ELECTRONIC PAYMENT SYSTEMS OBSERVATORY-NEWSLETTER

ePSO-Newsletter – No. 10 – November 2001

http://epso.jrc.es/newsletter

The Institute for Prospective Technological Studies (**IPTS**), has established the "electronic Payment Systems Observatory" (ePSO) on behalf of DG ENTR within the ISIS programme. One activity of ePSO is the publication of this monthly electronic newsletter: **ePSO-N**. The Institute for Technology Assessment and Systems Analysis (**ITAS**) of Karlsruhe Research Centre has been commissioned to edit this newsletter (cf. [10&9] Masthead for details).

Michael Rader	**Yannis Maghiros**
co-ordinating editor	**ePSO project leader**
rader@itas.fzk.de	ioannis.maghiros@jrc.es

[10&2] Guaranteed Transactions, the Quest for the ‘Holy Grail’

Oliver Steeley (oliver.steeley@consult.hyperion.co.uk), Consult Hyperion, Guildford, United Kingdom

/credit cards/Internet payment systems/security

In a change to their previous strategy of collaboration, Visa and MasterCard have recently announced their own separate initiatives with regards to securing Internet transactions. 3D Secure and SPA/UCAF are variations on a theme of passing the cardholder back to their card-issuer to authenticate themselves before the merchant seeks an authorisation. This is one more step in a long and arduous journey, which shows no signs of coming to a speedy conclusion.

The legend of the search for the Holy Grail became the principal quest of the knights of King Arthur and has endured for hundreds of years in western literature and arts.

It may now only be 5 years since the card schemes published the specification for the SET protocol, but for many in the Internet transactions industry, it feels like centuries. The quest for mass deployment of a protocol for guaranteed transactions in a cardholder not present environment continues, as the knights of the ‘rectangular table’ in the card schemes gallantly battle on.

To celebrate the 5th anniversary of the beginning of their crusade, this article looks at two of the most recent developments in the saga from the main protagonists, VISA and MasterCard and highlights the difficulties they face.

3D Secure

A recent press release from Visa points out that Worldpay are the first solution provider to implement 3D Secure in Europe. Worldpay's 11,000 online retailers world-wide will be able to take advantage of the protection that Visa is offering from cardholder repudiation. Regardless of whether the cardholder is 3D Secure capable or not, 3D Secure merchants will no longer be liable for card not present charge backs from April 2002 in Europe and April 2003 globally.

The transaction flow for a 3D Secure (“Verified by Visa”) transaction is summarised in the diagram below. The solution requires no software to be loaded onto the cardholder’s PC although it does require the cardholder to register a “password” or some other authentication mechanism (such as a smart card) with their issuing bank to enrol in the scheme.

At the point when the cardholder hits the “buy” button on a merchant web site, a plug-in is activated (on the merchant site), which queries the VISA directory server to determine whether the cardholder is enrolled in the scheme. If they are, then the merchant plug-in is given the web site address of the ‘Issuer Access Control Server’. The merchant plug-in then sends an authentication request to the issuer via the cardholder’s browser such that a pop-up window appears to the cardholder. This pop-up window contains details of the purchase and prompts for the authentication information. The issuer validates the authentication information and formats an authentication response, which is digitally signed and returned to the merchant. This response will include a unique cryptographic value based upon the transaction data called the ‘Cardholder Authentication Verification Value’ or CAVV. A copy of the authentication response message is also sent to the Authentication History Server. When the merchant receives the authentication response, the merchant validates the digital signature of the issuer, returns the positive response to the storefront software and submits an authorisation request to the acquirer. This authorisation request includes three additional pieces of information from the Issuer’s authentication response. These are the CAVV, the Electronic Commerce Indicator or ECI (which identifies this as an Internet Transaction) and a unique transaction identifier called the XID. The acquirer maps these pieces of data into the existing Visanet fields for an authorisation request message and passes it into Visanet. Visanet then verifies the CAVV with the copy stored on the Authentication History Server (although this element of the service is not yet live) and forwards the authorisation request to the issuer. The issuer receives the authorisation request with the authentication information and processes the transaction in the normal way. The whole process takes 10-15 seconds.

