ISSUER IMPLEMENTATION.....	17
Supporting Cardholders.....	18
Issuer Reporting.....	19
A Comparison of the Merchant Experience under Visa 3-D Secure and MasterCard SPA.....	20
Merchant Integration Process.....	20
Merchant Reporting.....	22
Ongoing Maintenance.....	23
A Comparison of the Acquirer Experience under Visa 3-D Secure and MasterCard SPA.....	24
Technology Implementation.....	24
Supporting Merchant Upgrades.....	26
Acquirer Reporting.....	26
A Comparison of the Visa 3-D Secure and MasterCard SPA Architecture.....	28
CENTRALIZED OR DISTRIBUTED?.....	28
Support for Compliance Mandates.....	30
INTEROPERABILITY WITH OTHER CARD COMPANIES.....	30
A Comparison of Visa 3-D Secure and MasterCard SPA Security Architecture.....	32
Conclusion.....	34
Glossary.....	35

Visa 3-D Secure vs. MasterCard SPA

Background

Consumers do not have confidence in sending their credit card details over the Internet but they actually fear this for the wrong reason. Most people are concerned that their credit card details will be intercepted on the way to the merchant, which is almost impossible. The use of the SSL protocol, which is used by all major eCommerce sites, encrypts the credit card details during transmission over the Internet ensuring its confidentiality.

The real problem, which most people do not realize, is that there has been no way to “authenticate” a customer in an online credit card transaction. This means that we have not had a widespread mechanism to confirm the identity of the buyer at the time of purchase.

Authentication is the verification of a credit card owner made during a card purchase. Credit cards were originally designed for transactions made in the physical world. In the physical world authentication is achieved through a physical signature, which is manually checked at the point of sale.

In today’s environment, an online buyer simply types the credit card details into a website in order to make a payment. This has introduced a major problem as anyone can type in anyone else’s credit card details in order to make a purchase and the online merchant has no way of determining if the buyer is genuine.

Without effective authentication there are many problems including lack of confidence for customers, higher cost of transactions and loss of revenue for merchants, higher cost of services and charge-backs for banks and ultimately damage to the image of credit card companies. The lack of authentication in online transactions also opens up the possibility for alternative (non credit card) payment methods to gain market share.

In the early 90’s Visa, MasterCard and American Express realized that for credit cards to become the dominant instrument of payment over the Internet a means of authenticating customers on the Internet was necessary. They decided to develop a common standard called Secure Electronic Transaction (SET) to address the issue.

SET was a technological masterpiece, which involved every cardholder, every merchant, and every bank receiving and managing a digital certificate (PKI). Unfortunately it was far too costly and complex to implement and it therefore failed to gain widespread market acceptance.

Meanwhile, eCommerce continued to grow and with it the number of fraudulent credit card purchases and charge-backs increased. These fraudulent purchases continued to gain widespread media coverage, which in turn added to the uncertainty for customers and merchants transacting over the Internet. Today the amount of online credit card transactions accounts for 2-4% of the total credit card transactions, which is still relatively small. However, the incidence of fraud has been estimated at twelve times higher in the online world as it is in the physical world. If eCommerce keeps expanding at the current rate it will become

a major problem in the future. Visa and MasterCard are well aware of this problem and have attempted to meet the challenge.

In 2001, five years after introducing SET, the major credit card companies went back to the drawing board to introduce new authentication standards for online purchases. This time, rather than working together, Visa and MasterCard have decided to introduce competing authentication standards for online transactions. Visa has introduced a system called 3-D Secure (“Verified by Visa”) and MasterCard has introduced a system called Secure Payment Application (SPA).

The operation of 3-D Secure and SPA are technically different but under both solutions the customer is going to be required to enter a username and password or a PIN number in order to authenticate themselves for online purchases.

With these new standards even if a hacker manages to gain access to card numbers they will not be able to use them to make purchases unless they can also obtain the owner’s username and password for their payment card.

Visa 3-D Secure Overview

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 organizations using Visa’s infrastructure

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.

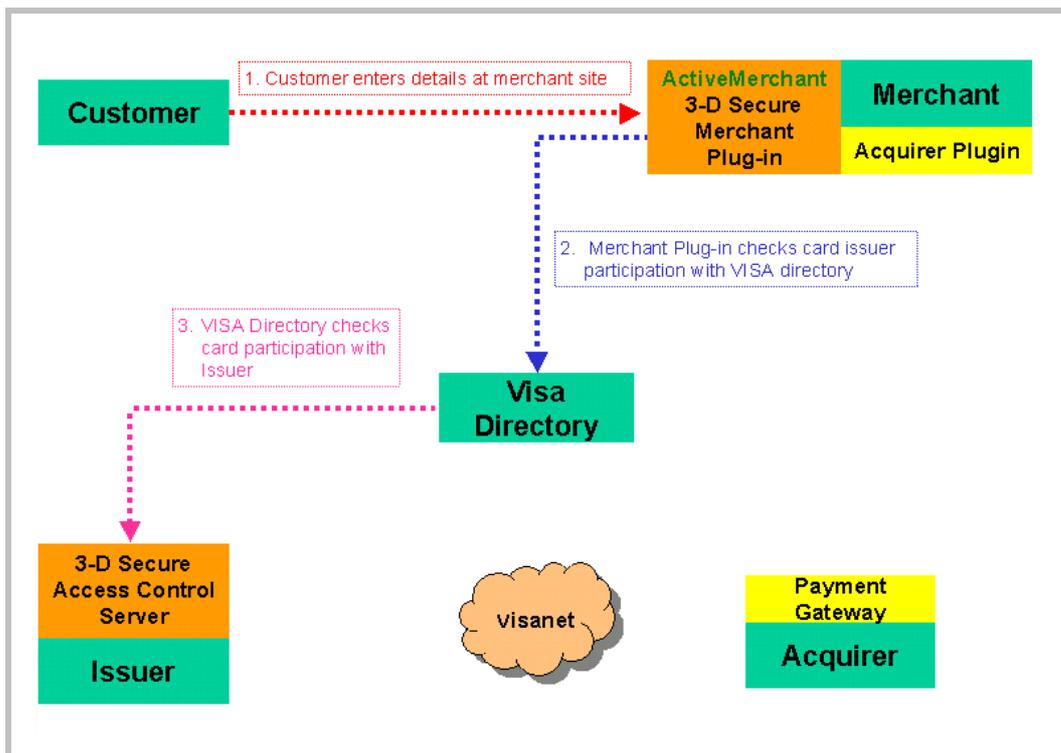
In the “Issuer domain” the issuer is responsible for deploying an issuer system comprised of enrolment, receipt and access control servers. The issuer system handles communication with 3-D Secure merchants and a centralized Visa directory, which acts as a communications intermediary between merchants and issuers.

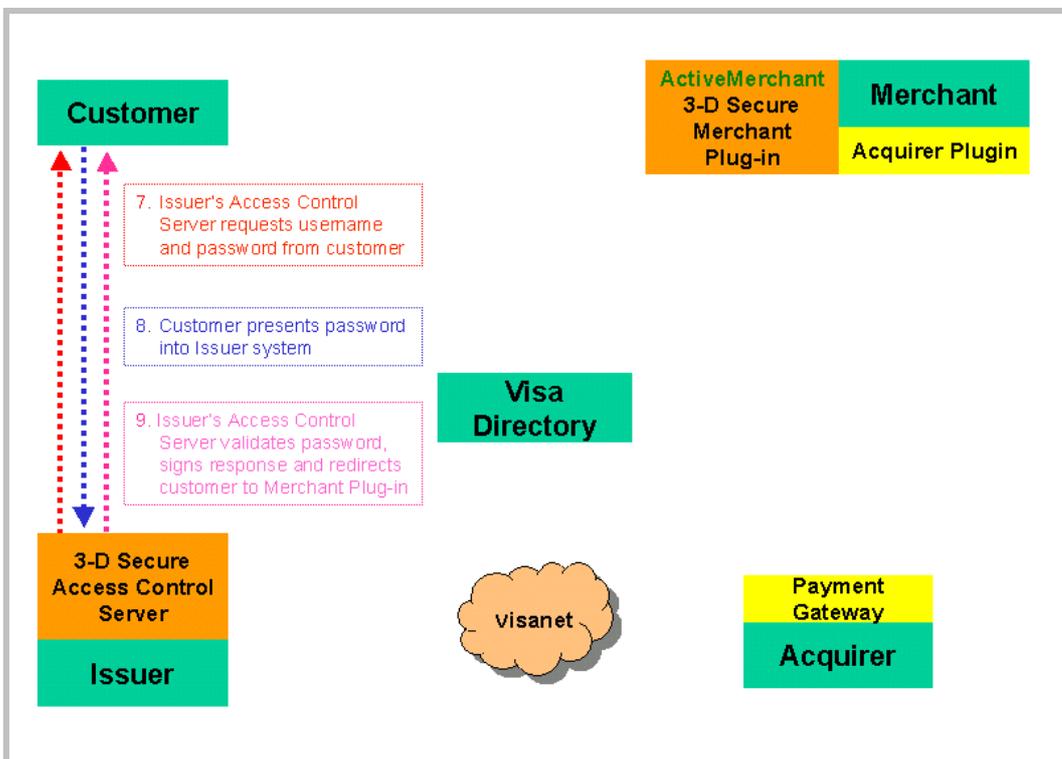
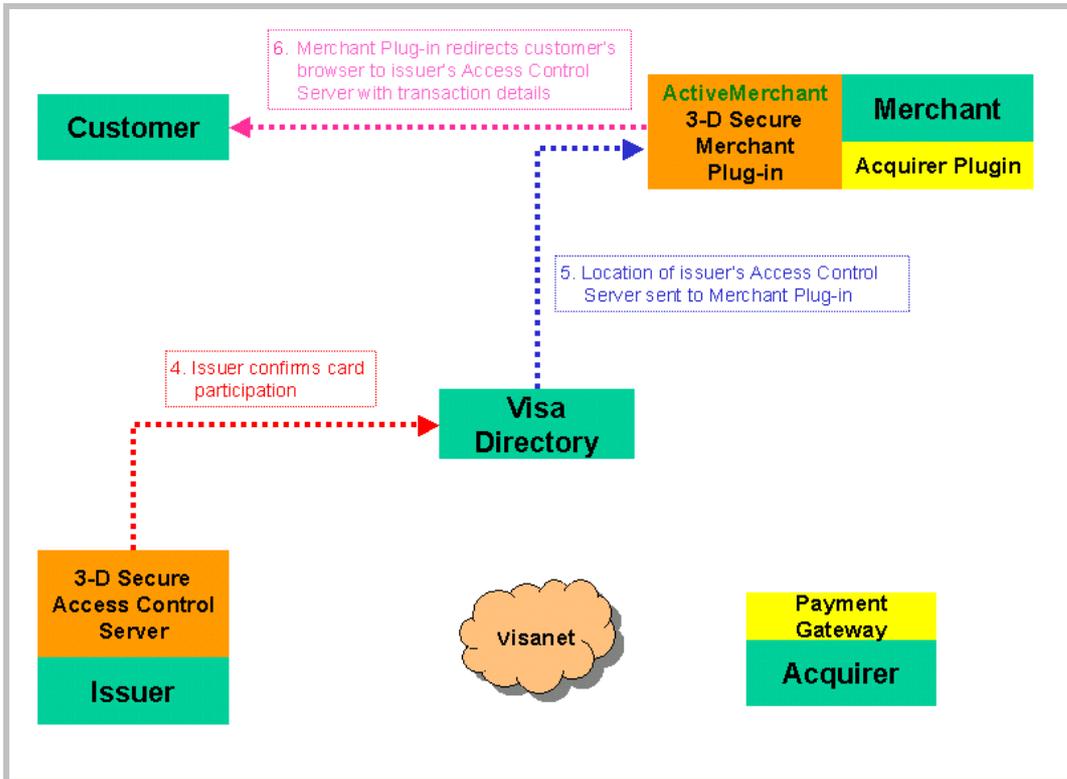
The issuer system handles all interactions with the customer at multiple Internet access points that support a browser. The software deployed by the issuers needs to be integrated with their backend card systems providing access to cardholder information.

