



Michael Sisk
Feb 01 '05, Bank Technology News

Psst! What's the Password?

*Institutions from Bank of America to **Riggs** are placing bets on password management and user provisioning. While the cost savings can be substantial by cutting down on help desk calls, the technology is also proving a powerful security and compliance tool.*

There's a city in Latin America where the incidence of bank robbery and fraud is so high, where fears of an inside job are so acute, that a leading bank has chosen to randomly assign its tellers to different branches every single day. In the mornings, the tellers call up and are told where to report. This way, the reasoning goes, the tellers will never learn enough about one branch's operation to plot any heists.

According to Cindy Sterling, a director for business development at BMC Software, which was hired by the bank to create the password management and user provisioning systems to make such daily reassignments possible, the bank's strategy has worked, dramatically reducing fraud in the year it's been in place. She declined to name the bank or the city. "Every day you find out where you're going to be a teller and every day the access rights are reassigned. Every day ID and passwords change. The BMC system can track the switching of access rights, authenticate that process every day, and allows the bank's services to be up and running."

As password management and user provisioning systems go, this is an extreme example, to be sure, but it does show the possibilities available to banks. And experts in the field say that while banks that have implemented these technologies so far would be classified as early adopters, this kind of technology is on the cusp of moving from those early adopters into the industry as a whole. "Where are we on the adoption curve? We're starting the early mainstream. It's becoming an assumed part of the security architecture. It's still very hot and moving downstream from the early adopters and fast followers," says Jonathan Penn, principal analyst, identity and security at Forrester Research. He adds that so far there have been 500 to 600 of these deployments, typically by banks with 5,000 employees or more.

And in a sure sign that the sector is heating up, M&A activity is on the march. Roberta Witty, research vp, security and privacy, at Gartner, says vendors that had been expecting 100 percent growth, are seeing 150 percent, with more vendors now vying to offer more complete solutions. BMC bought Magic Software last year from Network Associates, as well as privately held Calendra in January. Meanwhile, Computer Associates bought Netegrity for \$430 million in the fourth quarter.

Help for the Help Desk

Password management, broadly defined, is technology that reduces the number of passwords an employee needs, ensures those passwords are regularly changed for security purposes, and often allows for self authentication of employees who forget a password or need to reset one. User provisioning is the automated authorization, tracking and termination of password access to various applications within an institution. Industry experts say there are three major drivers behind adoption of these technologies: cost reduction, internal security controls, and regulations, particularly Sarbanes-Oxley (SOX).

The cost savings connected to password management can be particularly significant and immediate in terms of saving time within IT departments. As Penn puts it, "ROI is not the be all and end all it once was, but it helps."

Witty writes that "user provisioning software license costs for a 15,000-user enterprise run as high as \$700,000, and with password reset and user ID problems representing 15 percent to 35 percent of help desk call volume-with a typical cost per call of \$10 to \$31-enterprises need, and want, to justify the cost of an identity management project. To do so, they typically consider several factors: head count reduction of the help desk or security administration organization performing password resets and user account management; productivity savings for end users (they can reset their password faster than calling the help desk) and business management (for faster access-request approval processing); and finally risk management, including electronic data processing audit management, best practices and regulatory compliance."

Robert Miller, VP of marketing at **M-Tech**, which counts as clients Wells Fargo, Washington Mutual, Sovereign and **Riggs Bank**, says, "Typically password management is the first step before ID management, because it provides a strong ROI and that smooths the way for additional projects." He estimates that overall about a third of a help desk's time is spent handling password resets. "It's a particular problem after long weekends. Help desks will usually bring in all the managers to sit on the help desks after a long weekend. ...What P-Synch does is it allows people to authenticate themselves. In two to five minutes they can have a new password and the help desk didn't have to do anything."

Charlie Dixon, VP of client services at **Riggs Bank**, says his intention when he implemented the **M-Tech** solution called P-Synch for password management last summer was to reduce the calls to the service desk related to password problems. The result was a quick 50 percent reduction in such calls. From January to April of 2004, there were 5,532 password related calls, where employees couldn't remember their passwords, or their passwords were out of synch with other systems, or the passwords had expired. From August to November, after the July implementation, the total number of such calls had been pared to 2,772. "We're saving about 60 hours a month, and that's not to mention the users' loss of productivity waiting for us to reset the password," says Dixon. A big time saving was authorizing the employees at **Riggs Direct** to self authenticate, which has ensured that those employees, who deal directly with the public, are not locked out of their systems for any substantial length of time. Dixon estimates the total cost of purchase, training and implementation was \$40,000 to \$50,000. "Now we can do more diagnostic work."

