PROCESSOR

Products, News & Information Data Centers Can Trust.   Since 1979

IT Standards & Technologies Primer

Development Involves Many Steps & Revisions

by Ericka Chickowski
• • •

INTEROPERABILITY IS TAKEN for granted in today's heterogeneous IT environment. But the ease with which you can make multiple vendors' products work together belies the truth behind the convenience. None of this would be possible without the development of technological standards—a lengthy and sometimes difficult process.

What Are They?

Standards are everywhere. From the electrical plugs you push into wall sockets to the languages used to produce Web sites, these technologies have been so widely used because they are the same no matter what manufacturer makes them.

But agreeing on standards in technology is not an easy process. It can take years to develop a standard deemed suitable for the entire industry. And if there is not a concerted effort to come up with a uniform standard, the industry must wait out a capitalist slugfest between manufacturers as the consumers decide what will become the standard for a particular technology.

If buyers need the technology immediately, they risk putting money into the losing technology. Sometimes the winner may not even be the best choice but instead is the one created by the company with deeper pockets and better marketing.

Standards Categories

There are two types of standards: open and de facto. An open standard is developed by an autonomous organization tasked with coming up with standards with the consensus of the entire industry. Some of these bodies are created as a result of international treaties among various governments, while others are voluntary, nontreaty organizations. Technology developed with open standards includes TCP/IP and the wireless 802.11 formats.

A de facto standard is what happens after the slugfest; it is technology the industry has generally agreed upon as the norm for its type. Some examples include Microsoft's Windows OS and Adobe's PostScript page description language.

While de facto standards are helpful to prevent mass anarchy in the market, experts generally agree that the ideal standard is an

Three-Factor ID

Identification Involves What You Have, What You Know & Who You Are
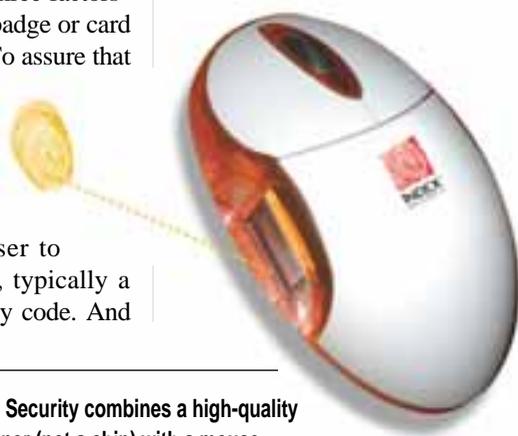
by Steven S. Ross
• • •

SECURITY SYSTEMS THAT feature variations of the classic "three-factor ID" are catching on, thanks to inexpensive and reliable identity cards and card readers and pressure from the federal government's Department of Homeland Security. But vendors warn the new technology will fail without a corporate attitude change. That's especially true when confronting the greatest security threat of all: disgruntled employees or even employees who

have been dismissed but still have access.

The first of the "three factors" is the token, an ID badge or card that triggers entry. To assure that only the person who is supposed to have it is using the card, the security system may also require the user to "know" something, typically a four- or six-digit key code. And

to guard against the code being stolen or obvious enough to crack, the system can also sense something unique about the cardholder—a biometric. That's typically a thumbprint, but it

could also be a facial scan or even an iris scan.

In theory, that leaves only one security loophole: two or more people entering on a single employee's card, key code, or biometric scan. That loophole can be closed, says Ezra Hedaya, president of Index Security, by using motion sensors at doorways, cameras, or a double-door system.

More Than Meets The Eye

There's more to security than technology, however, and corporate attitudes are hard to change. Sidney Furst, president of Access Denied Systems, says, "The first thing is that a company has a

The Zmouse from Index Security combines a high-quality optical thumbprint scanner (not a chip) with a mouse.

