

The Role of Biometrics in Enterprise Security

Although security solutions using biometric technology have been a popular topic since the events of 9/11, this technology is still not widely understood. Biometrics are designed to verify identity and bind an individual to an action or event, but they also can be used for strong user authentication—replacing or augmenting a standard password. This article explores what biometrics are, how they are being used as an authentication mechanism in the enterprise IT environment, what types of products are currently available, and what biometric standards are in place.

BY CATHERINE J. TILTON

Related Categories:

Authentication

Biometrics

Security

Visit www.dell.com/powersolutions
for the complete category index.

Despite the interest in biometric security solutions since the events of 9/11, much about biometric technology—and how it is being used as a strong authentication mechanism in an enterprise IT environment—is still not well understood. This article provides a high-level overview of biometric technology, how it is being used, its benefits, and some enterprise deployment considerations.

What are biometrics and how do they work?

Biometrics are defined as the automated recognition of individuals based on their biological or behavioral characteristics. Common forms of biometrics used for logical and physical access control include fingerprint, facial, iris, retina, speaker (voice), hand geometry, key-stroke, and handwriting recognition. Unique human characteristics are used to identify an individual or to verify an identity. Biometric authentication generally involves the latter—verifying or authenticating a user's claim of identity based on a one-to-one comparison of the presented biometric credential(s) to the registered (enrolled) biometric.

Because biometrics are designed to verify the claimed identity of a user and tightly bind an individual to an action or event, they can be used for strong user authentication in a workstation, network, or application—replacing or augmenting a standard password. Why would an enterprise implement a technology that appears to be excessive for a simple user login? In most cases, the rationale for using biometrics involves improved security, enhanced convenience, or lower cost when compared to traditional security measures.

Other authentication technologies—such as passwords, smart cards, keys, or certificates—rely on something an authorized individual knows or possesses. For each of these technologies, all that is truly known during an authentication event is that the correct information was presented to the system, not who was entering or holding that information. Biometric authentication, in contrast, involves a characteristic inherent to the physical person; users cannot forget, lose, write down, share, or guess their credentials. This tightly binds the credentials to a specific individual. And because biometric

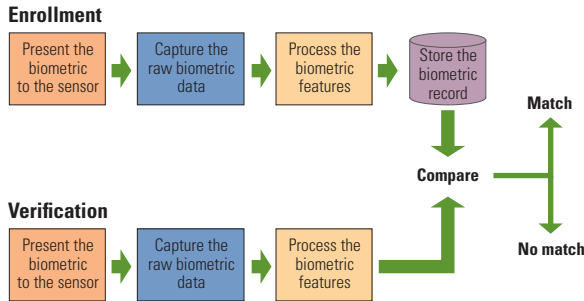


Figure 1. Biometric authentication process

authentication is convenient—credentials do not need to be carried around or remembered—users may be more likely to use the authentication mechanism as it was intended, without attempting to circumvent it.

Biometric authentication process

Biometric authentication involves two stages: the administrative process of initial biometric enrollment and the subsequent use of the live biometric for system access. In each case, the biometric sample is captured and processed. During enrollment, the resulting biometric record, or *template*, is securely stored for future matching; during verification, the live sample is matched against the previously enrolled record to determine whether access should be granted. Figure 1 depicts the biometric authentication process.

Biometric matching is not a binary comparison operation. When two biometric samples are compared, they are determined to have a level of similarity, which represents a probability that the samples came from the same person. This comparison results in a *matching score*, which is compared against a preset threshold criterion to determine whether the score is high enough to be declared a successful match.

Biometric authentication components

Implementing biometric authentication requires the following components: a capture device or sensor, secure storage for the enrolled template, and biometric algorithms that perform the processing and matching operations. These components can be acquired separately and integrated. Alternatively, enterprises can deploy packaged solutions, which are available for several common IT environments, such as the following:

- Microsoft® Windows® 2000 and Windows XP Active Directory® networks
- Novell® eDirectory™ environments
- Single sign-on implementations
- Remote access environments, such as Citrix applications

Capture devices include dedicated hardware, such as a single-purpose USB fingerprint scanner, and commodity devices, such as a high-resolution Webcam that can be used for facial recognition. They may also be integrated into other peripheral devices. Original equipment manufacturer fingerprint scanner units, for example, are integrated into a variety of devices—such as keyboards, mice, notebooks, personal digital assistants, cell phones, and memory sticks. Combination fingerprint scanners and smart-card readers are also available, and prototypes of smart cards with a silicon fingerprint chip integrated into the card itself are being developed. Figure 2 shows examples of biometric capture devices.

