



3D SECURITY:

by Richard Crookston,
head of Solutions Marketing,
ACI Worldwide (EMEA)

Securing Internet Payments in an Unsecured World

Payment cards have emerged as the natural currency of the Internet, which represents enormous business potential for banks. However, the growth of e-commerce has exposed weaknesses in the way card transactions are typically processed. This has caused all participants — merchants and consumers — to become vulnerable to an unacceptable level of risk.

The Problem

According to Eduardo Merigo, chairman of the Visa European Union (EU) Board, “Today, over 50 percent of online transactions are made on a Visa card—but online transactions are significantly more likely to be disputed than a transaction made in the physical world—clearly not a sustainable business model for merchants or banks.”

During the past year, in the Visa EU region alone, Visa members have been faced with disputes that cost an estimated US\$250 million. These disputes could have been prevented by proof that the authorized cardholder initiated the transaction.

But the problems facing the industry are global in nature and astronomic in the level of potential risk. A global examination of this problem that includes all card schemes brings potential losses to more than US\$1 billion.

Most e-commerce providers are currently accepting the risk in order to grow their business in the virtual world.

Securing e-commerce Transactions

Security in the transaction-processing world of e-commerce is a moving target. Two security solutions in use today are secure sockets layer (SSL) and secure electronic transactions (SET™), with a variety of other options under development.



The SSL Handshake Protocol was developed by Netscape Communications Corporation to provide security and privacy over the Internet. SSL is widely deployed and easily implemented, but does not

provide authentication and validation of the consumer and merchant. SSL will continue to play a role and provide the only security mechanism in some applications. In an environment where mail order/telephone order (MOTO) is used today, the merchant may accept the risks, but SSL provides the confidentiality for card information that cardholders require. The underlying rationale for using SSL is that it is simple, quick to implement and cost effective.

FACT

A survey of American financial losses attributable to computer crime topped \$10 billion in 1999. In a study of 643 public agencies and U.S. corporations, it was found that 90 percent detected security breaches, a quarter of which were from outside....

Source: Computer Security Institute, San Francisco, California

The SET specification is an open technical standard developed by Visa and MasterCard to facilitate secure payment card transactions over the Internet. SET is a well-defined, robust standard that addresses the business needs of authentication and validation. Software vendors whose products pass SET compliance testing are eligible to display the SET mark on their products, as are merchants and financial institutions that use approved software. The SET specification is available at <http://www.setco.org>.

Other solutions to the problem of providing a secure and cost-effective application are constantly emerging. These include:

• Secure card payment protocol (SCPP).

Developed by Barclays Bank with the cooperation of Europay, SCPP is based upon the use of the new generation of chip-based debit or credit cards. These new cards conform to the EMV specification developed by Europay, MasterCard and Visa. SCPP was designed to use off-line verified PINs to provide similar levels of security to SET. It achieves this with less processing overhead and with only minor extensions to the established POS infrastructure.

From a cardholder's perspective, authorization for a transaction would take only slightly longer than at the merchant's own premises.

• **Pseudo or Random-numbers.** This technique has gained some industry interest. It could be thought of as "super message authentication," with each transaction running through a cryptographic algorithm to create a pseudo primary account number (PAN) rather than using the real number. This is still in its early days of development as an industrial-strength system. Some card schemes have expressed a great deal of interest in this method, as it could provide security with little impact to existing payment systems.

Whatever solution is adopted, it must allow banks the flexibility to determine the way in which cardholders and merchants are authenticated, including chip technology, digital certificates and passwords. This is critical for ensuring that consumers can securely purchase through any Internet or Web-enabled channel, which includes PCs, mobile phones and digital TV.

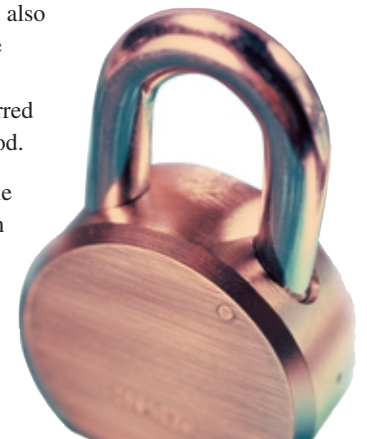
The Three Domain Model

Faced with the rapid growth of national, regional and intercontinental e-commerce transactions, and the emergence of a distinct e-commerce industry, one key initiative has been undertaken to address the problem of fraud. It has been decided by the banks involved that, to reduce the risk and costs, additional authentication has to be introduced for all participants in the transaction.