Product Releases | 14

■ **Acrosser** announced the AR-M9939, a low power Internet security appliance. ■ **AirMagnet** released AirMagnet Laptop Analyzer 5. ■ **Barracuda** introduced Barracuda Spyware Firewall, an anti-spyware and Web-filtering gateway appliance. ■ **Dell** announced it is offering Microsoft Operations Manager 2005 Workgroup Edition to small and midsized businesses for $50 per server. ■ **EMC** unveiled the EMC Celerra NSX NAS gateway. ■ **Emerson Network Power** announced the new Liebert FPC and FDC power distribution systems. ■ **HP's** four-way Pro-Liant BL45p and ProLiant DL585 blade servers are gearing up to include dual-core AMD Opteron 800 series processors. ■ **Nexsan** and **Diligent** an-nounced a new enterprise virtual tape backup and recovery product. ■ **Winchester Systems** SA-700 SATA disk array lets users control up to 6.4PB of data from a single management

Three-Factor ID

security policy in the first place. But a lot of companies with fewer than a thousand employees do not have a security officer working with IT."

Frances Zelazny, director of corporate communications for Identix, says security "is really about a process and how the back-end process is actually set up. The bottom line with any security system is the trade-off between convenience, cost, and the access you are trying to protect."

Zelazny notes, "Everyone treats security as a cost center," with no offsetting immediate benefit.

The Case For Biometrics

Corporations also may have outdated notions of what is cost-effective. The standard five years ago was a keypad, where a user entered an ID code. The pads are cheap and reliable. But the IT department has to maintain a help desk to reset the access code when someone forgets it or says the code has been compromised. Likewise, a password system to access a terminal or a network is cheap to implement. But employees tend to use weak passwords or even leave them within easy reach. And the IT help desk will spend time resetting passwords that users forget or compromise.

A person's thumbprint will never change. But a few years ago, biometric readers were expensive and unreliable. "There's been a radical change," says Hedaya. "We started our business pre-9/11, and I could not find anything that worked. It

took a year and a half to find the right technology partners."

Hedaya notes the advantages of thumbprint scanners rather than low-resolution imaging chips, even though the chip-equipped readers are a third to half the price (roughly $40 compared to $100) for readers that guard computers. The Zmouse (a scanner built into a mouse) sells for $100 to $120. Door-entry thumbprint readers sell for about $200. The chip-based scanners have improved, as well, in part due to higher resolution and in part to better software.

Considering the cost of help desk time, the thumbprint scanner may save money. It is clearly more secure, as well. "It is easier, faster to log into your system using a thumbprint reader than to type a password," says Furst. "And the system can get you back to exactly where you were when you stepped away."

The Computer Insurance Institute estimates that 1.2 million laptops and PDAs are lost between hotels and airports each year. "What is the real value of the computer? A lot

more than the equipment cost," Furst says. A thumbprint activation system (IBM's and HP's are built into some models; others use a USB connection) is a cheap investment by comparison.

Almost Science Fiction

Companies that have special security needs may be surprised at what's available. "We have a lot of equipment that isn't in the catalog, including an ultrasonic scanner

> ## "We never sell equipment alone. There's always software. We can sell a turnkey system or network security package."
>
> *- Sidney Furst, Access Denied Systems*

that can read a fingerprint through latex gloves," says Furst.

Index Security sells a USB flash memory stick that is thumbprint-protected. It does not require any software to be installed on the host computer, so it can easily be moved from machine to machine, yet only the owner can activate it. Costs range from about $160 to $280 depending on the memory capacity.

One of Index Security's clients wanted RFID cards that could be read at long range. RF readers would be embedded into the corridor walls to keep track of employees' every move. The system was not implemented, he says.

"Video software alone can cost you $3,000 to $4,000 depending

on the type of tracking solutions," he says. "Let's say someone lifts a handbag. I can backtrack to see the handbag, circle it with a wand, and tell the software to show frames where the bag shows up later in the building."

The Security Plan

"We never sell equipment alone," says Furst. "There's always software. We can sell a turnkey system or network security package."

The most important link is the one between the personnel office and IT. "You don't need to have a full-time security person to administer a biometric system within a corporation, but you would need an IT person," says Zelazny.