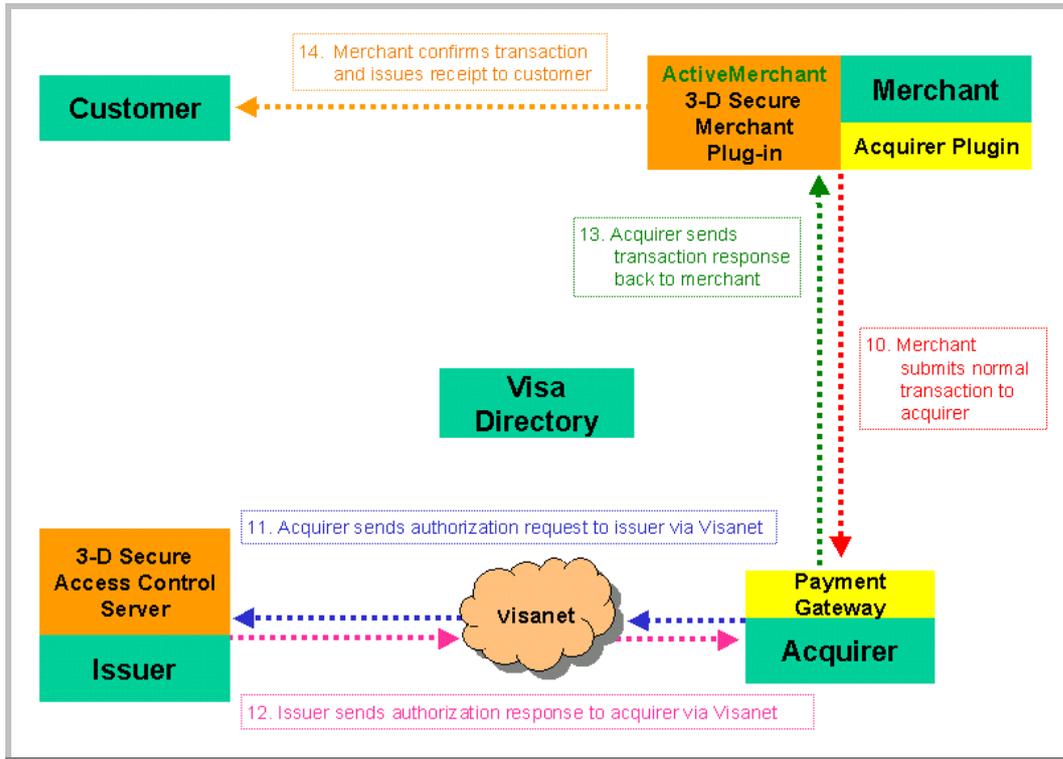
3-D Secure has minimized the requirements for cardholders mandating that they only need a browser to participate unless they are making a chip purchase in which case they require client-side software as a minimum pre-requisite.

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) or connect to a 3-D Secure Merchant Server to handle communication with the centralized Visa directory and the customer's credit card issuer. This requires code-level changes to be made to the merchant's existing shopping cart system.

Visa has introduced the Visa Directory, which is an Internet-based system that provides information on participating credit card issuers and the location of their Access Control Servers on the Internet. Issuers' Access Control Servers and Merchants' 3-D Secure solutions all communicate with the Visa Directory in order to provide authenticated transactions. Visa still uses the normal Visanet communication channel between credit card issuers and credit card acquirers for credit card authorization.







MasterCard SPA Overview

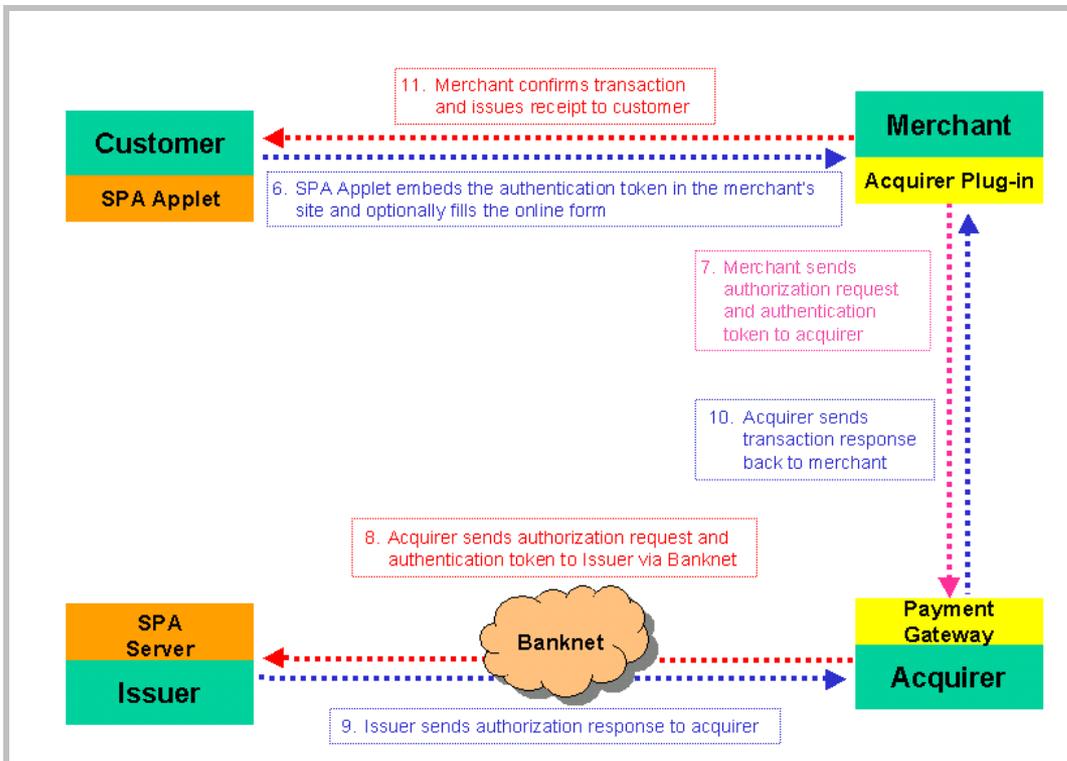
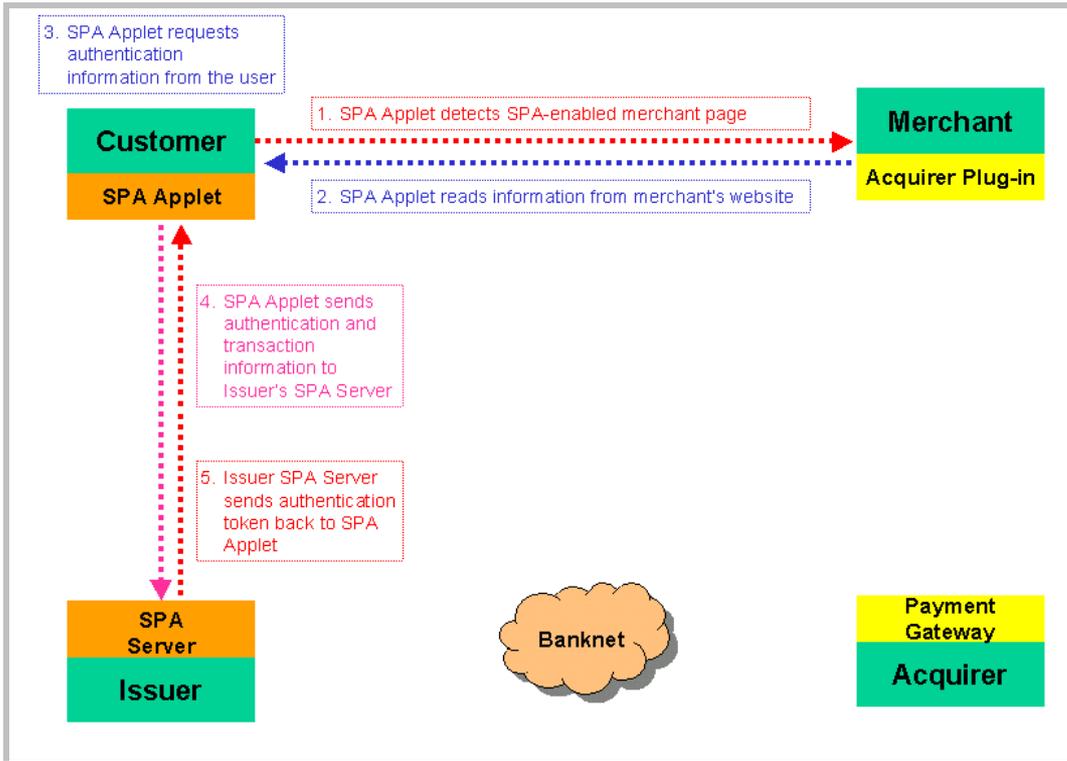
SPA is an authenticated payment environment, which requires the cardholder's issuer to be participating, the merchant to be participating and the cardholder to use "thin client" software known as a SPA applet.

