

[Microsoft.com Home](#)[Site Map](#)

Search Microsoft.com for:

[Sign Out](#)**Microsoft**

OEM Connect

[OEM Connect Home](#)[OEM Connect Program](#)[Sales and Marketing](#)[Technical](#)[Strategic Guidance](#)[Product Guide](#)[Security](#)[Worldwide Sites](#)[Strategic Guidance](#) > [Exclusive Insights](#) > [Road Map](#) > **Biometrics Gets a Boost in Longhorn**

## Biometrics Gets a Boost in Longhorn

By Robert L. Scheier  
February 2004[E-mail this Article](#)[Print this Article](#)[Letter to the Editors](#)

## Road Map

### Protect your PC

**1 2 3****3 steps to help ensure your PC protection**

Unable to find what you are looking for?

**Let Us Know!**

Can you imagine offering consumer PC buyers an **easy way to manage PC access** to keep older children from accessing sensitive files and Web sites? Using the biometric capabilities Microsoft will build into Longhorn, children can touch a fingerprint scanner to verify their identity before logging into their individual profiles on the PC. When the parent places a finger on the same scanner, it gives them access to their own account with all their files and unlimited access to the Web.

These are among the family-friendly security capabilities Microsoft plans to offer customers with its next-generation Longhorn operating system. While parents can already set up password-protected user accounts in [Microsoft® Windows® XP](#), the new biometrics capabilities now under development **will make such access control even easier** in Longhorn.

The technology promises some **interesting opportunities for OEMs**. USB-based memory keys, for example, could be bundled into systems with built-in fingerprint scanners. Jarad Carleton, an industry analyst with Frost & Sullivan, says the memory keys could save users time and aggravation by storing not just a fingerprint image but passwords to all their on-line accounts as well. "Look at it from the point of view of convenience, rather than of security," he suggests. "That's what is going to sell these things."

### Early Biometrics Advice for OEMs

- ▶ Bundle fingerprint scanners with keyboards and mice
- ▶ Market new ability for users to more easily set and enforce children's account privileges
- ▶ Bundle PCs with fingerprint scanners and USB-memory sticks to ease log-on to multiple accounts

Sources: Microsoft Corp.; industry analysts

### Biometric Basics

Biometric security uses unique physical characteristics to prove a person's identity, such as a fingerprint, voice, handwriting or the unique pattern of blood vessels in the eye. Historically, vendors of biometric security devices have **based their products on proprietary hardware**, device drivers middleware and APIs (application programming interfaces), says Stefan Richards, program manager in Microsoft's Windows Core Security Group.

"This locks a customer into one device and one set of hardware," says Richards. Applications written for such devices, he says, have usually **been targeted to specific markets** such as financial services or defense. These industries have both a high need for security and the ability to pay for it as an add-on to their other authentication methods such as passwords, he says.

Microsoft **hopes to widen the market** by building a common infrastructure for biometric applications into Longhorn, the next generation of the Windows operating system due to be released within the next two years. While the technology under development will eventually accommodate anything from voice recognition to iris scans, Richards says the first high-volume application likely to use the new platform is fingerprint recognition. For more information about Longhorn, see the regularly-updated articles in OEM Connect's [Longhorn Update](#).

### Fingerprints Go First

Why fingerprints? Richards says it's the most **mature and reliable of all the biometric technologies**, having proven itself in areas such as physical access control and time clock authentication. It is also affordable and will drop in price further by the time Longhorn ships.

Still, fingerprint recognition **has shortcomings that likely will limit it to consumer use**, rather than the enterprise market for the foreseeable future. Perhaps the biggest shortcoming with any biometric device is that it must send the actual measurement to the entity authenticating it. With passwords (which can be used to derive a key) and smart cards (which hold a secret key protected by tamper-resistant hardware), a user can prove their identity by showing they have use of a key rather than actually sending the key itself. With proper protocol design in place, this type of design is the most secure of all.

If, for example, a legitimate enterprise user with dirt or a cut on their finger tries to log in, the authentication server might notice a discrepancy and fail to authenticate the user. A typical home computer setup, on the other hand, can afford to be more lenient. In most cases, **a lower acceptance threshold is acceptable** for the average consumer who will store, and authenticate, only a few fingerprints.

Says Richards: "It will take some time for enterprise-ready fingerprint authentication to be able to **guarantee the same level of security** as today's most common methods -- smart cards and passwords. It will require current biometric devices to change or leverage a Trusted Platform Module (TPM). For now, biometrics in security applications would be best used in combination with other authentication methods, like a biometric-enabled smart card."