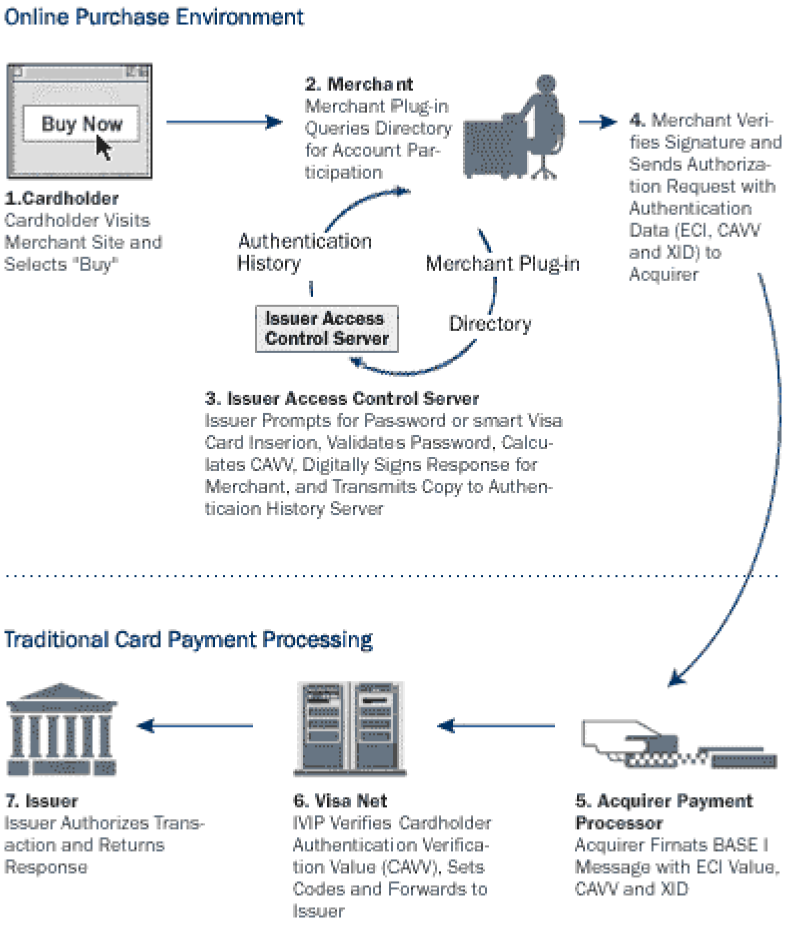
Online Purchase Environment
Buy Now
1.Cardholder
Cardholder Visits Merchant Site and Selects "Buy"
2. Merchant
Merchant Plug-in Queries Directory for Account Participation
4. Merchant Verifies Signature and Sends Authorization Request with Authentication Data (ECI, CAVV and XID) to Acquirer
Authentication History
Merchant Plug-in
Issuer Access Control Server
Directory
3. Issuer Access Control Server
Issuer Prompts for Password or smart Visa Card Inserion, Validates Password, Calculates CAVV, Digitally Signs Response for Merchant, and Transmits Copy to Authenticaion History Server
Traditional Card Payment Processing
7. Issuer
Issuer Authorizes Transaction and Returns Response
6. Visa Net
IVIP Verifies Cardholder Authentication Verification Value (CAVV), Sets Codes and Forwards to Issuer
5. Acquirer Payment Processor
Acquirer Firnats BASE I Message with ECI Value, CAVV and XID

Figure1: 3D Secure

SPA

In May 2001 MasterCard announced it's own Secure Payment Application (SPA). SPA is based around the Universal Cardholder Authentication Field (UCAF) and has been designed to minimise integration and deployment costs to the merchant. Fundamentally, UCAF is a 32-byte field with a flexible data structure that can be tailored to support a variety of security and authentication approaches including SPA, biometrics, smart cards, digital certificates and others. MasterCard has designated Data Element 48, sub-element 43 to contain the UCAF. In a SPA transaction, the UCAF field is populated with a unique cardholder authentication value for each transaction that can be verified by the issuer as part of the authorisation transaction. Merchants and acquirers are simply responsible for collecting this value and including it with other information when they submit an authorisation request.