The issuer is required to implement a SPA 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 SPA Server and distribute SPA applets to their cardholders. The SPA 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).

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 upgrade their payment gateway plug-in, which supports the passing of the security token via an extra parameter.

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 applets.

The cardholders are required to use client-side software under the SPA system. This could be emailed to the cardholder, distributed on floppy disk/CD-ROM or downloaded from the issuer's website. These "thin client" applets do not carry certificates like the "fat" SET wallets of the past. The SPA applet is designed to "wake-up" when a SPA-compatible payment page is encountered. Under SPA the purchasing process begins with the user logging into their SPA applet when shopping at a merchant site. This allows issuers to provide a range of value-added services such as form filling, which expedites the payment process, and reduces shopping cart abandonment by the user.



A Comparison of the Cardholder Experience under Visa 3-D Secure and MasterCard SPA

This comparison is based upon the “vanilla” 3-D Secure and MasterCard SPA cardholder experiences with username and password as the authentication method. Visa 3-D Secure only requires a browser for username and password authentication and does not mandate a client –side application unless a chip card is used as a stronger form of authentication.¹ MasterCard SPA mandates the use of a client applet for both username/password and chip authentication. The Cardholder Experience has been examined from the perspective of initial registration, the purchasing experience and purchasing experience from computers in multiple locations.²

CARDHOLDER EXPERIENCE

Initial Registration Experience

The issuer can define both Visa 3-D Secure and MasterCard SPA registration/enrolment processes. As such a single registration process could be used for issuers, which need to support both 3-D Secure and SPA registration. The registration process can be performed entirely online or it can use a combination of a physical mail out of the password and online registration.

A typical registration process for 3-D Secure could take approximately 2.5 minutes assuming that the cardholder doesn't read the terms and conditions in full and just clicks accept. A typical registration process for SPA would vary depending on whether the SPA applet was downloaded over the Internet or distributed via floppy disk, CD-ROM or as an attachment to email. If it is assumed that most client applets will be downloaded over the Internet a typical SPA enrolment could be expected to take 3-4 minutes³.

Visa's approach in eliminating the need for the cardholder to download client-side software has been widely marketed as a differentiating advantage of 3-D Secure over MasterCard SPA. The download of a SPA applet lengthens the registration process and may also introduce compatibility problems with older browsers or platforms that do not support a client applet.

The original digital wallets, such as IBM's digital wallet released in 1996, certainly did introduce a high level of friction for the cardholder. Weighing in at approximately a 4.3 MB download and requiring the user to run a Setup.exe for installation made the digital wallet concept impractical for the average cardholder. What made the process even worse is that the original digital wallets required the cardholder to request a digital certificate, which then needed to be issued by the Bank. Finally, when the digital certificate was obtained from the issuer, the cardholder would then be required to load the digital certificate into the wallet for it to function.

¹ The situation where a client applet or server-based eWallet is used for a Visa 3-D Secure transaction is beyond the scope of this document and does not form a good comparison as it makes the Visa 3-D Secure cardholder experience almost identical to the MasterCard SPA experience

² A different location computer is defined as a computer which is different from the initial registration computer which may be at home, work, in a library or in an Internet café.

³ A 350kb SPA plug-in would add about 1min 40secs download time at 56kbps for SPA.

The applets required for MasterCard SPA have evolved considerably from their earlier forebears in that they are easier to use and do not require digital certificates. A SPA applet may be in the range of 100-500 KB depending on functionality and install directly into the customer's browser without the need for them to even run an installation program. As bandwidth has increased the download time has reduced to the point that it is almost negligible and there is no effort required on behalf of the cardholder for installation.

Internet users have also become more proficient in the use of the Internet and it has been demonstrated that customers are prepared to download software if they perceive there is value in it.⁴ It is probably not appropriate to examine the download time for a client applet without having regard to the timesaving that a client applet affords the cardholder in subsequent purchases through automatic form-filling.

If the time taken to download client software to cardholder machines is too onerous for the individual it has two major ramifications. The first is that cardholders do not perceive the ability to make an authenticated payment over the Internet as important as being able to perform other tasks such as reading .PDF files, decompressing .zip files or playing .mp3 audio files where the user must also download client software. Secondly, chip card authentication will never be successful as a stronger form of authentication for Internet purchases. All chip transactions require a piece of software to be installed on the cardholder's machine in addition to the requirement for the machine to have a chip card reader.

If Visa suggests that software downloads introduce too much resistance they will be effectively undermining their own 3-D Secure chip authentication standard, which requires software to be downloaded to the cardholder's machine. They may also be restricting their members' autonomy to maintain control of their own customer data and end up forcing their members to rely on services from technology firms such as Microsoft and AOL. Microsoft and AOL already have large installed bases of client software running on cardholder's desktops in the form of Internet Explorer and the AOL Browser. They will be positioned to leverage this advantage to gain control of the payments market through online authentication services.

Purchasing Experience

In order to investigate the online purchasing experience it is necessary to examine one of the major problems in online purchasing to date - shopping cart abandonment. Many customers begin the online purchasing process only to stop before completing a transaction. There are various estimates of how many purchases fail in this manner ranging from 30-60%. However, 40% of cardholders cite the time taken or the number of fields that need to be filled out as a major reason for Shopping Cart Abandonment.⁵

Visa has not taken any steps to address the problem of shopping cart abandonment in the 3-D Secure standard. The transaction flow in Visa 3-D Secure adds ten additional messages that need to be sent across the Internet in comparison with the current payment process. Each of these messages is subject to the available Internet bandwidth and may even incur time-outs if a

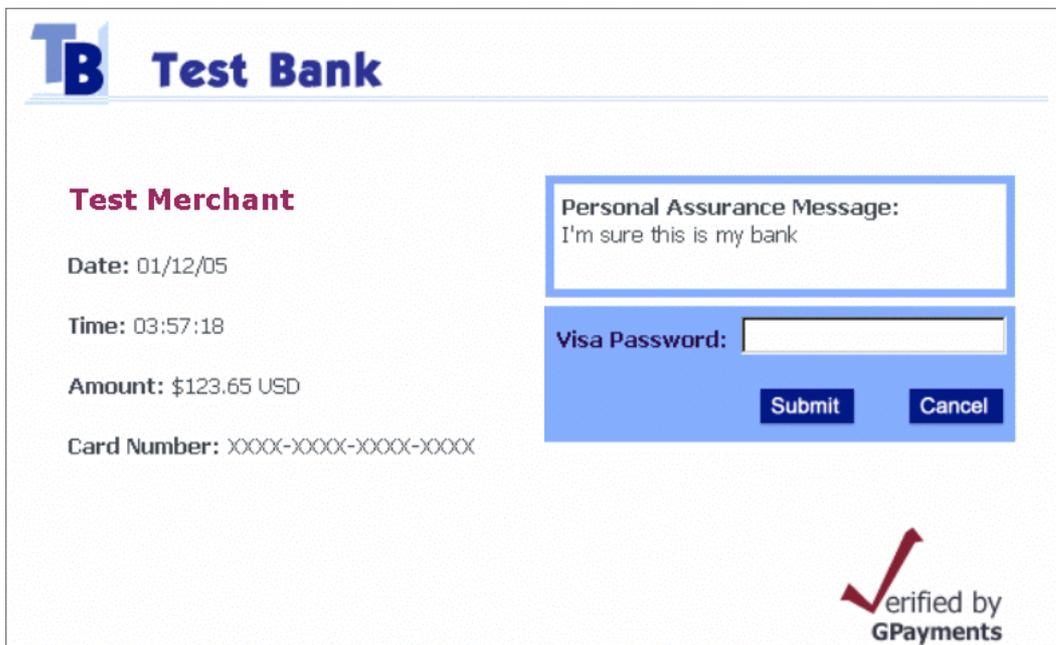
⁴ Over 38 million users managed to download Napster which had a file size of 1MB. Most Internet users download Adobe Acrobat reader (> 3MB) and other programs such as Winzip, Winamp etc.

⁵ Understanding the e-Wallet user, A Market Research Report p.2

server does not respond. Visa states that the introduction of 3-D Secure adds approximately 10-15 seconds to the current online purchase experience. However, in practice it can add more than that due to the nature of Internet communications, which can experience delays due to network load.

All cardholders that register for 3-D Secure will be faced with an additional screen from their credit card issuer following the submission of their payment information to the merchant. On this screen they will be required to confirm the transaction value and check their personal assurance message before entering their password or PIN code. The personal assurance message is the only mechanism, which the cardholder has to protect himself against a “man-in-the-middle” attack e.g. the merchant pretending to be the credit card issuer in order to capture the cardholders’ password or PIN for future malicious use. However, there are already methods available to fraudulent merchants, which will allow them to capture the personal assurance message, using software, which is freely available over the Internet.

Visa 3-D Secure Authentication Screenshot



An example of an issuer access control server, ActiveAccess, prompting a cardholder for an authentication password.

The 3-D Secure cardholder experience has prompted some interesting responses from online merchants who have been seeking ways to reduce the time spent for a customer to make an online purchase. Many larger online retailers register all their customers’ details (including credit card information) in order to streamline the purchase process for repeat customers.

