globalpayments

GLOBAL IRIS™

Powered by realex payments

Global Iris

RealMPI 3D Secure

Service Overview

February 2013

Payer Authentication Service

What Is Payer Authentication?

When selling on the internet and accepting payments by credit and debit card it is possible to authorise a transaction in real time. Until now a merchant has never been sure that the person using the card is the actual cardholder. Consequently online trading has been limited by the fact that merchants were liable for any possible fraud.

In order to eliminate this risk, Visa have developed a process referred to as Verified by Visa and MasterCard a process called SecureCode. Collectively they are known as 3DSecure. The cardholder will need to verify themselves to their bank at the time they are buying online. This will assure that the person using the card is the actual cardholder. Merchants who wish to benefit from this service need to modify their internet application so that it includes the process of getting the cardholder to authenticate himself. This is payer authentication – verifying that the cardholder is the actual person using the card.

How Can Merchants Benefit From This?

Internet merchants who implement a scheme-certified payer authentication service will benefit from a liability shift. Up to now the liability for chargebacks rested with the merchant. When payer authentication is used, the liability is with the issuing bank - so long as the merchant has attempted to authenticate the cardholder and follows all other normal procedures and regulations.

At the same time as making the merchant better off, the process also makes the cardholder more comfortable as they will be verifying themselves to their own bank.

How Does A Merchant Implement A Payer Authentication Service?

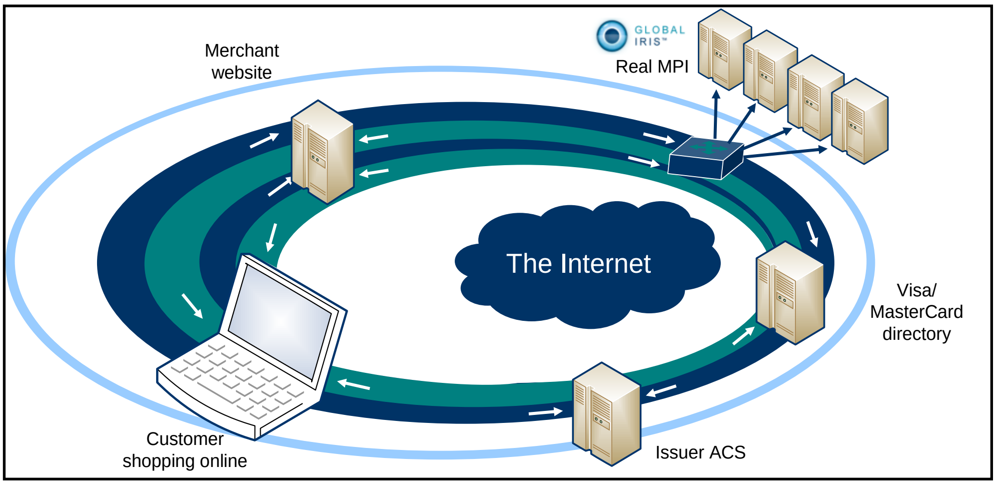
Merchants must modify their internet applications in order to become compliant and get the benefits. A merchant must use what is referred to as a “Merchant Plug-In”; this is software that has been certified and tested by Visa and MasterCard as compliant with the new real time processes and message exchange.

A merchant can approach this in a number of ways - implementing and certifying their own software; buying and implementing third party software or by using a service – such as the Global Iris RealMPI service. Global Iris RealMPI will have you up and running in minutes and eliminate the need for you to develop, implement and pay for third party software.

Implementing Global Iris RealMPI

Global Iris has developed a solution to enable merchants to benefit from payer authentication with the minimum amount of technical change and disruption to existing internet applications.
Our payer authentication service – referred to as Global Iris RealMPI has the following benefits:

- It can be used independently of your authorisation solution.
- It is fully approved and tested by Visa and MasterCard to the latest standards.
- In order to use the Global Iris RealMPI service no additional software or hardware is needed by the merchant – Global Payments host the MPI on our systems and interface with the Visa and MasterCard directories.
- To use the service you must modify your internet application so that prior to authorisation you determine, via us, the issuing bank of the card being used and then open a new browser for the cardholder to login to their issuer and authenticate himself. The result of this attempt is sent to us to decode and verify – once you know that the cardholder authenticated successfully you authorise the transaction.



- The authorisation request will require the transport of additional data collected during the authentication process.
- If you use Global Iris for your authorisations then the two processes may be integrated in more detail if desired.
- Once you agree to go ahead we will provide you with access to a full test environment and supply integration support/advise along with sample code in an assortment of languages – ASP, Java, PHP, Perl etc.