By working in partnership with industry advisory groups and suppliers, a program of measures has been developed. From this industry-wide activity a new approach to tackle these issues is being introduced, mandated by leading card schemes, and implemented at a regional level.

The card issuers and acquirers must be capable of ensuring cardholder and merchant authentication. They also must be able to have maximum choice in selecting their preferred authentication method.

This is made possible through the adoption of a framework,



FACT

Many businesses are complacent; in a survey, 82 percent of business do not have any firewall protection, 59 percent do not protect their Web sites and 63 percent have never undertaken any IT risk assessments.

Source: UK Government, Dept. of Trade and Industry, 5th industry survey

known as the “Three Domain Model” or 3DM. The 3DM framework splits the authentication into three distinct parts or “domains.”

- **THE ACQUIRER DOMAIN**, where it is the responsibility of the acquirer (subject to certain specified minimum requirements) to define the mechanism whereby the acquirer is satisfied that the merchant is genuine.
- **THE ISSUER DOMAIN**, where the issuer has the responsibility of authenticating that the participating cardholder is valid and using a valid card.
- **THE INTEROPERABILITY DOMAIN**, where transaction data is exchanged using a common protocol.

The Three Domain Model may finally provide the globally interoperable approach to authentication that provides participants confidence that it is both a legitimate cardholder and a bona fide merchant involved in the Internet transaction. This approach provides the flexibility required for varying market conditions around the world, yet ensures that regional solutions are interoperable. As a result e-commerce merchants can have the same benefits as those in the physical world for face-to-face transactions.

One Internet merchant has already welcomed the development. Chris Alexandre from Jungle.com said, “For us, this is great news—it means that the millions of cardholders out there will be feeling much more confident about shopping online and will enable us to perform our role in a far more efficient manner. We have been waiting for this for some time.”

The implementation of 3DM will be driven by the international card schemes. In the Visa EU and Latin American regions, mandates are already in place for use of 3DM by issuers and acquirers. Both regions have initially required the use of SET to authenticate and secure transactions.

ACI Worldwide’s role in supporting 3DM

ACI offers Internet transaction acquirers and card issuers a range of solutions that support the 3DM model and will help them meet their objectives in a timely and cost effective manner.

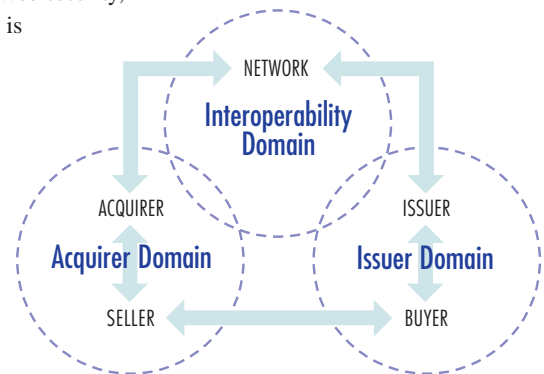
ACI’s e24® Commerce solutions have been developed to handle all aspects of Web-initiated payments and include value-added features to enhance customer

service, merchant reporting and management, and Web-centric fraud detection and management. The solutions employ SSL or SET-based security to ensure that every transaction is secure, every time. Key to the approach adopted is the ability to incorporate new security standards and payment methods as they emerge.

In the issuer environment, the provision of electronic wallets is a tool that can enhance payments security and enable issuers to build a stronger, dynamic relationship with their customers. The introduction of e24-pod (personal online data) wallet technology by ACI establishes this next link in the chain. By providing this user-centric tool, banks can make the use of either today’s or emerging payment security transparent to their customers. It can even enable the use of different methods for different transactions.

Through the use of state-of-the-art technology and by utilizing the latest in Web security, connectivity and access, ACI is ensuring that its customers can easily hook their new commerce-enabled Web sites into current payments processing environments. This will allow for the optimization of customer service levels, funds management operations, aggregation of transactions for reduced processing fees, and better overall payments risk management. And today, at an operational level, ACI provides support for address verification solutions (AVS), which continue to be useful to identify high-risk transactions, while the new technologies are deployed.

ACI’s secure e-commerce solutions allow acquirers and issuers to quickly deploy both SET and SSL existing security methods and incorporate emerging models to gain acquiring for multiple card types and use the capabilities of their existing payment engine to route transactions for authorization to the various card schemes. ●



For more information about ACI’s e24 solutions, contact Gene Hinkle at hinkleg@tsainc.com.