Nevertheless, Microsoft has a **good chance of expanding the market** for biometrics, says Frost & Sullivan's Carleton. Besides the marketing muscle it likely will put behind Longhorn's biometric capabilities, he says, Microsoft has been working with a small number of innovative biometric companies to further develop this portion of the Longhorn platform.

---

### Built on BAPI

Longhorn's biometric infrastructure **is being built on BAPI** (the Biometrics Application Programming Interface) that will allow developers to write applications utilizing any kind of biometric security. BAPI includes a device driver development kit and the Biometric Resource Manager, an operating system service that routes calls from the API to biometric devices such as fingerprint readers and iris scanners.

Microsoft has **already released to developers** preliminary versions of the Biometric Resource Manager, technology which will allow developers to eventually build out complete solutions around multiple forms of biometric authentication. It also plans to release an initial version of the driver development kit by the first quarter of 2005. About the same time, Microsoft plans to release a Windows Hardware Quality Lab (WHQL) definition of the requirements for hardware to work with a biometric infrastructure.

Meanwhile, Microsoft is **extending and simplifying the existing capabilities** within Windows for creating separate user access accounts, says Richards. This should make it easier and more secure for parents to, say, "lock down" a machine to specific hours of use by their children.

---

### A Matter of Convenience

To prep the market for biometrics, Frost & Sullivan's Carleton advises OEMs to begin educating users now. He says many will be surprised to learn that, Hollywood movies aside, it's very tough to trick the latest generation of fingerprint scanners. Because these scanners use RF (radio frequency) technology to trace the patterns of fingerprints below the layer of the skin, he says, **it's nearly impossible to fool them** with a fingerprint on a glove or reproduced on paper.

That's why the sweet spot for marketing biometrics to a broad consumer audience is convenience,

### Four Biometrics Marketing Tips for OEMs


1. Focus initially on the consumer, not business market
2. Focus on fingerprint scans as the first widespread biometric technology
3. Educate consumers about the reliability of fingerprint scans
4. Emphasize convenience over absolute security

Sources: Microsoft Corp.; industry analysts

### Biometrics: Areas of Interest in Longhorn

- ▶ Built around the Biometrics Application Programming Interface (BAPI)
- ▶ Includes the Biometric Resource Manager to route calls from API to biometric devices
- ▶ A Device Driver Development Kit will ship in early 2005
- ▶ Technology will help developers build complete solutions around multiple forms of biometric authentication
- ▶ Local log-in solution includes a wizard that walks a user through the process of teaching the system to recognize his or her fingerprints

Source: Microsoft Corp.

says Richards. "There's no need to remember a password, or keep a smart card, or something I need to lug around" to log onto a PC or other device, he says. This will make it far easier for non-technical PC users to take advantage of the access control features already built into Windows -- but which today force users to create and protect different passwords for different uses. **"It's the most convenient authentication factor you can think of,"** he says. 

---


### For More Information

[Press release on Microsoft's cooperative agreement with I/O Software Inc.](#)

[Web site of biometrics software vendor I/O Software Inc.](#)

[Web site describing a Sony USB media device with a fingerprint scanner](#)

### About Frost & Sullivan

Frost & Sullivan was founded in 1961 and publishes consulting information and intelligence on emerging high-technology and industrial markets. It employs over 400 consultants, market analysts, corporate trainers, account managers and customer support staff globally providing consulting and corporate training to clients in more than 20 major industries. For more information, go to [www.frost.com](http://www.frost.com) .

### About the Author

Robert L. Scheier is a freelance writer based in Boylston, Mass. He is the former technology editor at *Computerworld*, and previously was a senior editor at *VARBusiness* and *PC Week*. In addition, he was an analyst for The Hurwitz Group specializing in databases and middleware.

Have a question? Want more information? Contact the writers and editors at [oemedit@microsoft.com](mailto:oemedit@microsoft.com).

© 2004 Microsoft Corporation. All rights reserved. This document is for informational purposes only and subject to change without notice. MICROSOFT MAKES NO WARRANTIES, EITHER EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT. The entire risk of the use or the results of the use of this document remains with the user.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any writer license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Last Updated: February 23, 2004

---

[Manage Your Profile](#) | [Contact Us](#) | [E-mail this Page](#) | [Newsletter](#) | [All Rights Reserved](#) | [Terms of Use](#) | [Feedback](#) | [Site Help](#)

©2004 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Privacy Statement](#)