The Electronic Commerce Challenge

By Stephanie Denny
Independent Consultant
Email: stephanie@dc3.com
Web Site: http://www.denny.dc3.com

Stephanie Denny has worked in the banking and credit card industry for 26 years, most recently as VP & Director of Marketing Communications for a major credit card issuer. She is currently an independent consultant specializing in payment systems for electronic banking and commerce.

Abstract

One of the biggest challenges in the development of electronic commerce has been for banks and merchants to overcome the issues of customer identification and account verification for online purchases. While the credit card systems have a process in place to verify and authorize transactions, the Internet poses challenges for merchants to not only validate that funds are available in an account, but to positively identify that the customer is in fact authorized to use that account for purchases.

Early in the life of eCommerce, this situation led to the development of the SET protocol (Secure Electronic Transactions). While the initial version of SET was written in 1995, it has yet to be implemented for a number of reasons.

More recently, there has been a standard proposed called x9.59 (Account Authority Digital Signatures, or AADS), which recognizes the necessity of binding a certificate to an account number. Lynn Wheeler , the author, appropriately summarizes the current situation in his document: "To make electronic commerce real, it will be necessary to demonstrate integration of public-key bindings into the core account-based business processes. This requires changes to the installed data processing implementations. Without this integration, there is little hope of deploying electronic commerce on a large scale."

One of the biggest challenges in the development of electronic commerce has been for banks and merchants to overcome the issues of customer identification and account verification for online purchases. While the credit card systems have a process in place to verify and authorize transactions, the Internet poses challenges for merchants to not only validate that funds are available in an account, but to positively identify that the customer is in fact authorized to use that account for purchases.

In the physical world, merchants can validate the identity of the accountholder by comparing the signature on the credit card with the signature on the sales slip. But in a virtual world, where the customer is not present, the merchant does not know if that person is authorized to use the account number provided for the transaction. The danger in the eCommerce environment is that without some additional controls, the exposure to losses from fraudulent usage is exponentially greater.

The Development of SET

Early in the life of eCommerce, this situation led to the development of the SET protocol (Secure Electronic

Transactions). While the initial version of SET was written in 1995, it has yet to be implemented for a number of reasons. But the catalyst for SET was the realization that there must be a way to positively identify individuals in an online environment, and that the identification process must include the binding of the individual to a specific transaction. This is absolutely critical to the effective management of credit card and debit card account usage.

The implementation of the SET protocol has been challenging for a number of reasons, and as time has passed there have been other standards and solutions proposed as alternatives. No doubt there will be many more, as eCommerce is still in its relative infancy. But with each iteration of SET or other proposed solutions, it's clear that the industry has recognized the major obstacles, both technically and operationally, and is working to overcome them.

When the first version of SET was released in 1995, it became clear to me that there were monumental operational issues related to its implementation which were not addressed in the specification. Most notably, I saw two major obstacles:

- While the role of a Certificate Authority is to guarantee the identity of an individual, in the case of financial transactions, it must extend far beyond that -- it must also link the identity of that individual to a certain account number. This greatly increases the issue of liability for the CA.
- The linking of digital certificates to specific account numbers would require an overhaul of the mainframe systems and operational functions that manage credit cards or other transactional accounts, and the cost of implementation could be significant.

An Alternative Solution

More recently, there has been a standard proposed called x9.59 (Account Authority Digital Signatures, or AADS), which recognizes the necessity of binding a certificate to an account number. It was developed by Lynn and Anne Wheeler, a husband-and-wife team of computer scientists who work at First Data Corp. Their understanding of credit card processing and account management is reflected in this proposed standard, as it addresses three major issues:

- The fundamental concept of AADS is that it limits the scope of a digital signature to a specific account, so that the CA's liability is limited as well. In this case, it would be far more attractive to the banks to issue digital certificates; and they would be in the best position to do this since they would have both the customer and the account information.
- Since a digital certificate is tied to a specific account, it makes the operational process for the bank or card company manageable. If a card is reported lost or stolen, or if there is a credit problem with the account, both the account number and the certificate can be blocked at the same time to limit liability.
- The customer's public key would reside with the account record, eliminating the need for a parallel system and the associated operational issues and costs.

AADS, proposed as industry standard x9.59, is now heading towards final standards vote. If you're not already familiar with AADS, the proposal is worth reading: http://www.garlic.com/~lynn/aadsover.htm. AADS advocates the use of public key cryptography, yet it incorporates business operational considerations that are necessary to the cost-effective implementation of electronic commerce. This viewpoint is critical for widespread acceptance and every-day use.

Lynn Wheeler appropriately summarizes the current situation in his document: "To make electronic commerce real, it will be necessary to demonstrate integration of public-key bindings into the core account-based business processes. This requires changes to the installed data processing implementations. Without this integration, there is little hope of deploying electronic commerce on a large scale."

AADS advocates the use of public key cryptography, yet it incorporates business operational considerations that are necessary to the cost-effective implementation of electronic commerce.