The largest online retailer, Amazon.com, has decided not to participate in Visa 3-D Secure at this point.

"From our standpoint, the amount of friction that Verified by Visa introduces for the customer outweighs the benefit from reducing fraud. It would turn one-click ordering into four-point, three-click ordering."⁶

⁶ Mark Britto, Amazon's director of corporate development.

Visa has always remained focussed on its core business of payment and authentication and it could be that Visa sees techniques such as automatic form filling to be in the domain of technology companies rather than card companies. This may prove to be a costly mistake on Visa's part in a convergent economy where banks now face a threat from external entrants such as telcos, portals, media companies and technology companies.

Visa's member banks currently see their customer information as their own proprietary data and are threatened by the introduction of competing online services from technology companies.⁷ This may eventually alienate Visa's member banks that see their customer data as a unique competitive advantage and seek to provide Internet-based services directly to cardholders rather than through an intermediary such as a technology company.

Furthermore, under Visa 3-D Secure the cardholders must authenticate themselves for every purchase made at different sites during a single shopping session. In this respect 3-D Secure has been designed to provide authentication for consumers who only make purchases rarely rather than businesses, which may make multiple purchases per day. It is feasible that a purchasing officer in a major corporation could be making continuous purchases over the Internet every day and under 3-D Secure would be required to constantly re-authenticate with their issuer.

The other area that can create a confusing user experience under 3-D Secure occurs when the issuer opens a new browser window for the input of the customer's password. If the user accidentally clicks on the original browser window, the password entry page can be sent behind the main browser page. This can leave an inexperienced user waiting indefinitely for their payment to complete while the payment process is actually waiting for their password to be inputted. This scenario would result in a timeout and a failed online purchase.

The MasterCard SPA purchasing experience can leverage the advantages of an cardholder applet which include automatic form filling, reduced Internet messaging during a transaction and greater security⁸. Automatic form filling is not possible to achieve without a cardholder applet and requires the storage of personal information including multiple credit cards, shipping and billing addresses on either the cardholder's local machine or at a server-based system managed by the issuer.

Automatic form filling itself has improved remarkably over the past couple of years. The first generation eWallets were only able to form-fill on a limited number of websites that were pre-defined. The form-filling function was also crippled every time the online merchant changed the website layout or payment process. This was clearly not satisfactory for a global marketplace where new websites are launched every day and websites are often upgraded to provide new functionality. The new form-filling techniques are based upon "intelligent form population" which allows a cardholder applet to potentially fill-in any online payment forms with a high degree of success.⁹

⁷ Microsoft Passport and the launch of Microsoft's .NET MyServices may see the increased storage of cardholder details on centralized Microsoft servers.

⁸ A client plug-in provides greater protection against "man-in-the-middle" attacks such as the situation where the merchant "mocks up" the Issuer's Verified by Visa screen in order to capture the cardholder's password.

⁹ Intelligent form population can fill 100% of websites complying to the ECML standard and fully populate over 90% of websites which do not conform to the ECML standard.

The major benefit of automatic form filling for cardholders is the sheer amount of time that it saves during the online form-filling process. Cardholders may need to type in the following information in order to effect a purchase online:

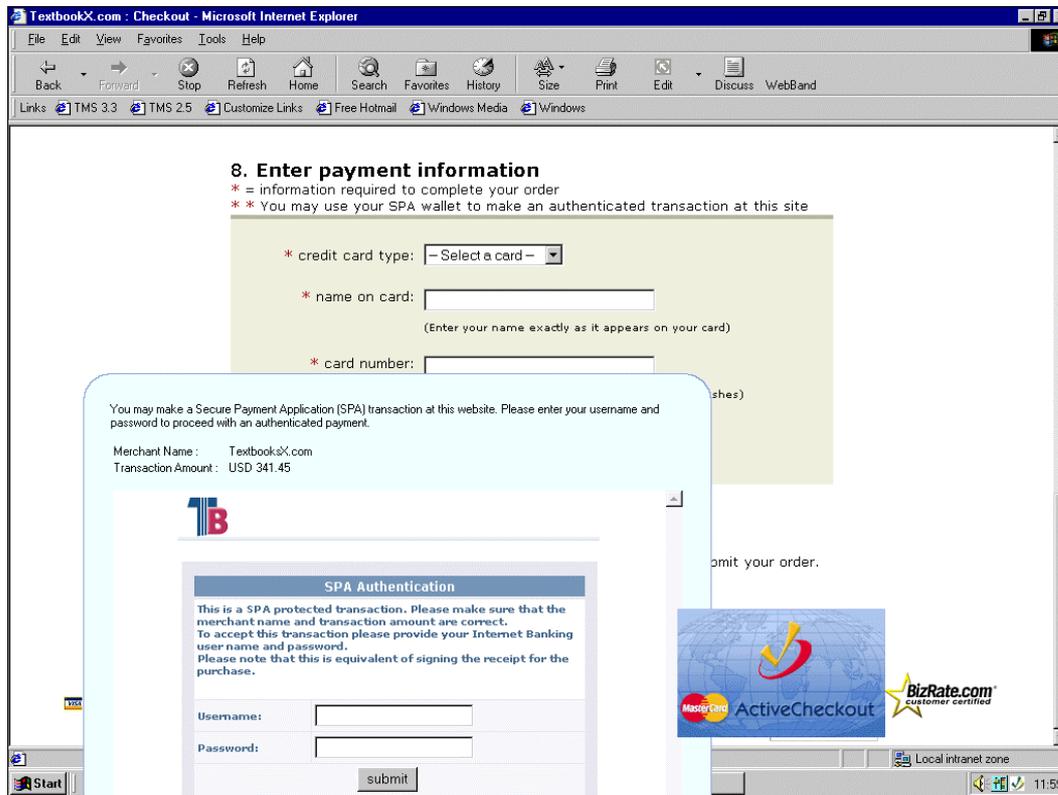
email address
billing address:
first name
last name
street address
city
state
postal code
country
phone number
shipping address:
first name
last name
street address
city
state
postal code
country
phone number
payment information:
credit card type
name on card
card number
expiration date

This is a daunting task for anyone who is not familiar with a computer keyboard. It may even be a prohibitive task for some older Internet users who wish to make online purchases. It is assumed that even a reasonably competent typist will take two minutes to fill out this amount of information. Through the use of automatic form filling the MasterCard SPA purchase experience saves 60-90 seconds in comparison with the existing online purchasing process for each purchase. This is such a significant time saving that people who make more than one online purchase per year could actually justify the additional time required to download a client applet to their local machine. 79% of cardholders that have experienced automatic form filling cite the ability to fill out online merchant forms automatically as an extremely important feature.¹⁰

Another advantage of the MasterCard SPA purchasing process is that cardholders may only be required to authenticate once and can then buy multiple products from different sites without the need to re-authenticate with their issuer. This makes MasterCard SPA a more suitable standard for multiple purchases within a single shopping session.

¹⁰ Understanding the e-Wallet user, A Market Research Report p.7

MasterCard SPA Authentication Screenshot



An example of a cardholder applet, ActiveCheckout, prompting a cardholder for an authentication password.

Multiple Location Purchasing

Internet access is fast becoming available at a range of different computer terminals. Most people access the Internet from home or work. However, it is now possible to use the Internet in Internet cafes, libraries, petrol stations, fast-food outlets and hotels. Wherever a person is able to use the Internet it is possible that they may wish to make an online purchase.

Visa 3-D Secure has a uniform browser-based cardholder experience for purchases made from any computer on the Internet. There is no impact on the purchasing experience regardless of where the online user is located at the time of purchase.

MasterCard SPA requires a cardholder applet in order to make an authenticated purchase at every Internet location. As such a cardholder may be required to download an applet at a remote location in order to make a purchase. The first generation of eWallets made it an unviable proposition for cardholders to make purchases at more than one computer due to the download size and the need for a digital certificate to reside on the local computer. These earlier eWallets were also inhibited in that the client/server communication method would not always work through corporate firewalls.

It is important to note that the cardholder applets used by MasterCard SPA may not be intrinsically linked to any particular cardholder. The cardholder applet can be a "shell" program, which is identical for every cardholder. Following successful

log-in by the cardholder these applets are generally populated with the cardholders information sourced from a SPA Server residing on the Internet. A cardholder who is already registered for SPA with their issuer does not have to go through a registration process again at a remote location in order to use a cardholder applet. They would have the option of simply downloading a new “shell” and logging on. If another cardholder had already downloaded a cardholder applet to the computer a new cardholder would simply be able to log-in to this “shell”.

Visa 3-D Secure definitely has an advantage for remote purchasing if a cardholder uses a cardholder applet, which stores information locally.¹¹ However, depending on the connection speed at the remote location, it may actually be faster for a cardholder to download a cardholder applet¹² and use the automatic form filling to make a purchase than performing a 3-D Secure transaction.

Additional Services

The focus of this section of the whitepaper is to compare the standard online purchasing process under Visa 3-D Secure and MasterCard SPA. It is, however, worth noting that Visa 3-D Secure limits issuers to only providing an online authentication and payment service to their cardholders. In contrast, the use of a cardholder applet under MasterCard SPA allows a range of diverse services to be provided to cardholders. Examples include online receipt capture, online transaction reporting, loyalty point reporting, merchant site links, storage of passwords for accessing sites on the Internet, electronic bill presentment and payment, pseudo account numbers, P2P payments and use of a virtual pin pad for additional levels of authentication (e.g. debit purchases).



An example of a server-based eWallet, ActiveWallet, offering additional services such as online bill payment.

¹¹ It is possible for cardholders to use a cardholder applet for MasterCard SPA which stores cardholder information on the local machine and only connects to a server for transmission of authentication information.

¹² which uses server-based information storage

A Comparison of the Issuer Experience under Visa 3-D Secure and MasterCard SPA

The comparison for issuers will examine technology implementation at the issuer, the issuer's role in supporting cardholders and reporting for the issuer.