Global Iris RealMPI is specifically designed to make the implementation of Verified by Visa and MasterCard SecureCode as easy as possible for internet merchants.

How It Works

Your website currently allows customers to purchase goods or services. At the end of the shopping process, the customer is presented with a total amount and asked to enter their credit or debit card details. They then press the “Pay Now” button and their card is authorised via your card processor. If subsequently the customer denies the payment, you may have no choice but to accept liability for the fraud and refund the customer, and possibly pay a bank fee for the pleasure. This process is known as a chargeback. If you have too many chargebacks, Visa and MasterCard can impose extra fines upon you.

The reason that you must accept the liability is because you have no evidence to prove the customer made the purchase. In a customer-present situation such as a high-street store, you would be able to produce a Chip and Pin receipt, but online you have no such evidence. It was against this backdrop that the 3DSecure service was proposed. 3D Secure is designed to provide the online evidence a merchant needs to prove that a customer did in fact make a certain purchase.

The 3DSecure approach works by shifting the liability incrementally depending on how many of the pieces of the chain are in place, thereby forcing each party to implement the solution, or face the liability for the chargeback.

The parties involved are:

- The Merchant (you);
- The Card Processor (Global Payments);
- The Issuing Bank (the bank that gave the card to the customer); and
- The Customer (who is shopping on your site).

The best approach to explaining how it works is to describe what happens in the fully implemented situation (i.e. where every link in the chain is implemented) and then to describe what happens when some links aren’t.

After a customer enters their card details, they click the “Pay Now” button. Instead of going straight for authorisation, the card details are first put through the process of Authentication, using a piece of software called a Merchant Plug-In (or MPI) such as Global Iris RealMPI.

- The card details are sent to a central Visa or MasterCard Directory to check which bank issued the card.
- The Directory contacts the bank and electronically asks if the customer is set up with a 3DSecure password.
- The issuing bank returns the web address of their customer authentication application (this is called the Access Control Server or ACS).
- Your MPI opens a new web browser window and loads the ACS web page into it.
- Because this page is from the issuing bank, the customer recognises their bank logos and sees that they need to enter either specific characters from or their full password before they can continue. (They have already agreed this password with their bank when they got their credit card – just like they would have agreed their PIN).
- This is sent back to the MPI on your site, which checks the signature, confirms that the authentication was successful and finally goes to your card processor to authorise the sale – including this new code in the message.

Once this happens the liability is pushed back to the issuing bank. They are responsible for their cardholder’s actions at this point and the onus is on them to implement the ACS system and give all their cardholders a password to use online. **This point is the key to the success of the 3DSecure process – even if the cardholder does not yet have a password, the merchant is not liable because of the way Visa and MasterCard have made the rules.** Because the merchant and the card processor have both implemented the system, the liability rests with the issuing bank.

NOTE: Some card types are not covered by the liability shift in the event of a “Not Enrolled” response. These may include commercial cards and anonymous prepaid cards. Please check with Global Payments to confirm the rules in your situation.

A Technical Comment

Like our other services, Global Iris MPI is based on the exchange of XML (Extensible Markup Language) messages between the merchant’s internet site and Global Iris. All connections are made over SSL (Secure Socket Layer) and there are additional digital signatures required to validate each party.

The process is as follows:

- The merchant’s internet application submits an XML request to us with the transaction details – you post the data over https.
- Global Iris RealMPI responds in seconds with the issuer’s URL and some additional data.
- The merchant’s site posts the data to the URL supplied and after the cardholder attempts to authenticate himself to his issuing bank a reply is sent back to the merchant.
- This reply is forwarded to Global Iris and we verify the response and the parties involved and return the result to the merchant – if you also use the Global Iris RealAuth service then we can auto-authorise the transaction if required.

For further information please contact the Global Iris helpdesk on 0845 702 3344*.

Global Payments
51 De Montfort Street
Leicester
LE1 7BB
Tel 0845 702 3344*
Textphone 0845 602 4818
Email globaliris@realexpayments.com

Global Payments is HSBC’s preferred supplier for card processing in the UK.

Global Payments is a trading name of GPUK LLP. GPUK LLP is authorised by the Financial Conduct Authority under the Payment Services Regulations 2009 (504290) for the provision of payment services.

GPUK LLP is a limited liability partnership registered in England number OC337146. Registered Office: 51, De Montfort Street, Leicester, LE1 7BB. The members are Global Payments U.K. Limited and Global Payments U.K. 2 Limited. Service of any documents relating to the business will be effective if served at the Registered Office.

*Lines are open between 9am – 5pm Monday to Friday excluding public holidays. To help us continually improve our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property. We also provide a Textphone service on 0845 602 4818.