

# AMERICAN BANKER<sup>®</sup>

THE FINANCIAL SERVICES DAILY

Wednesday, November 20, 2002

## First Data Unit Says It's Untangling Authentication

■ BY DAVID BREITKOPF

A newly formed subsidiary of First Data Corp. has developed a digital signature authentication protocol that executives say will boost an area of Internet authentication that has been stymied by its complex infrastructure.

First aSuretee LLC and its Account-Based Digital Signature technology will compete against such digital signature companies as Identrus LLC and VeriSign Inc. The newcomer's technology allows companies to use digital signatures as a means of authenticating electronic users to their existing accounts without moving through a certificate authority.

A Visa spokesman said that First Data is aiming at back office and business-to-business transactions, not at consumer transactions, which are the focus of Verified by Visa. First Data is a Verified by Visa provider.

First aSuretee executives said their product will be easier to manage and understand than its competitors and that it will forgo some elements that have hindered adoption of digital signatures. Perhaps the biggest difference between the Denver company's ABDS technology and standard digital signatures, they said, is that it will

not rely on certificate authority, which is a middleman piece in the public key infrastructure of digital signatures.

In a conventional digital signature, transactions move through a certificate authority, which generates a temporary identity for the business or consumer. That ID then moves along with the transaction information to, say, a bank, which then has to validate the user's identity with the certificate authority before the transaction can be completed.

First aSuretee's version does away with the certificate authority, the company says. A token simultaneously generates the private and public keys that identify the user, but the transaction goes directly to a bank or company.

"We give you the public key and you recognize your customer the way you've always recognized him," said Curtis Beeson, the chief technical officer for First aSuretee. "Your identity is with who you're doing business with, not with a certificate authority."

In this case, companies set up "redundant data that's always slightly out of synch" and in constant need of updating," he said.

"Why would you have to have" customer

information "in two places?" Mr. Beeson said. "Put the public key in that and you don't need to spend money to buy the certificate authority software to run on a separate box that you had to buy also, and you don't have the add operational expense to update two systems."

All the company needs to add is the ability to put one more field in the account records, or about 40 bytes of information, he said.

Avivah Litan, vice president of financial services at the Gartner Inc. consulting firm in Stamford, Conn., said public key infrastructure "has failed because it's so slow and there's not enough bandwidth when you do credit card authorizations to get a quick response. It introduced a technology and process that was outside the credit card infrastructure that required a different server, and different technology, and different protocols."

Geoff Kahler, vice president of marketing for New York-based Identrus, said it was too early to assess First Data's new program but that his company was researching it. He called Identrus "technology-agnostic" and said it would be willing to "adapt and use whatever technology we want to support our platform." ■