ISSUER IMPLEMENTATION

It is the Issuers who face the greatest challenge in implementing cardholder authentication standards. Acquirers who have already implemented an Internet Payment Gateway are faced with the prospect of upgrading their systems and merchants. Issuers, however, are faced with the prospect of building new environments, deploying new systems and integrating these with back-office systems, Internet banking systems and in some cases, payment switches. Very few issuers have implemented a server-based wallet system, which can be upgraded to support Visa 3-D Secure and/or MasterCard SPA.¹³

In order to comply with Visa's 3-D Secure protocol each Issuer is required to sign up to a 3-D Secure Access Control Server (ACS) provided by one of Visa's managed services or run their own 3-D Secure ACS in-house. A 3-D Secure Access Control Server is required to manage communication with 3-D Secure Merchant Plug-ins, manage communications with the Visa Directory and authenticate cardholders using the Issuer's chosen authentication method. The use of a Visa managed service reduces the initial cost, as the issuer does not have to purchase hardware to run the ACS. Regardless of whether the Issuer uses a managed service or in-house ACS they will be required to implement a process/interface for regularly loading their cardholder data to the ACS and a process/interface for allowing the ACS to authenticate their cardholders during 3-D Secure registration and ensuing 3-D Secure transactions.

If an issuer is ever going to run an Access Control Server in-house they could reduce total cost of ownership by implementing it in-house straight away. There are a number of advantages in running a 3-D Secure ACS in-house which include closer integration with the issuer's card system. An in-house ACS also removes the need for a card issuer to send their sensitive cardholder information to managed services residing in different countries/time zones. This reduces administrative costs in setting up and maintaining regular batch tasks to keep the cardholder data in the issuer's card system and the managed service synchronized. An in-house ACS allows the issuer to fully brand/customize their ACS rather than participating in a "vanilla" co-branding arrangement with Visa. It also allows the issuer to leverage an issuer's existing enrolment systems such as an Internet Banking logon for first-time enrolment of cardholders.

3-D Secure is based upon PKI and the issuer's ACS has to sign authentication responses sent to 3-D Secure merchant. For this reason, the Issuer will need to apply for a digital certificate from a Visa certificate authority and configure their ACS to communicate with the Visa Directory.

3-D Secure gives the Issuer complete discretion to authenticate their cardholders using a browser (minimum authentication criteria), cardholder applet, server-based eWallet, digital certificate, chip card or biometric device. 3-D Secure only

¹³ Issuers who distributed SET wallets will not be able to leverage their investment for either Visa 3-D Secure or MasterCard SPA.

mandates the issuer to provide client software to their cardholders to support chip authentication¹⁴. The primary focus of this paper is to examine the default authentication mechanism, which is username and password.

In order to support MasterCard SPA each Issuer is required to sign up to a SPA Server provided by a managed service or run a SPA Server in-house. A SPA Server is required to manage communication with cardholder SPA applets and generate the Accountholder Authentication Value (AAV) which is sent to the cardholder applet for entry into the merchant's website. The SPA server is also responsible for matching the AAV received from the acquirer with the AAV generated for the particular transaction in order to verify the transaction has been authenticated.

Regardless of whether the Issuer uses a managed service or in-house SPA Server they will be required to implement a process/interface for regularly loading their cardholder data to the SPA Server and a process/interface for allowing the SPA server to authenticate their cardholders during SPA registration. The issuer will also require an interface to their card system/switch to allow the SPA server to authenticate cardholders during ensuing SPA transactions.

SPA gives the Issuer discretion to authenticate their cardholders using a cardholder applet (minimum authentication criteria), server-based eWallet, digital certificate, chip card or biometric device. SPA mandates the issuer to provide downloadable client software for all SPA transactions. In order to support SPA the issuer may provide a cardholder applet download facility from their Internet Banking site.

Supporting Cardholders

Under Visa 3-D Secure the issuer will have to provide sufficient instruction for cardholders to enroll for 3-D Secure and treat their password confidentially. The issuer will also have to educate them of the importance of the personal assurance message. Under 3-D Secure the personal assurance message is the only safeguard that a cardholder has against a "man-in-the-middle" attack initiated by a fraudulent merchant who "mimics" the issuer's authentication page in order to capture the cardholder's password. This is a basic limitation of an authentication protocol that uses a standard browser and it is only a matter of time before it is exploited. It is also likely that the issuer will field support calls from cardholders that experience "time-outs" due to the numerous Internet messages that need to be exchanged during a 3-D Secure transaction.

MasterCard SPA uses a more evolved technology for the cardholder in the form of a cardholder applet. While it provides a faster online shopping experience and greater online security benefits it will inevitably introduce some compatibility problems with older browsers and operating systems. The most important thing to educate SPA cardholders about is how to register for SPA for the first time and to make it easy for cardholders to access their issuer's SPA applet homepage so that they can download subsequent applets at different computer locations. Cardholders must be taught to identify the presence of their cardholder applet as a "security blanket" for online payment transactions.

¹⁴ If the issuer wants to support chip they will have to purchase hardware security modules (HSM) which are capable of decrypting the cryptograms at the issuer's ACS and they will also have to distribute card readers to their cardholders.

Issuer Reporting

There is a range of reporting which can be provided to issuers for both Visa 3-D Secure and MasterCard SPA in relation to their cardholders, transactions and usage.

Under 3-D Secure the issuer will receive basic reporting on the transaction status of each 3-D Secure transaction. This will include items such as the date, purchase price, credit card number and authentication status.

Under MasterCard SPA the issuer receives more comprehensive reporting as the SPA protocol goes beyond simple authentication to introduce concepts of “transactional integrity”. This means the issuer has access to information on split shipment purchases, recurring transactions etc.



The screenshot displays the 'ActiveAccess Administration' web interface. The top navigation bar includes 'Settings', 'Users', 'Certificates', 'Report', 'Change Password', 'Version 1.0.0', and 'Logout'. A left-hand menu lists 'General Settings', 'Restart Server', 'Database Settings', 'Time-out Settings', 'Extensions', 'Plug-ins', 'AHS Servers', and 'Servers'. The main content area is titled 'General Settings' and contains the following configuration fields:

Visa server port :	<input type="text" value="8730"/>	*
User server port :	<input type="text" value="4346"/>	*
Administration port (public) :	<input type="text" value="4347"/>	*
Administration port (private) :	<input type="text" value="4348"/>	*
Wrong password attempt :	<input type="text" value="0"/>	*
Wrong password lock time :	<input type="text" value="0"/>	*(milliseconds)

An 'Apply' button is located at the bottom right of the settings area.

An example of the administration module of an issuer authentication server, ActiveAccess.

A Comparison of the Merchant Experience under Visa 3-D Secure and MasterCard SPA

It has already taken a concerted effort just to connect the merchants to Internet payment gateways provided by acquirers or third party processors for online credit card authorizations. Merchants now need to perform additional work if they wish to support authentication standards from both Visa and MasterCard.

Merchants are always loath to change their existing systems, especially if it involves integration and additional costs. Some online merchants have a fraud problem for which they are liable under the current system. These merchants will be keen to introduce support for authentication standards, even if it doesn't immediately make a major difference to their problem due to slow registration of cardholders for the new system.¹⁵ Other merchants will delay upgrading their sites for as long as possible.

The comparison for merchants will look at the integration process, the reporting process and ongoing maintenance.

Merchant Integration Process

In order to support the 3-D Secure protocol each merchant is required to embed a 3-D Secure merchant plug-in (MPI) in their website or register with a 3-D Secure Merchant server provided as a managed-service by their acquirer or third party processor. The merchant will need to apply for a digital certificate from a certificate authority and have their MPI or Merchant Server configured to communicate with the Visa Directory. The merchant must also alter their existing shopping cart process to communicate with the 3-D Secure MPI or 3-D Secure Merchant Server at the end of the shopping cart process.



The screenshot shows the 'ActiveMerchant Administration' interface. The top navigation bar includes 'Settings', 'Merchants', 'Certificates', and 'Report'. The 'General Settings' section is active, displaying a table of configuration options for the 3-D Secure merchant server. The table includes fields for version, cache expiry, connection and response timeouts, IP/DNS address, and various ports. An 'Apply' button is located at the bottom right of the settings area.

Field	Value	Unit/Notes
3-D Secure version :	0.7	
Cache expiry period :	24	(hours)
Connection time-out :	300	(seconds) *
Response time-out :	300	(seconds) *
IP/DNS address :	192.168.0.71	*
MPI port :	4343	*
Administration port (public) :	4344	*
Administration port (private) :	4345	*

An example of the administration section of a 3-D Secure Merchant Server, ActiveMerchant.

¹⁵ Visa is predicting that only 6% of their cardholders will register for 3-D Secure by the end of 2002.

The timeframe for the merchant to implement a 3-D Secure merchant plug-in is difficult to estimate and will vary greatly based upon the complexity of the merchant's online system. It is important to note that implementation of 3-D Secure will require code-level changes to the merchant's shopping cart process. Some merchants will have in-house expertise and will be able to integrate themselves while others will have to employ third parties to perform the integration for them. A senior developer with intimate knowledge of an online merchant's site could feasibly implement a merchant plug-in in a couple of days. However, the early experience of merchants in 3-D Secure pilots is that it has taken 2-3 weeks to implement a 3-D Secure Merchant plug-in. Larger merchants who have rigorous acceptance testing procedures before changes are moved to their production machines obviously take longer to migrate a 3-D Secure merchant plug-in to their 'live' site.

The major cost to a merchant is not the merchant plug-in or even the technical implementation process. The merchant's main problems are administrative and procedural. Visa's 3-D Secure system is reliant on PKI and the merchant's 3-D Secure plug-in must be able to decrypt authentication messages received from the issuer which have been signed with a public key. For this reason the merchant has to apply for a digital certificate from a recognized Visa authority. The merchant will also have to configure their merchant plug-in to communicate with a test environment prior to going 'live'. The merchant will also have to update their website to notify their customers that they can participate in "Verified by Visa".