Furst says, "One of the easiest things to keep track of is the departing employee. HR knows who leaves. They send a memo to IT to disable the account. Period. It's over. If there's no onsite IT, does HR have to make a phone call

for someone to come out and disable an account?" If such a company is your customer or client, do not take security for granted. Such firms may be the source of leaks about your proprietary processes or technologies or critical items such as customer lists.

There's also a need to keep track of logons. "The Justice Department Web site has a section on cybercrimes," says Furst. "There's the story of a young accountant who got into a standalone computer at Cisco Systems and used it to issue $6 million in stock to himself. He had no right to be on that computer."

"We've also been selling to small communities. A housing inspector at one noted that all of the blueprints and floor plans in town, for government as well as public buildings, are on one computer running AutoCAD, and nine times out of 10 when they walk in, there's no one else around or using the computer."

The Experts' Advice

- Make sure the link between HR and IT is fast and foolproof so that terminated employees lose access immediately.

- Decide how valuable an asset is before setting a budget to defend it.

- Consider hardware such as thumbprint scanners to substitute for network passwords as well as for physical security.

- Check on security at suppliers, professional contractors, and sometimes even customers.

- Investigate specific laws such as those that seek to protect credit card or medical data, as well as Homeland Security, and improve your security to fit.

- Don't be afraid to ask about special technology. It may exist, and your security consultant can usually obtain it for you.

PROCESSOR.

Tech & Trends <mark>Second Article on Index Security</mark>

General Information
<mark>*April 22, 2005 • Vol.27 Issue 16*</mark>
Page(s) 27 in print issue

<mark>Who's Holding That Smart Card?</mark>

Modern ID Cards Include A Password Or Biometric Information To Confirm The User

Contactless cards using RFID technology have become the norm for facilities access. They're cheap ($3 or $4 each) and have recently been combined with "smart cards" at $15 to $50 per card, depending on features and the amount of memory in the on-board chips. They're also rugged and, unlike magnetic-stripe cards, are tough to counterfeit.

Until now, smart card applications have been overwhelmingly for large-volume users such as subway systems and credit card companies and have rarely included RFID. The government of Malaysia recently placed an order for 23 million national identity cards. But industry experts say that security applications are gaining, and that firms with fewer than 1,000 employees will find them cost-effective.

Now that prices have come down, their technology is being turned into end-user products by dozens of smaller firms. The idea is that it is not enough to hold a card to gain access. Users must also supply some extra data, and this information is matched with data stored on the card itself. RFID cards alone can't do that.

■ Authenticate The Cardholder

The most common form of user confirmation is a keypad into which users enter a PIN to confirm that the card is their own. The PIN (and other data) is stored in the card's memory. But biometrics, especially thumbprint readers, is rapidly coming to the fore. The thumb, face, or iris scan is compared to an image or a mathematical representation on the smart card's chip.

Former Identix chairman and CEO Bob McCashin says, "Today the weakest link in smart card security is the method used for identifying and authenticating the true card owner. We believe that simply requiring knowledge of a four-digit PIN-code or PUK-code to verify smart card ownership is unreliable and very risky."

An example is the Model 330m Biometric-Enabled Smart Card from SafeNet, which absorbed Datakey in December. It's designed for customers that want an extra level of identity certainty and the convenience of using a fingerprint for authentication. A fingerprint replaces or supplements the PIN, serving as the secure method of authentication to activate the smart card and make use of the stored credentials (certificates and public/private keys, usernames/passwords, etc.). Organizations that need more security can require their employees to use both a biometric and a PIN to authenticate the smart card. It's what the industry calls three-factor security.

<mark>Not all levels of security have to be used at any one checkpoint, however. Ezra Hedaya, president of Index Security, says that many companies might want to use only the card's</mark>

RFID component at the front gate. A quick wave of the card near the contactless reader lets the employee pass. "The quick scan reduces the chance of a bottleneck," Hedaya says. "Bottlenecks are bad for security because they annoy employees." RFID readers themselves cost about $400, says Hedaya.

