GPayments
Innovate - Empower - Adapt

Authentication and Payment Solutions

Verified by Visa Overview

The 3-D Secure authentication standard

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.

Verified by Visa Overview

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 UCAF (Universal Cardholder Authentication Field).

The operation of 3-D Secure and UCAF 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.

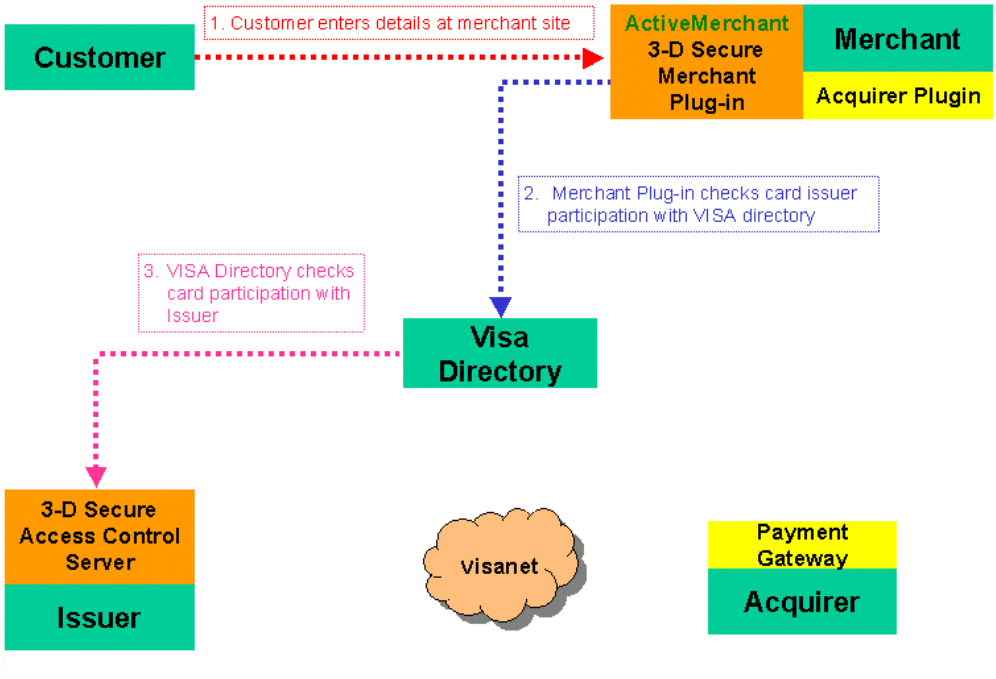
In the "Issuer domain" the issuer is responsible for deploying an issuer system comprised of enrolment, receipt and access control servers. The issuer system handles communication with 3-D Secure merchant plug-ins and a centralized Visa directory, which acts as a communications intermediary between merchants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

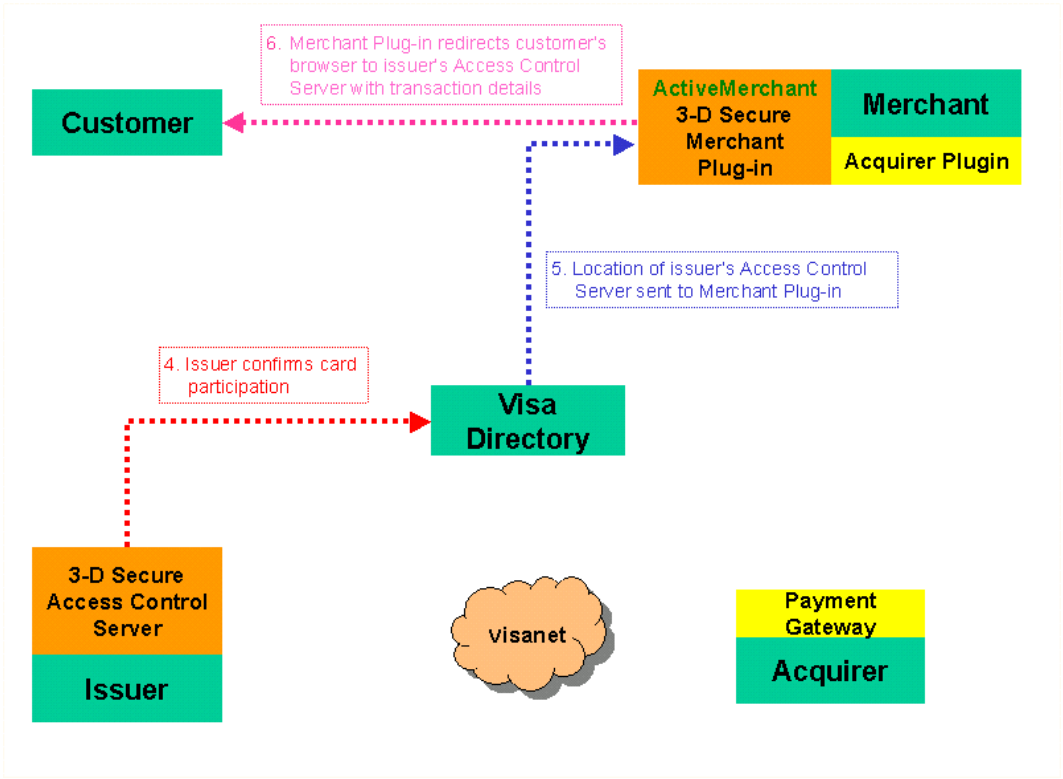
The issuer system handles all interactions with the customer at multiple Internet access points that support a browser. The software deployed by the issuers needs to be integrated with their backend card systems providing access to cardholder information.