3-D Secure does not require the merchant to alter their existing payment gateway interface with their acquirer. Under 3-D Secure, authentication is a separate process from authorization, which happens prior to authorization. The merchant is the pivotal point in the transition from authentication processes to authorization processes. In contrast, MasterCard SPA treats authentication and authorization as a single process, which pivots around the issuer.

The fact that the normal acquiring process is not affected under Visa 3-D Secure is positive from the perspective of implementation as it does not require acquirers and third party processors to upgrade their payment gateways and the merchant interfaces to their payment gateways. This is not to say that the requirement for upgrading a merchant's interface to a payment gateway is not uncommon. For example, in 2001 merchants had to upgrade their payment gateway interface to support Visa's eCommerce indicator.

Upgrading the merchant's payment gateway plug-in to support SPA is not a major change and is probably easier than implementation of a 3-D Secure merchant plug-in. Under 3-D Secure, merchants which already have a plug-in from their payment gateway to process payments may now have two plug-ins on their merchant server – one for authentication and one for authorization through their payment gateway provider. Some payment gateway providers will combine these two plug-ins into a single plug-in for the merchant. Other payment gateway providers will provide a managed 3-D secure merchant service eliminating the need for the merchant to install an authentication plug-in at all.

Visa implemented a number of merchants as part of its 3-D Secure pilot program. The response of merchants was varied. "Merchants who like 3-D Secure's guaranteed payment offering think the system needs revamping before it can be implemented on a large scale."¹⁶ One merchant interviewed by The Asian Banker said technical failure – especially for card verification – is one of the major

¹⁶ Visa prepares 3-D Secure for mass adoption November 30, 2001, Asian Banker

hurdles. The most common failure encountered during the pilot project was the disruption in connection that made the merchant unable to process customers' orders, thus requiring customers to redo the transaction. The merchant decided to temporarily disable 3-D Secure to shield itself from a negative customer experience.¹⁷

The introduction of 3-D Secure is a challenge for merchants. However, the newer vendors of 3-D Secure merchant solutions have rectified many of the problems experienced by merchants deploying the first 3-D Secure Plug-in used in Visa's pilots. The second generation of 3-D Secure merchant plug-ins and merchant servers are designed to minimize the impact on merchants and should result in an easier integration process.

In order to support MasterCard SPA the online merchant must embed hidden UCAF fields in their website which are capable of providing information to a cardholder applet and receiving an Accountholder Authentication Value (AAV) from the cardholder applet. The merchant must pass this AAV to their acquirer. This will typically involve the merchant altering their existing payment gateway interface so that the AAV can be sent to their acquirer. MasterCard SPA does not have any reliance on PKI or certificate authorities, which means the merchant does not need to go through a digital certificate application process. MasterCard SPA is a de-centralized system, which does not require the merchant to embed an authentication plug-in to communicate with a centralized Internet directory.

Under SPA, the merchant has the option of providing a transaction reference number to the cardholder applet, which can be checked once the security token is received from the SPA applet. This can provide extra protection against "man-in-the-middle" attacks by ensuring that the original customer is still the purchaser and has not been replaced by a fraudulent imposter during the purchase process. This is not a mandatory requirement for the merchant but would require additional coding to support it and use the capability productively.

Some merchant websites have already implemented 'single-click' purchasing systems for their repeat customers. In order to support SPA these sites must implement an AAV Transfer page. The use of an AAV transfer page does not alter the single-click purchasing experience for the customer and is automatically managed by the cardholder applet. This resolves the problem some online merchants, such as Amazon, have had with authentication schemes which add friction to their single-click purchasing.

Merchant Reporting

Online merchants generally receive their transaction reporting through their online payment gateway. Due to the separation of the authentication and authorization processes under 3-D Secure, merchants may not be able to go to one source to get consolidated reporting of all their transactions with indication as to which transactions were 3-D Secure transactions. The merchant will get reporting on all their transactions through their payment gateway but will get reporting on which transactions were 3-D Secure through their merchant plug-in. The only instance where common reporting is possible is where the merchant uses a 3-D Secure Merchant Server provided as a managed service by their payment gateway and the payment gateway has integrated 3-D Secure reporting with their standard transaction reporting.

¹⁷ Visa prepares 3-D Secure for mass adoption November 30, 2001, Asian Banker

Under MasterCard SPA the payment gateway at the acquirer or third party processor will need to be upgraded to accept the AAV. For this reason the payment gateway operator will be able to provide common reporting of all transactions and will be able to provide integrated reporting and searching on MasterCard SPA transactions. This will mean that merchants will be able to perform all their transaction reporting and management in a single location.

Ongoing Maintenance

The merchant may have to upgrade their 3-D Secure merchant plug-in in the future if Visa issues a subsequent release of the 3-D Secure protocol specification which is not compatible with earlier releases. Merchants may want to upgrade their merchant plug-ins if they wish to support different forms of mCommerce. Visa 3-D Secure uses extensive XML messaging which has actually proved too cumbersome for mobile WAP devices to support. As a result, Visa has released a new “condensed” form of messaging for communications with WAP devices. Furthermore, Visa 3-D Secure was not originally designed to support Mobile SMS or Voice Devices. Visa is introducing a new transaction flow for 3-D Secure transactions sent over SMS and Voice Devices. Due to 3-D Secure’s reliance on PKI, the merchant will also have to implement procedures for renewing their digital certificates when they expire.

The merchant does not have to embed an authentication plug-in in their site under MasterCard SPA, which means there are no software upgrade and implementation issues when newer versions of MasterCard SPA are released. However, some vendors of 3-D Secure merchant solutions have also added support for SPA within the same solution. MasterCard SPA does not have any reliance on digital certificates, which means there are no ongoing requirements to renew certificates or re-apply for certificates in the case of a machine crash.

A Comparison of the Acquirer Experience under Visa 3-D Secure and MasterCard SPA

The comparison for acquirers will look at technology implementation at the acquirer, the acquirer's role in supporting merchant upgrades and reporting for the acquirer.

Technology Implementation

The level of technology implementation required for an acquirer under 3-D Secure will depend on the acquirer's current level of support for Internet payment processing. It is also assumed that the acquirer has already implemented an Internet Payment Gateway for standard SSL credit card authorizations.¹⁸ It is also assumed that all acquirers have now implemented Visa's electronic commerce indicator. 3-D Secure does not require any additional changes or upgrades to be made to VisaNet.

There are currently two models for acquiring Internet transactions from online merchants. One involves the acquirer providing software plug-in to the merchant, which is designed to communicate with the Internet Payment Gateway over the Internet. This is generally referred to as the "API" model. The other model involves the merchant using hyperlinks to redirect their customers to the payment gateway site, hosted by the acquirer or third party processor, for entry of the customer's credit card details. This is generally referred to as the "URL" model.

If an acquirer is using the URL model they will need to run a 3-D Secure Merchant Server in addition to their existing Internet Payment Gateway system. In this situation the acquirer runs a 3-D Secure Merchant Service on behalf of a number of merchants. The acquirer will assume all initial configuration and maintenance responsibilities for enabling and maintaining 3-D Secure capability for the merchants including certificate management.

If an acquirer is using an API model they can either distribute a 3-D Secure merchant plug-in to their merchants or provide a 3-D Secure Merchant Service. A 3-D Secure Managed Service is the preferred model as it reduces the effort required by the merchant to become 3-D Secure enabled. A 3-D Secure Managed Service is particularly useful if an acquirer supports both URL and API connection models to their payment gateway.

However, if the acquirer decides to distribute a 3-D Secure merchant plug-in this will form a second plug-in which they will require their merchants to embed in their website. (This is additional to the payment gateway plug-in used for the API model.) Alternatively, the acquirer can integrate their existing payment gateway plug-in with a 3-D Secure merchant plug-in and provide one new plug-in to their merchants to replace the payment gateway plug-in which the merchant already has in place. Under both of these situations it will be the merchant's responsibility for integrating the plug-in, applying for a digital certificate from a Visa-approved certificate authority and configuring their merchant plug-in to communicate with the Visa directory.

¹⁸ Unfortunately, acquirers that have implemented a SET Internet Payment Gateway will not be able to leverage their existing infrastructure to support 3-D Secure.

It is expected that most payment gateways, which use an API processing model, will also provide a 3-D Secure Merchant Service to eliminate the need for an additional plug-in to be deployed in the merchant's local environment. Under this model the merchant keeps their existing payment gateway plug-in and simply sends a request to the 3-D Secure Merchant Service prior to the normal acquiring process. This effectively hides the details of the 3-D Secure process, such as certificate management, from the merchant. It also maintains the segregation of the authentication and authorization processes which is inherent in the 3-D Secure architecture.

For an acquirer to run a 3-D Secure Merchant Service they do not have to go to the extra effort of integrating a source development kit (SDK) version of the Merchant Server with their Internet Payment Gateway. This is a complex and time consuming process which requires additional coding by the acquirer and introduces further complexity every time they receive an upgrade of the 3-D Secure Merchant Server from their supplier. Acquirers can simply run the 3-D Secure Merchant Server in parallel with their existing payment gateway and use a common data repository for transaction records. This approach also allows the acquirer to scale out the 3-D Secure Merchant Service by load balancing multiple 3-D Secure Merchant servers if they have significant transaction volumes.

All MasterCard's acquirers are going to have to implement the upgrade to Banknet to support transmission of the AAV through the UCAF field. This is similar to the process, which Visa just went through to introduce the electronic commerce indicator on Visanet. If the Banknet upgrade is a slow process it will delay the rollout of MasterCard SPA and may give Visa an insurmountable lead in introducing 3-D Secure. Under MasterCard SPA the level of technology implementation required for an acquirer will also depend on the acquirer's current model for supporting Internet payment processing.

If an acquirer is using an API model they will be required to distribute a new payment gateway plug-in to their merchants to replace the existing merchant plug-in. The implementation of this new plug-in will be the merchant's responsibility but will be virtually identical to the plug-in it is replacing. The acquirer may assist the merchant in this process if it chooses to do so but this is basically a patch to the existing payment gateway process, which allows the merchant to send the AAV to the Internet Payment Gateway.