We're very happy with the product."

Dixon says that going forward, the bank wants to keep adding applications to the single sign on project and eventually get down to one password for everything. Also on the agenda, he says, is creating a series of questions and answers unique to individuals that would allow self-authentication to roll out beyond the **Riggs** Direct group. (PNC Financial Services Group intends to buy **Riggs** National Corp. pending resolution of investigations into the Washington, D.C. bank's embassy accounts business.)

Bank of America has had similar success with Netegrity's Siteminder, designed to manage all internal users and ultimately provide them with a single sign on (SSO) access to applications. Overall, BofA was on target to save about \$3 million by the end of 2004, with about 225 applications as part of its SSO project, according to Netegrity. By the end of 2004, BofA had reduced the number of associates with more than six passwords by 54 percent, and the number of associates with 12 or more passwords by 64 percent. During this period of password reduction, BofA experienced a 65 percent reduction in the number of associates that have called the help desk three or more times in a three month period for password issues. It reduced total password-related help desk calls 73 percent.

But the savings are not just possible with the relatively straightforward password management solutions, says John Aisien, VP of marketing and business development at Thor Technologies, which provides provisioning or ID management solutions. Imagine, he says, an investment bank hires an outside contractor for six months. For that time period that person will need an e-mail account, access to certain platform systems, specific access to certain areas of the general ledger, and read only access to other areas. Finally, all that access will need to be turned off on a certain date after the contractor's stint has expired.

The Thor solution allows a relationship manager to request that and have it implemented from a central server. Aisien says the solution saves costs in three key ways. Reducing the cost of manually imputing all of these bespoke access privileges, reducing the hard cost of security once needed to track these individuals, and reducing the soft cost related to delays. Instead of that contractor waiting a week until all his necessary privileges are in place, he can be up and running in a day. Thor's clients include Barclays and Lehman Brothers-the latter of which uses the Thor product to manage ID for more than 400 applications.

Tight Security

The benefits of tighter controls over passwords and access go beyond cost savings, however. Better security is a key benefit. "All security starts with who you are and managing what you can do and managing it in a way that's efficient and structured so that policies are being enforced," says Penn. He notes that at many banks people will accumulate access rights over their tenure that are never turned off even if their job description changes. There is actually quite a bit of movement at big companies, and it's important, he says, that if a person moves from the research side to the investment banking side, for instance, that the employee no longer has the same access privileges within the research arm of the business.

Miller of **M-Tech** says the technology can reduce low tech but sometimes serious areas of weakness in a security system-such as sticky notes on the side of

computers, or passwords that are too easy. Tight security is particularly necessary at banks, which have surprisingly strong seasonal shifts in employee hiring, up to five percent swings in total employees, he says. Typically, tax season will see a temporary surge in the employee rolls, as will the summer when many banks hire summer interns from college. The access given these temporary employees must not only be closely monitored and controlled, it must be turned off after they leave or the bank risks a security breach. "Access is often not turned off even after people leave," Miller says. "We find orphan and dormant accounts and turn them off. Our ID-Synch user provisioning product grants access to certain applications and revokes access when you leave. It's about managing the lifecycle of the user."

Critically, these technologies create audit trails allowing banks to not only answer the question about who has access, but who granted access, and why. If there was some exception made, what was the rationale? All in all, it allows banks to better adhere to their own internal controls. "It's about policy control," says Penn, and he argues that while SOX is certainly a factor in tighter audit controls, "businesses are being held more accountable not just by regulators, but by investors and Wall Street." Still, the long arm of SOX cannot be ignored. "Regulatory compliance issues are overtaking the cost reduction issues as a driver," says Witty at Gartner. "SOX is causing a lot of action, and I expect that to continue for the next two years as companies have to show who has access, to what, prove it, and enforce it." She explains that for regulators to be comfortable, banks will need to show a separation of duties between audit, compliance and attestation. For instance, she says, a manager needs the authorization to request X but that same manager cannot be allowed to approve X. "You need to build rules and enforce them, but you also have to prove they are being followed. Because of SOX, banks need to manage business roles closely."

One result of SOX is that executives and boards of directors are much more personally responsible for what goes on within their organization. With this in mind, last fall **M-Tech** released ID-Certify, which allows CEO and CFOs to monitor all access privileges throughout the organization and see that they have been signed off on by the right manager all the way up the chain of command.

Over at **Riggs** Bank, Dixon says the bank uses Magic Software to closely track who requests what access for whom, whether that access has been granted, and ensuring it's been revoked at the appropriate time. "The regulators are looking at our process to make sure there are no holes, and we're feeling pretty good about it."