Which biometric is best?






Determining the type of biometric to implement can be difficult because this selection depends on what needs to be accomplished. The requirements of the application, user population, and environment drive the selection of biometric technologies—as well as cost. In addition to determining which type of biometric is most appropriate, enterprises should also consider the specific product because a wide range of high-quality and high-performance offerings exist. Figure 3 provides a high-level comparison of the most widely deployed biometric technologies today.

How are biometrics being used today?

As mentioned earlier, biometrics can verify the identity of a computer system user—that is, they can perform user authentication for logical access control. Authentication is distinct from authorization, which associates privileges or access rights with an identity once it is determined to be valid. Therefore, biometrics typically can be used anywhere passwords are used today. Besides large-scale government applications such as e-passports for border crossing and



Figure 2. Biometric capture devices

Type of biometric	What it does	Benefits	Disadvantages
Fingerprint 	Measures characteristics associated with the friction ridge patterns on fingertips	<ul style="list-style-type: none"> • One of the oldest and most widely used biometrics • Relatively high accuracy • Generally fast and easy • Many vendors and forms available 	<ul style="list-style-type: none"> • Dedicated device required • Small percentage of population have unusable prints • Occasional lingering criminal connotation
Face 	Measures characteristics of facial features	<ul style="list-style-type: none"> • Standard still photos or video capture can be used • Passive (“no-touch”) capture • Compatible with existing photo databases, such as those used for badging 	<ul style="list-style-type: none"> • Sensitive to lighting conditions • Sometimes affected by eye glasses, facial hair, or expression • Privacy objections to covert use, such as surveillance applications
Iris 	Measures the unique features of the random texture patterns of an iris	<ul style="list-style-type: none"> • Highly accurate; low false-match rate • Passive collection using infrared illumination • Users can wear glasses or goggles • Safe for eyes 	<ul style="list-style-type: none"> • Dedicated device required* • Users sensitive about subjecting their eyes to scanning process • Usability affected by cataracts • Frequently confused with retinal scanning
Voice 	Compares live speech with a previously created speech model	<ul style="list-style-type: none"> • Socially acceptable and nonintrusive • Standard components and audio channels can be used • Language independent • Interoperable with passphrases or challenge/response mechanisms 	<ul style="list-style-type: none"> • Background noise can interfere with capture • Illness and stress can impede effectiveness • Relatively long enrollment times • Large data record generated
Hand geometry 	Measures the dimensions of a hand, including the shape and length of fingers	<ul style="list-style-type: none"> • Deployed extensively for physical-access control and time and attendance • Fast and easy • Nonintrusive • Suitable for outdoor installation 	<ul style="list-style-type: none"> • Devices are bulky—not generally suitable for desktop use • Those with arthritis may find it difficult to use • Somewhat less accurate than other biometrics, but suitable for one-to-one verification

*Dual-purpose iris/video cameras are now available.

Figure 3. Comparison of biometric technologies

other law enforcement applications, biometrics have made great strides in several commercial sectors, such as healthcare, finance, and manufacturing.

Healthcare. With the requirements of the Health Insurance Portability and Accountability Act (HIPAA) now in effect, healthcare providers are using biometrics to provide the strong authentication necessary to protect personal health information such as medical records. This protection extends to administrative and clinical systems and applications, including mobile or wireless “bedside” platforms.

Finance. The financial industry is all about trust. In addition to normal fiduciary responsibility, the Gramm-Leach-Bliley Act requires financial institutions to design, implement, and maintain safeguards to protect customer information, and the Sarbanes-Oxley Act mandates stronger internal controls. Due diligence is causing financial institutions to consider biometrics for securing their infrastructures and providing strong authentication for transactions, document management, electronic signatures, and audit trails. Several Fortune 100 financial companies have each deployed biometric authentication solutions with 5,000 or more seats within the past several years.

Manufacturing. The manufacturing sector has two primary reasons to be interested in biometrics: protection of intellectual property, such as research and development information, and integrity of the manufacturing process. The latter is particularly important in the chemical and pharmaceutical sectors, which have strict regulatory requirements such as part 11 of the Title 21 Code of Federal Regulations (21 CFR Part 11). In each case, stronger access controls for the IT systems that house information or control processes help to address these concerns.