The acquirer is also going to be required to patch their existing Internet Payment Gateway so that it can accept the AAV from the merchant and then pass this to MasterCard's Banknet so it can be sent through the UCAF field. Obviously, this patch to the Internet Payment Gateway cannot be performed prior to the upgrade of the UCAF field on Banknet.

If an acquirer is using the URL model they may need to upgrade the pages of their Internet Payment Gateway which are displayed to cardholders following redirection from the merchant website. Depending on the individual implementation, these pages may need to support the provision of "hidden" UCAF fields, which can be read and populated by a cardholder applet. The AAV captured from the page displayed to the cardholder then needs to be passed to Banknet in the same manner as the AAV received from a merchant plug-in under the API model.

Supporting Merchant Upgrades

It is likely that in most cases the acquirer is going to assist the merchant in upgrading their eCommerce sites to support Visa 3-D Secure and/or MasterCard SPA. The acquirer is first going to have to educate the merchant on the benefits of participating in Visa 3-D Secure and/or MasterCard SPA.

The merchant support required for upgrading merchants using a URL model does not directly impact the merchant from a technology perspective. It will, however, have an operational impact on the merchant.

In order to support an API merchant upgrading to 3-D Secure the acquirer may have to distribute a 3-D Secure merchant plug-in to the merchant. The acquirer may train support personnel to assist merchants implementing the 3-D Secure merchant plug-in and may want to provide a test facility to ease the implementation and configuration of the 3-D Secure merchant plug-in by the merchant. The acquirer may also implement a process to assist merchants in applying for, installing and renewing digital certificates.

In order to support an API merchant upgrading to MasterCard SPA the acquirer will have to distribute a new payment gateway plug-in to the merchant. The acquirer may also want to supply information on changes required to the merchant's website to support SPA-UCAF. Due to the distributed nature of MasterCard SPA, the testing required for a merchant to become SPA compliant does not require access to an external test facility. However, it is expected that the acquirer will provide a cardholder applet to the merchant so that the merchant can test the implementation of MasterCard SPA on their website from the perspective of a cardholder.

Acquirer Reporting

Under 3-D Secure the acquirer will have different levels of reporting depending on whether they are hosting a 3-D Secure Merchant Server or distributing 3-D Secure Merchant Plug-ins to their merchants. If the acquirer is running a 3-D Secure Merchant Server they will have full reporting on 3-D Secure transactions performed by their merchants. If the acquirer is distributing 3-D Secure Merchant Plug-ins for local implementation at merchant sites they will not receive any reporting on whether a particular transaction was a 3-D Secure transaction. The acquirer's reporting for a particular transaction will only show whether it was an eCommerce transaction by virtue of the electronic commerce indicator.

Under MasterCard SPA, the acquirer will receive the authentication status of all transactions, which pass through their Internet Payment Gateway. MasterCard SPA transactions will have an AAV attached to them and will have the brand set to MasterCard. Maestro transactions will not necessarily have an AAV attached to them (as this is optional under Maestro's online debit standard) but will have the brand set to Maestro.

ActivePayment Pro Administration - Admin [Logout](#)

14 November, 2001 **Transactions** Payments Administration OCV Server Developers

Transactions for:

Search

Daily

Weekly

Monthly

Analysis

Report

Transaction Search

Type:

Status:

Credit Card Type:

Credit Card Number: (no space)

Transaction Number:

Order Number:

Search By:

From: To:

An example of the administration section of an Internet Payment Gateway, ActivePayment.

A Comparison of the Visa 3-D Secure and MasterCard SPA Architecture

This architectural comparison will examine the structure, the transaction flows, performance, reliability, scalability, expandability and enforceability of the standards.

CENTRALIZED OR DISTRIBUTED?

Visa 3-D Secure has a centralized structure based around Visa's new Internet Directory service. The Visa Directory is simply a server, which resides on the Internet and maps the location of Issuer Access Control Servers to Issuer BIN numbers. Its function is to receive 3-D secure participation requests from merchants, route these to the relevant issuers, receive the responses from the issuers, and then reply to the merchants.

In reality, there will be multiple Visa Directories residing on the Internet, which have identical content and functionality for load balancing and redundancy purposes. However, the existence of a Visa Directory means that Visa will intermediate in all Internet transactions twice – once through the Visa Directory on the Internet and once through the private network, VisaNet which links acquirers with Issuers.

This begs the question “is this the first step in the transition of all payments to Internet infrastructure and a move away from proprietary payment networks?” The use of proprietary payment networks by financial institutions is currently very expensive for the financial institutions due to the fees that must be paid to service providers that maintain the proprietary networks. The Internet is a cheap and efficient global infrastructure, which is fast moving towards carrier-grade quality. Many people have speculated that financial institutions could create a “federated” payment network using Internet infrastructure in order to reduce the costs of dealing with proprietary payment networks such as VisaNet, Banknet and SWIFT. If Visa were concerned that VisaNet may be superceded by a competing Internet-based infrastructure then it would be a strategic defensive play to introduce an Internet-based Visa Directory. This would protect Visa's role as an intermediary in all Visa transactions in the future.

Visa has also introduced an Authentication History server. Each Issuer's Access Control Server is required to send a record of all authentications to Visa's Authentication History server. This is a totally new concept for Visa, which will give Visa an insight into the nature of Internet transactions performed by their members. While Visa will not divulge this information between its members, Visa itself will be able to perform data mining on this data for its own purposes.

However, the introduction of the Visa Directory is inefficient from a messaging perspective. The Visa Directory introduces a number of extra messages in the transaction flow, which have to be sent over the Internet in order to effect an authenticated payment transaction. Each of these messages is subject to bandwidth limitations and network delay, which could impact performance. In a worse case scenario it could result in a time-out forcing the customer to redo the entire transaction.

The introduction of the Visa Directory increases the complexity of the online payment process. Quite often increased complexity leads to multiple points of

failure and reduced reliability. When people first see the convoluted transaction flow for 3-D Secure they are instantly shocked at its complexity. Furthermore, the centralized Visa Directories may become hacker targets for “denial-of-service” attacks.

The Visa 3-D Secure architecture was created for a browser-based world. This is evident in the way the 3-D Secure uses browser re-directs extensively during its transaction flow. This has posed some problems in extending the 3-D Secure protocol to chip and mobile purchasing. Visa has already had to modify their protocol a number of times to cater for different authentication methods and device support. Different authentication methods such as chip and mobile devices such as WAP and SMS rendered the original browser-based architecture redundant. Visa has had to introduce client software in order to support chip authentication, a condensed messaging format for WAP devices and a new transaction flow for SMS/IVR payments adding complexity to the Issuer’s access control server. A system originally designed for a browser-based world does not neatly fit into a payment model based upon session-less messaging.

The Internet, as we all know, is a distributed network, which has not responded well to attempts to mandate standards or introduce centralization in the past. The failure of the original Microsoft Network to the failure of the ECML standard are constant reminders of the futility of past attempts to control the evolution of the Internet. If Visa were to succeed in upgrading every eCommerce site on the Internet, every Issuer’s infrastructure and enrolling every cardholder in 3-D Secure it would be a significant achievement. In introducing a centralized architecture for online payment transactions Visa is promoting a new strategy, which if successful, will guarantee its existence in the online transaction continuum.

In contrast to Visa’s approach, MasterCard SPA is built around a distributed payment architecture. MasterCard has not introduced a centralized directory and does not directly participate in every Internet transaction. In this way MasterCard is promoting a standard which more closely resembles the “federated” architecture of transactions initiated from POS terminals in the real world.

MasterCard has committed to upgrading its Banknet to support the passing of authentication data through the UCAF field. This means that MasterCard will only continue to intermedate once in the online transaction process through Banknet. This is equivalent to the same manner in which it intermediates in real world transactions.

By supporting a cardholder applet, MasterCard is gaining valuable real estate on the desktops of cardholders. MasterCard is actually adding value to cardholders by reducing the time required to make online purchases. MasterCard has also given their issuers a tool that can be used for both branding and the delivery of additional financial services to cardholders. This could form an effective insurance policy against attempts by financial institutions to create an Internet-based payment infrastructure, which competes with Banknet. MasterCard has also attempted to mitigate this possibility by joining the Liberty Alliance – something that the advocates of centralization such as Microsoft - are yet to do.

Support for Compliance Mandates

At an architectural level it is interesting to examine Visa 3-D Secure and MasterCard SPA from the perspective of enforcing mandatory compliance. Under both schemes all cardholders, merchants, issuers and possibly acquirers need to be participating for an authenticated payment to proceed.

Under 3-D Secure, authentication is a separate process from authorization that happens prior to authorization. The merchant is the pivotal point in the transition from the authentication process to the authorization process. Using the merchant as the transition point could retard the process of a mandatory rollout of 3-D Secure for all Internet transactions. For example, a merchant can implement a 3-D Secure Merchant Plug-in but can continue to accept standard (i.e. not Visa 3-D Secure) transactions indefinitely. Furthermore, a merchant could even “short-circuit” Visa 3-D Secure transactions and send enrolled 3-D Secure transactions to their acquirer as non-enrolled 3-D Secure transactions. The merchant’s acquirer has no ability to verify whether a transaction coming in was from a registered 3-D Secure cardholder or not. The merchant will never want to move to a scenario where they deny any transactions which are not Visa 3-D Secure as this is essentially business which they are turning down. Even if Visa mandates all issuers and acquirers to deploy 3-D Secure the rollout could be thwarted by merchants that choose to continue to accept non 3-D Secure transactions and 3-D Secure transactions which fail the 3-D Secure authentication process. The 3-D Secure architecture is not designed to assist in a mandatory rollout of the 3-D Secure protocol.

In contrast, MasterCard SPA treats authentication and authorization as a single process, which pivots around the issuer. Using the Issuer as the single point for determination of authentication and authorization gives an architectural advantage to MasterCard if they decide to introduce a SPA mandate for Internet transactions. For example, an issuer that implements SPA can choose to reject all Internet transactions, which are not accompanied by an AAV. The issuer can actually check the validity of the AAV as the issuer originally generated it. This opens the possibility for an issuer to dictate that both customers and merchants must use SPA to process an Internet transaction if they want authorizations to be successful.