But internal access to sensitive areas would require entering a PIN on a keypad, and critical areas would use a thumbprint reader after the card is inserted so that the matching data can be read and compared to the employee's input. The best thumbprint readers are quite reliable, allowing them to replace keypads at a small cost premium.

■ Counterfeits Always Possible

Nothing is foolproof. Communication between the card and the reader is two-way, and the data is encrypted (usually with a public key scheme, sometimes with DES, and sometimes with both) to make fraud more difficult. British researcher Markus Kuhn, who found most smart card chips vulnerable to attack five years ago, said recently that today's chips may still be vulnerable to a determined attack. But the level of sophistication and cost required is far beyond what is needed to fake a magnetic stripe and may not be worth it to the thief in most cases.

Hedaya suggests that even the latest cards cannot be relied upon without sophisticated supporting systems. "Start with the software; let's say you put in a regular [RFID] card reader and a keypad reader and a biometric. Every device, as soon as it is touched by a person, the event is recorded."

■ Look For Standard Software

The software is not expensive. "Most of the databases are set up with Microsoft Access and can be upgraded to SQL Server when volume demands," he says. "You can add interfaces to include recording of entry time and calculation of attendance." Basic database packages cost as little as $500 but can go to as much as $4,000.

Critical areas may need extra protection. "You want to know when people leave as well as when they come in," says Hedaya, "so we strongly recommend that a room will need two card authentication units, either at separate doors or on both sides of the same door."

"You're looking at $1,000 to perhaps $1,300 for each thumb-print reader," he says. Keypads for PIN entry at a door are much cheaper—only a few hundred dollars—and may even be more reliable in theory, but many employees share PINs or use PIN codes that are easy to remember, he says.

Hedaya also recommends using security cameras "to solve the second person problem and to have a visual record of the actual people." At the very least, he says, use a motion detector.

Thumbprint readers (based on a simple sensing chip) embedded on USB-interface security cards can cost as little as $40, but reliability has been a problem. So most firms recommend storing the thumbprint information on the dual-interface card and matching it to a high-resolution thumb scan taken at the security checkpoint.

Identix, which sells fingerprint biometric security identification and authentication solutions, has been selling its BioCard Software Developers Kit for a year. It allows card vendors to develop products that integrate finger-print biometric templates on smart cards.

The experts note that Americans are suspicious of thumb scans. "The problem is that Americans don't like biometrics, unlike Europeans, Chinese, South Americans," says Hedaya. "Part of the problem, to be very direct, is the average person is afraid their

fingerprints are being sent to the FBI."

Hedaya says employees get used to biometrics fairly quickly, learning to place their thumb squarely on the sensor, for instance, and to line up their face for a face or iris scan. He also says that once the software is set up, it requires little training to use. ■

by Steven S. Ross

View the chart that accompanies this article.
(*NOTE: These pages are PDF (Portable Document Format) files. You will need Adobe Acrobat to view these pages. **Download Adobe Acrobat Reader**)*