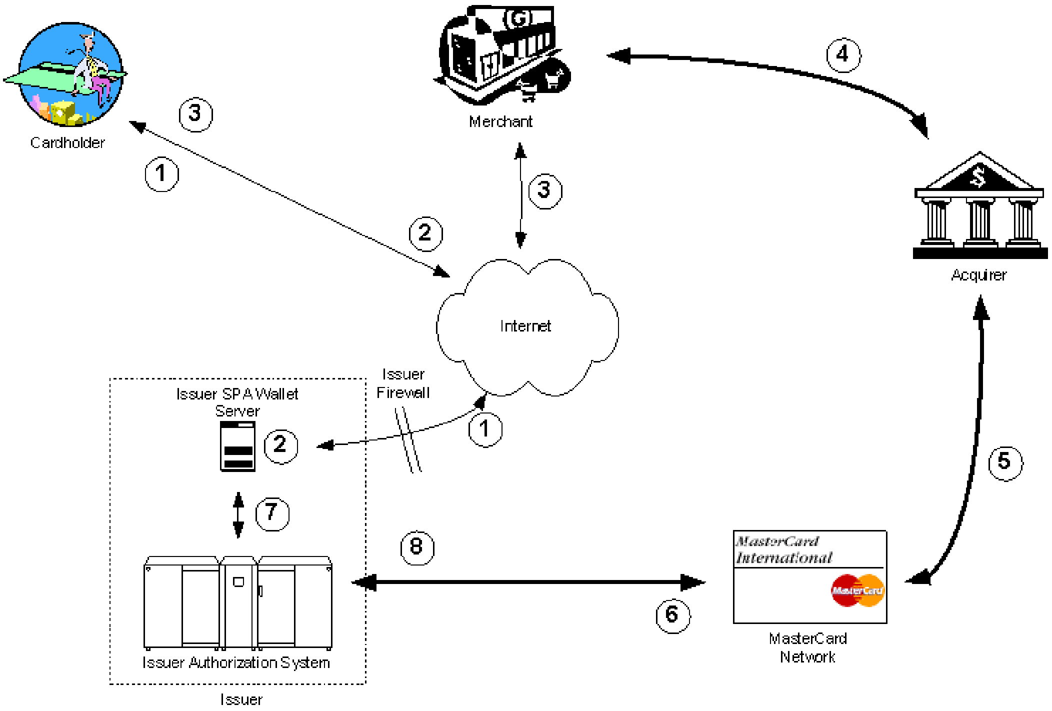

Figure 2: SPA/UCAF

The diagram above summarises a SPA transaction. Similar to 'Verified by Visa' a cardholder enrols for SPA with their issuing bank and the exact choice of authentication method is at the discretion of the issuer. During the shopping experience, when the merchant server requests the payment card details it also includes some hidden fields. These hidden fields include:

- The merchant name, ID, Address and country code
- The sale amount
- An unpredictable number (optional)
- Authentication Data (Blank UCAF)

The cardholder PC will need an applet or wallet application to detect these fields when sent by the merchant site. The wallet will then submit an authentication request to the issuer. The issuer then validates the customer in the agreed manner and generates a transaction specific token value to include in the UCAF field and to store ready for an incoming authorisation request. The SPA wallet then populates the hidden fields on the merchant site in order that the merchant can submit an authorisation request that includes the UCAF value via the acquirer into MasterCard's network and back to the issuer. If the value in the UCAF field matches (either comparatively or cryptographically according to the authentication method used) the value held at the bank for that transaction, the authorisation proceeds to be processed in the normal way.

Conclusions

It does seem paradoxical that for EMV and SET the card schemes even created jointly owned companies to manage interoperability (EMVCO and SETCO) and compliance issues, yet banks that issue and acquire both VISA and MasterCard and merchants that accept both schemes through their acquirer may need to deploy two separate protocols. Exactly how AMEX plan to join the fray remains unclear at this stage.

Whether this fragmented approach by the card schemes will facilitate speedy deployment or simply create further confusion and inaction amongst banks and merchants remains to be seen. Perhaps by "splitting-up" and looking in differing directions the knights are increasing the chances that one of them will triumph in their quest. What is clear is that the quest is far from over.

[**info**]

- http://www.greatdreams.com/arthur.htm
- http://usa.visa.com/business/merchants/verified_online_purchases.html
- http://www.mastercardintl.com/about/press/pressreleases.cgi?id=423
- http://www.mastercardintl.com/spa/demo/details.html
- http://www.mastercardintl.com/spa/demo/features.html
- http://www.cardforum.com/html/ccmissue/sep01cov.htm
- http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2811269,00.html
- http://www.worldpay.com/