Is SET Really the Answer to E-Commerce?

By Stephanie Denny
Independent Researcher and Analyst
Email: stephanie@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 researcher and analyst in credit cards and electronic banking and commerce. She resides in Mesa, Arizona

For the past two years, the Secure Electronic Commerce protocol (SET) has been promoted as the answer to safe and secure e-commerce. But the acceptance of SET has been slow to happen with US banks. Meanwhile, electronic commerce continues to grow in its absence. Consumers believe they are already making purchases in a secure environment with SSL (Secure Sockets Layer protocol). By the time we get around to a version of SET that s workable on a broad scale, it may be too late to sell it to the general public.

The latest version of SET promised to be the catalyst that would jump-start widespread commerce on the Internet. To date, some SET pilots are being conducted, primarily in Europe, Asia and Latin America. Only two US banks have agreed to a SET pilot so far; and at least one of those tests has been delayed until 1998. Even with the latest version of SET, lack of interoperability among software remains an issue. Why has the acceptance of SET been so slow to happen?

The complexity and the cost of making SET work are just beginning to be realized. While SET addresses the specifications for cardholder-merchant-acquirer transactions, it does not address the many operational requirements for card issuers to make it work on a large scale. Cardholder certificates are the cornerstone to providing the real value of SET, but the infrastructure has not yet been developed to manage them on a day-to-day basis. Many bank executives don t understand certificate authorities and digital signatures; and according to SET, it is the banks that are responsible for issuing cardholder certificates. It is not likely that the funding for this is included in many banks business plans for 1998.

What Is the Difference Between SET and SSL?

Unlike SSL, SET does solve the issue of identifying the cardholder in electronic transactions. But there s a real cost involved in doing that, and is it really the area of greatest risk? It is generally agreed that the greatest risk with e-commerce is catastrophic losses from large-scale theft of credit card numbers. If that occurred, it would more likely happen with break-ins to file servers, and not during the transmission of transactions through a secure pipe. SET does not protect against that-SET begins and ends with the individual credit card transaction.

How Are They Alike?

Secure electronic commerce is happening today with SSL encryption (Secure Sockets Layer), in spite of all the press about the lack of security on the Internet. SSL does some things as well as SET, and it s already available to consumers through their browsers.

Let s take a look at SET versus SSL. Both SET and SSL solve the following issues:

- Confidentiality of information, and protection against; hacking; or other interception during transmission across a public network, through the encryption of data.

- Integrity of data (like SET, SSL has the capability to determine if messages have been altered).
- Verification that the merchant has been certified by a trusted Certificate Authority. (While it may not be widely known, this capability exists today with SSL for the cardholder to verify that the merchant site is legitimate. If merchants want to conduct transactions in a secure environment, they must provide business licenses and other notarized proof of ownership to be certified by the CA.)

How Realistic is SET Implementation?

SET is working today in limited pilot tests, which are controlled environments. The issue really lies with widespread implementation and acceptance by the general public. Certainly, in an ideal world, SET could be the protocol of choice to ensure absolute security of transactions. But does the incremental benefit provided by SET justify the cost of its implementation? What is the fraud potential for Internet transactions with SSL, as compared to the fraud potential that exists today with MO/TO transactions going across phone lines?

I m not sure that even those who developed SET believe it can be fully implemented. SET specifies that cardholder certificates are optional at the payment card brand s discretion (v. 1.0, Book 1, Section 3.3). This may be an out if all else fails, but in the absence of cardholder certificates, who needs SET?