BioPKI™

DoD PKI Complient, TS/SCI approved

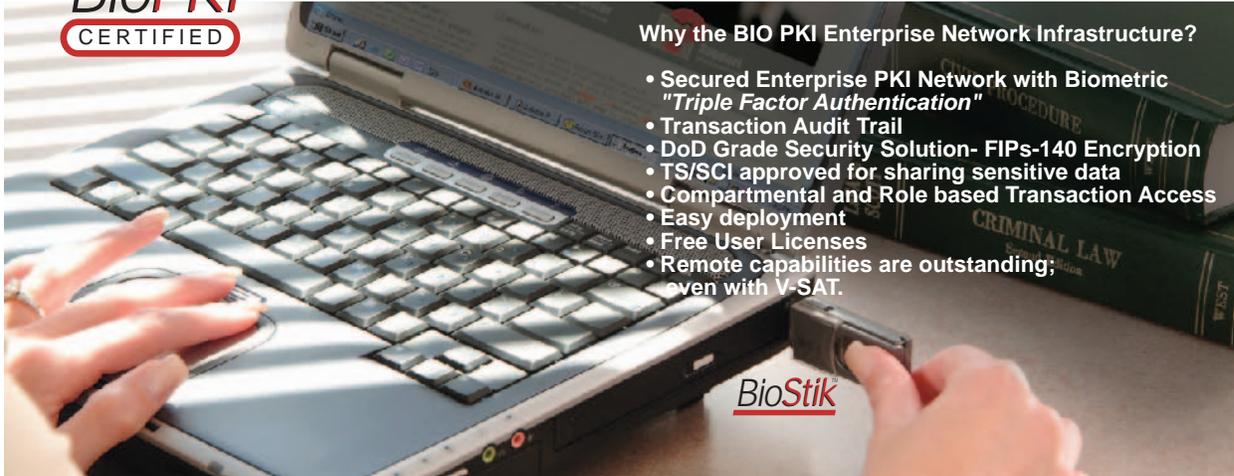**Personal Identity Verification (PIV)**
Enterprise Network

Are you sharing data securely?
BioPKI for true data security.

BioPKI™
C E R T I F I E D

**Why the BIO PKI Enterprise Network Infrastructure?**

• **Secured Enterprise PKI Network with Biometric**
  "Triple Factor Authentication"
• **Transaction Audit Trail**
• **DoD Grade Security Solution- FIPs-140 Encryption**
• **TS/SCI approved for sharing sensitive data**
• **Compartmental and Role based Transaction Access**
• **Easy deployment**
• **Free User Licenses**
• **Remote capabilities are outstanding;**
  even with V-SAT.

BioStik™

Our **BioPKI™** Enterprise security network solution meets all government laws from Sarbanes Oxley, HIPAA, Graham Leach Bliley Act, and 21 CFR part 11, besides being certified DoD PKI compliant. It's up to **YOU** to secure your network.

BioPKI™ *- The Ultimate Combination for True Identity to your Network.*
INDEX SECURITY — secure

BioPKI™ for your network means real security.
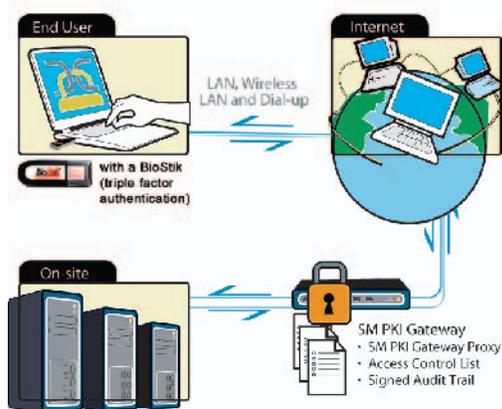
Our embedded SM PKI solution is a single appliance that provides a seamless level of security for multiple application servers without the need for modification. Set up is fast, easy and can be maintained and expanded by your current administrator and team.

With the Enterprise "BIO PKI Network solution" using Index Security biometric products like the BioStik™, there is no question who is on the other end accessing your network. We can control your servers' access for all applications, files, downloads and audit all transactions with the utmost security using a PKI server/client application that can be launched biometrically by our BioStik™ for "Triple factor Authentication".

Real security is everyone's responsibility, make it yours. The BIO PKI is a whole Enterprise Network Solution for the ultimate way to grant your users access biometrically; all digitally signed, with a complete audit trail by transaction. This gives management and network administrators the answers as to how to leave all data on your secured servers yet still share and track who, what, when, where, and how accessed.

End User
Internet
LAN, Wireless LAN and Dial-up
with a BioStik (triple factor authentication)
On-site
SM PKI Gateway
• SM PKI Gateway Proxy
• Access Control List
• Signed Audit Trail

from the Technology-makers at...

INDEX®
SECURITY

500 Parker Avenue , Suite "G"
Deal, New Jersey 07723-1435
Phone: 732- 531-9209   Fax: 732-531-2307
Toll Free 866-INDEX89 (866-463-3989)
www.index-security.com

GSA Listed