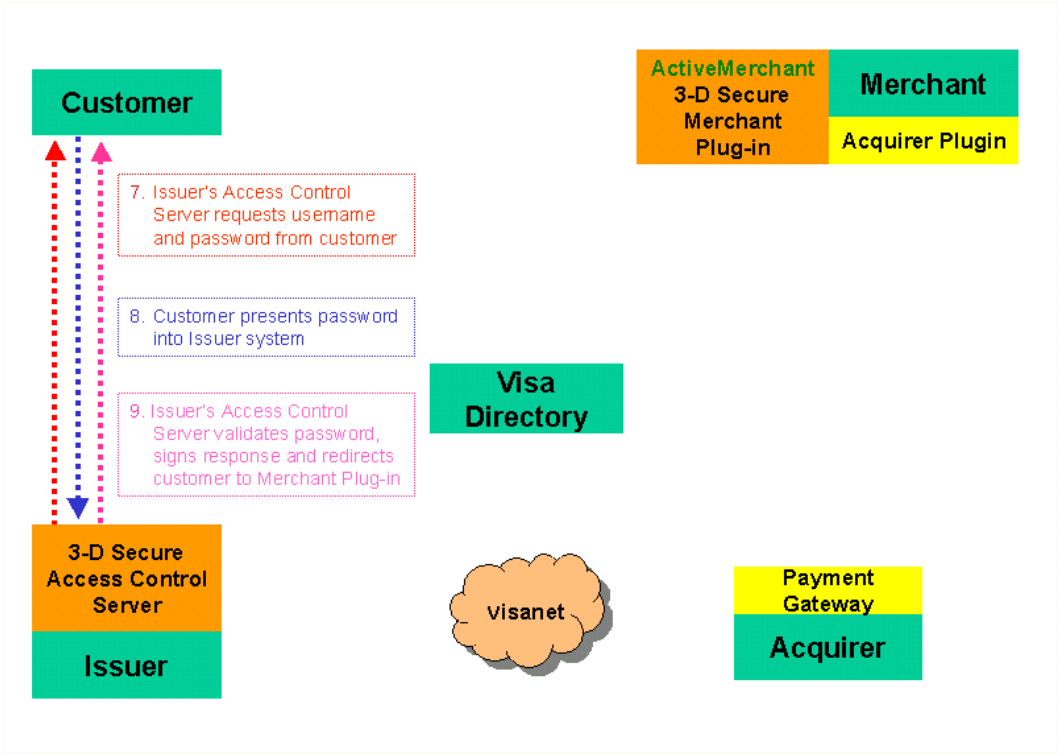
3-D Secure has minimized the requirements for cardholders mandating that they only need a browser to participate unless they are making a chip-authenticated purchase in which case they require client-side software as a minimum pre-requisite.