MasterCard SPA cannot be “short-circuited” by merchants who are reluctant to deny transactions, which are not registered for SPA. Under SPA the merchant has no control over the authentication process and the transition to the authorization process. The card companies have direct relationships with the issuers and acquirers, which is of assistance in enforcing compliance with new standards. However, the card companies do not have direct relationships with the merchant community.

INTEROPERABILITY WITH OTHER CARD COMPANIES

MasterCard is not mandating that Issuer’s provide their Authentication records to a centralized service. This means that MasterCard has created an open infrastructure, which could potentially be used by other card organizations. In contrast, any card organization that used Visa’s infrastructure would need to directly provide Visa with their BIN numbers. Any card organization utilizing Visa’s infrastructure would indirectly be giving Visa access to its online transaction volumes, the location of its online purchases and the card numbers of its online users.

The use of a cardholder applet reduces the number of messages that need to be sent over the Internet in order to effect an authenticated payment transaction. This creates the most efficient authentication architecture possible within a distributed network environment. MasterCard is effectively translating the real world payment process to the online payment process but utilizing the instant communication between a cardholder and their issuer made possible by a realtime connection. The Accountholder Authentication Value used in a MasterCard SPA transaction is really the digital replacement for the signature provided by the cardholder at the point-of-sale in a real world transaction. MasterCard SPA has a simple transaction flow allowing authentication and authorization to occur in a single process managed by the Issuer. In contrast, Visa's architecture treats authentication as a separate process that occurs prior to authorization and which is managed by the merchant prior to authorization being managed by the issuer.

The operation of MasterCard SPA is not intrinsically linked to the operation of a web-browser. The advantage of this approach is that the use of a cardholder applet gives flexibility to perform authentication on payment platforms, which do not natively run a web browser. These platforms do have to be capable of supporting an applet but can leverage other forms of messaging than browser re-directs without creating a separate transaction flow for the online payment process.

It seems that MasterCard has recognized that they do not have the ability to impose a centralized system upon the distributed architecture of the Internet. In order for them to make MasterCard SPA a success they have designed a system which works within the general principles of the Internet and can more easily evolve in concert with the evolution of the Internet itself.

In order to sum up the differences in architecture between Visa 3-D Secure and MasterCard SPA we can make the following statements.

- 1) A cardholder under Visa 3-D Secure has to pass the examination of the merchant, who colludes with the cardholder's issuer, before he/she is allowed to proceed with an online purchase.
- 2) A cardholder under MasterCard SPA enlists the help of his/her issuer in order to ensure that purchases he/she makes with merchants are protected against fraud.

A Comparison of Visa 3-D Secure and MasterCard SPA Security Architecture

It is possible to investigate some of the different approaches that have been taken to security in the 3-D Secure and MasterCard standards from an architectural perspective. However, it is important to note that the actual implementations of the standards by technology vendors may differ.

The major difference between the 3-D Secure and SPA security architectures is that under 3-D Secure, authentication is a process that is independent of authorization and precedes authorization. The merchant, or more specifically the 3-D Secure merchant plug-in or merchant server, is the pivotal point in the transition from the authentication process to the authorization process. In contrast, under SPA authentication and authorization are part of the same process with the issuer as the pivotal point.

From a security perspective it could be argued that a merchant eCommerce server is not an appropriate place for an online authentication process to conclude. A fraudulent merchant could bypass, emulate or hack the functions of the 3-D Secure merchant plug-in to suit their own malicious purposes. A fraudulent merchant that does not want to participate in 3-D Secure could subvert the authentication process entirely and accept 3-D Secure registered cards without sending them to the 3-D Secure Merchant plug-in. In a worse case scenario, the merchant could “mock-up” the issuer’s “Verified by Visa” screen in order to capture the cardholder’s 3-D Secure password. This would then allow the merchant to fraudulently make “authenticated transactions” at other sites. Visa recognized this problem and attempted to alleviate the situation by introducing the “personal assurance message” into the authentication page. However, this can be easily defeated using simple “screenscraping” techniques. There is also the additional danger that people will forget to check the personal assurance message and enter their password into fraudulent sites.

The Issuer’s server, which is where authentication is performed under MasterCard SPA, is a more secure environment for the authentication process to conclude due to the “trusted” nature of financial institutions. This does not mean that authentication under SPA is intrinsically more secure than 3-D Secure as the issuer’s environment may be subject to internal attack from rogue system administrators. For this reason it will be the SPA implementer’s responsibility to shield the issuer system from both internal and external attack. However, the fact that the merchant does not have any control over the transition from the authentication process to the authorization process under SPA is a positive.

Another major difference in security architecture between Visa 3-D Secure and MasterCard SPA is in the area of digital certificates. Visa has had to resort to the use of Public Key Infrastructure in order to bolster message integrity in the 3-D Secure transaction flow between the Issuer and the merchant. 3-D Secure only mandates the use of digital certificates by issuers and merchants, which is not as great a burden as SET where cardholders and acquirers also needed digital certificates. However, the use of PKI increases the administrative overheads of a system such as 3-D Secure and introduces further complexity. For example, there are requirements in 3-D Secure to inter-operate (cross certify) with multi-vendor CA environments. MasterCard SPA provides logic to the cardholder in the form of a cardholder applet. This means the Accountholder Authentication Value (AAV) can be transmitted to the merchant in encrypted form removing the need to rely on digital certificates for confidentiality.

Session management is an interesting point of comparison between the two standards. Under 3-D Secure there is effectively no session management for the cardholder. This is due to the stateless nature of communication between the issuer and the cardholder. The cardholder has no way of initiating a secure session directly with their issuer under 3-D Secure and can only respond to their issuer when a merchant asks the issuer to check the cardholder's password. This means that the cardholder has to re-authenticate for every purchase they make in a single shopping session. Visa's approach to authentication contrasts with that of Microsoft, AOL, Liberty Alliance and MasterCard SPA who are all emphasizing "single sign-on" services in order to reduce the friction currently experienced in online purchasing across multiple sites. The use of a cardholder applet under MasterCard SPA allows the customer to authenticate with their issuer and maintain a session with the issuer's system. This session management can use a method that is proprietary to the individual issuer. All Visa's communication under 3-D Secure uses standard browser redirects which may be open to "hijacking" or "spoofing".

Both Visa and MasterCard are relying on 128-bit SSL as the underlying protocol for maintaining integrity and confidentiality of information during transmission. Neither standard mandates the use of any other cryptographic algorithms although stronger forms of encryption are likely to be used in the issuer systems.

Another difference between 3-D Secure and SPA arises in the area 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.

Visa does not currently have a model for "transaction authentication" under 3-D Secure. The physical separation of the authentication process from the authorization process under 3-D Secure will make it difficult for Visa to extend 3-D Secure to support transactional integrity. This is not such a problem for online credit card transactions but has greater importance for online debit transactions, as there is no chargeback process for pure online debit transactions.

MasterCard or more specifically, Maestro has extended SPA beyond simple payer authentication to provide an additional level of "transaction authentication". This can ensure that the original transaction amount authorized by the customer is not exceeded in additional charges applied to the cardholder's account in subsequent transactions, which form part of an initial purchase.

Conclusion

Visa 3-D Secure and MasterCard SPA have set out to achieve the same outcome, which is the introduction of authentication for online payment transactions. We must remember that the introduction of online authentication is a positive step for online payment transactions and eCommerce in general.

We have examined some of the strengths and weaknesses of Visa 3-D Secure and MasterCard SPA from the perspectives of the participants – Cardholders, issuers, merchants and acquirers. We have also investigated some of the major differences from a general architecture and security architecture perspective. However, it must be made clear that the wide scope of each of these standards means it is not possible to adequately cover every aspect of these standards in an industry whitepaper.

From a technology perspective, MasterCard has attempted to “raise the bar” by introducing newer and more demanding technologies into the SPA standard. Cardholder applets with session management, automatic form-filling, transaction-specific security tokens and realtime transaction matching at the issuer are all high technology solutions. MasterCard has the promise of an exciting online future but it is yet to be seen whether the market is ready for these technologies.

Visa has introduced a more basic technology solution, which only provides authentication to the cardholder and actually creates more friction in the online purchasing process. Visa has resorted to using PKI for security and extensive use of browser redirects, which are an inefficient way of processing transactions in networks that are subject to delays and timeouts. The real question with Visa 3-D Secure is whether the benefit of cardholder authentication outweighs the extra steps and time it adds to the online purchasing process.

Visa is introducing a centralized architecture for online payment transactions. This is something that may be of concern to their member banks from a privacy perspective. It also makes the entire 3-D Secure environment a target for hackers. It would be a remarkable achievement for Visa to make 3-D Secure ubiquitous as no other organization (including Microsoft) has yet been able to bring structure and centralization to the distributed and often chaotic evolution of the Internet.

MasterCard has decided to create a decentralized standard, which leverages the distributed architecture of the Internet with client-server applications. SPA has a consistent and robust security model, which could form the foundation for a range of stronger authentication technologies and wider device support in the future.

Based upon technical merit, the general industry consensus is that MasterCard has created a more elegant standard for online payments. However, it is not always the most elegant standard that achieves widespread adoption. Visa has a first mover advantage and is investing heavily in piloting and marketing 3-D Secure. Both Visa and MasterCard are facing competition for online authentication from Microsoft, AOL and the Liberty Alliance. There is a chance that neither Visa nor MasterCard will dictate the standard for online authentication.

If either Visa 3-D Secure or MasterCard SPA are successful in the market it will be the merchants, issuers, acquirers and card organizations which stand to benefit.

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 SPA 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

BIN The first 6 numbers of a credit card number which identify the issuer of the card

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.

Cardholder Applet A software plug-in which is installed on the cardholder's machine in order to secure online purchases.

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.

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.

SET Secure Electronic Transaction. A certificate based payment and authentication standard developed by Visa and MasterCard in 1996.

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.

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



GPayments
Innovate - Empower - Adapt

www.gpayments.com.au