GPayments
Innovate - Empower - Adapt

Authentication and Payment Solutions

An Introduction to Authentication
The solution to online credit card fraud

At a glance

Through a series of questions and answers this fact sheet describes the problems surrounding authentication and provides a brief overview of authentication from the 3-D Secure and SPA perspective.

GPayments Pty Ltd
Suite 201 Building C
14 Rodborough Road
Frenchs Forest NSW 2086
Australia

T: +612 9453 5411
E: info@gpayments.com
W: www.gpayments.com

Authentication – The solution to online credit card fraud

Do we have a problem?

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 integrity.

What is the real problem?

The real problem, which some don't 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.

What is this Authentication?

Authentication is the verification of a credit card owner made during a credit card purchase. In the physical world authentication is achieved through a physical signature which is manually checked at the point of sale.

Why do we need Authentication?

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.

Whose problem is it?

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.

Has there been a solution for this problem?

The credit card companies, namely Visa and MasterCard, realized as far back as 1996 that a means of authenticating customers on the Internet was necessary. They decided to develop a common standard called Secure Electronic Transaction (SET) to solve the problem.

SET was a technological masterpiece, far too complex and difficult to explain here. SET involved every cardholder, every merchant, and every bank receiving a digital certificate. Unfortunately it was also far too costly to implement and it therefore never gained widespread market acceptance.

Where are we at now?

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. Even today, the amount of online credit card fraud is very small in comparison with fraud in the real world. However, if eCommerce keeps expanding at the current rate it will become a major problem in the future. Visa and MasterCard know this all too well.

What is being done about this?

In 2001, five years after introducing SET, the major credit card companies have gone back to the drawing board to tackle payer authentication. This time, rather than working together, Visa and MasterCard have decided to introduce their own authentication standards for online transactions. Visa has introduced a system called 3-D Secure and MasterCard has introduced a system called Secure Payment Application (SPA).

How do they work?

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 in order to authenticate themselves for online purchases. In most cases customers will be provided with a digital "Wallet" which captures the username and password during the purchase and in real-time requests an equivalent of a "digital signature" from the bank. This one-time "signature" is then provided to the merchant as a proof of identity of the customer. With these new standards even if a hacker manages to gain access to credit card details they will not be able to use them to make purchases unless they can also guess the owner's username and password for the credit card. Even when credit card details are 'hacked' from a website they would be of no use to a thief who would fail the authentication step during a purchase and be unable to fraudulently use the credit card details.

What will happen next?

The real question now is "*how fast can Visa and MasterCard convince all the banks and online merchants to upgrade their systems to support the new authentication standards*?"

The new authentication standards will provide a reliable and trusted environment for doing business online, but the challenge is to educate banks and merchants on these benefits so that they in turn start offering these services to their customers.

As a cardholder what do I need to do?

Cardholders will be informed by their bank, when their bank introduces support for secure and authenticated payments. The cardholder will need to register with their bank for authenticated payments in a process that will generally be conducted online. In most cases the cardholder will be provided with an electronic wallet and then use this when they intend to go shopping online.

As a Merchant what do I need to do?

Merchants will be required to modify their online shopping cart to provide cardholders with the ability to make an authenticated payment. This will involve the merchant embedding an authentication plug-in in their website, which can communicate with the cardholder's bank. The merchant will also need to provide additional information on their checkout page, which can be read by a cardholder's electronic wallet.

As a Card Issuer what do I need to do?

Credit card issuers will be required to install a "wallet server" to handle the cardholder authentication process. This will also create the "one-time" signature, which is ultimately given to the merchant by the cardholder in order to validate the cardholder's identity. These Issuers or banks will also need an "Access Control Server" to register their participating cardholders with Visa's directory.

As an Acquirer what do I need to do?

Merchant Acquirers or Acquiring banks will have to install an Internet payment gateway, which is capable of accepting the authentication message given to the merchant by the issuer. This authentication information will need to be captured and sent to inter-bank networks. Authenticated transactions will carry a lower fee than those which have not been authenticated.

What can GPayments offer?

GPayments provides solutions for all parties wishing to take part in authenticated transactions, which includes the following products:

ActiveWallet: electronic wallet for cardholders, which is generally distributed to cardholders by their card issuers.

ActiveMerchant: Authentication plug-in for merchants, which will work with any Issuer capable of providing cardholder authentication. Learn more about ActiveMerchant here.

ActiveAccess: Access control server for card issuers wanting to participate in 3-D Secure transactions.

Learn more about ActiveAccess here.

ActivePayment: Internet Payment gateway for online payment acquirers wanting to receive payments from merchants over the Internet.

See Also:

GPayments_Authentication_Whitepaper

2FA-An Industry Wide Solution