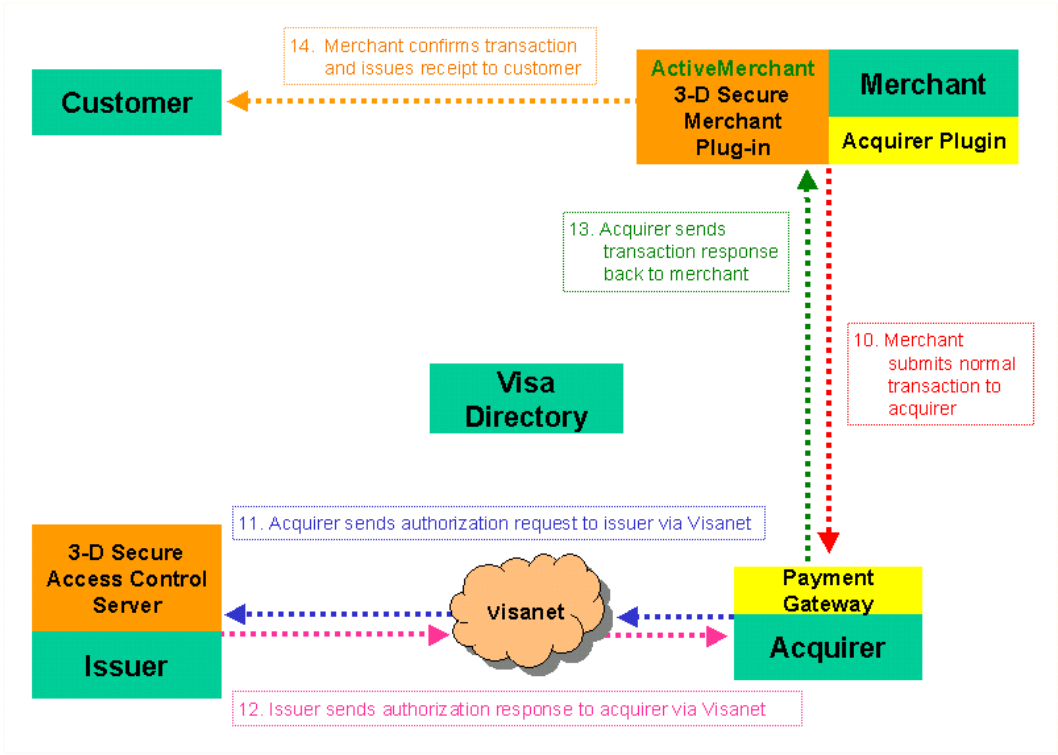
In the Acquirer domain, acquirers are responsible for deploying a payment gateway and merchants install payment gateway plug-ins in exactly the same way as a typical SSL environment. Under 3-D Secure the merchant also needs to install a 3-D Secure Merchant plug-in (MPI) or connect to a 3-D Secure Merchant 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' MPI's 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.


1. Customer enters details at merchant site
Customer
ActiveMerchant
3-D Secure
Merchant
Plug-in
Merchant
Acquirer Plugin
2. Merchant Plug-in checks card issuer participation with VISA directory
3. VISA Directory checks card participation with Issuer
Visa
Directory
3-D Secure
Access Control
Server
Issuer
Visanet
Payment
Gateway
Acquirer


6. Merchant Plug-in redirects customer's browser to issuer's Access Control Server with transaction details
Customer
ActiveMerchant
3-D Secure
Merchant
Plug-in
Merchant
Acquirer Plugin
5. Location of issuer's Access Control Server sent to Merchant Plug-in
4. Issuer confirms card participation
Visa
Directory
3-D Secure
Access Control
Server
Issuer
Visanet
Payment
Gateway
Acquirer


Customer
ActiveMerchant
3-D Secure
Merchant
Plug-in
Merchant
Acquirer Plugin
7. Issuer's Access Control Server requests username and password from customer
8. Customer presents password into Issuer system
9. Issuer's Access Control Server validates password, signs response and redirects customer to Merchant Plug-in
Visa
Directory
3-D Secure
Access Control
Server
Issuer
Visanet
Payment
Gateway
Acquirer


14. Merchant confirms transaction and issues receipt to customer
Customer
ActiveMerchant
3-D Secure
Merchant
Plug-in
Merchant
Acquirer Plugin
13. Acquirer sends transaction response back to merchant
10. Merchant submits normal transaction to acquirer
Visa
Directory
11. Acquirer sends authorization request to issuer via Visanet
3-D Secure
Access Control
Server
Issuer
Visanet
Payment
Gateway
Acquirer
12. Issuer sends authorization response to acquirer via Visanet

www.gpayments.com.au