How do biometrics fit into an IT infrastructure?

The main architectural decisions for enterprises implementing biometric authentication involve where the biometric data should be stored and where the biometric matching operation should occur. Enterprises can choose from four possible locations for each process: a central server, the local workstation, the biometric device, or a token or smart card. Biometric products typically use a variety of implementations, such as server-based, client-based, and smart card-based architectures.

Server-based architectures. In this implementation, the biometric data is stored centrally, usually in a directory. The live biometric data is captured at the client and is securely transmitted to the authentication server, which retrieves the enrollment template from the directory, performs the biometric matching operation, and interacts with the network access control component to grant or deny access. This approach facilitates central administration, policy enforcement, and auditing; and it works well when network access is required. Credential caching schemes may be used in conjunction to support disconnected logins.

Client-based architectures. In this implementation, the biometric data is stored and matched on the client workstation. This architecture is ideal when access to a specific workstation is being protected; however, protection of the biometric data is required. The client-based implementation also works with certificate-based network logins, where the biometric is used rather than a password or personal ID number to protect the private key or signature certificate used in the authentication process—as, for example, in the Kerberos protocol.

Smart card–based architectures. Smart cards may be used to provide secure, portable storage of the biometric data, easing many privacy and security concerns. Some cards can even support biometric match-on-card, in which the biometric is both stored and matched on the card—resulting in either opening of the card for further authentication operations, such as the use of certificates, or returning the results for off-card authentication purposes.

Biometric standards

Work is progressing at the national and international levels in the area of biometric standards, most of which directly apply to their use in enterprise security. Within the United States, the International Committee for Information Technology Standards (INCITS) Technical Committee M1 addresses biometrics.¹ Since this committee's inception in November 2001, it has issued eleven ANSI standards in the areas of interfaces, data formats, and application profiles. At the international level, the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1, Subcommittee 37 (ISO/IEC JTC1 SC37) was formed in June 2002 to deal with biometrics.² Four projects within this ISO subcommittee have been approved and several others are at the Final Draft International Standard (FDIS) level, the last stage prior to approval.

One of the most important standards is the BioAPI specification, which defines a standard application programming interface (API) between a software application and the underlying biometric technology.³ This specification helps ensure interoperability and interchangeability within a biometric solution, preventing users from getting “locked in” to a particular technology or vendor and providing a level of plug-and-play capability for biometric products. In February 2002, version 1.1 was approved as ANSI INCITS 358-2002. Currently, more than 40 BioAPI-compliant products are available. The international version of BioAPI (version 2.0) is at the FDIS stage, but products compliant with this version are not expected to be immediately available.

Deployment considerations

Along with the many advantages of biometric authentication come some unique deployment considerations. First, an enterprise requires a complete biometric authentication solution—not just biometric technology. Some enterprises may attempt to deploy a bottom-up, device-oriented implementation; instead, they should implement an integrated top-down, requirements-driven business solution.


Next, biometrics are unique in that user participation is required to register the biometric on the system. Biometric enrollment may require face-to-face technical support and verification, unlike a password that can be given over a phone or an access card that can be handed out by a receptionist. Self-enrollment schemes that use a one-time password can overcome this issue, but security policy may require supervised enrollment. Training administrators to conduct proper enrollments can be critical to subsequent system performance.

In addition, biometric authentication requires a biometric sensor at the client workstation. For face, voice, signature, or typing biometrics, the sensor device may be built into the PC. However, for other biometric types, a new device must be attached; most are USB compatible. For networked environments, biometric software can be automatically delivered.

At times, temporary inability of the biometric system to acknowledge a legitimate user—caused by device failure or injury to the biometric feature—can prevent access. Backup mechanisms or procedures may be necessary to address this situation. Some individuals may have trouble enrolling or using a particular biometric because of a physical condition or disability. Therefore, a system that supports more than a single biometric device is generally preferable, especially across a large organization with a diverse user population.

Privacy issues can generally be avoided by putting in place—in advance of the deployment—a privacy policy delineating how the biometric data, which is considered personal information, will be handled and protected. In general, the policy should follow the Code of Fair Information Practices,⁴ stating the purpose of the data collection, prohibiting third-party sharing or other uses of the data, providing user access and change mechanisms, and taking adequate precautions to safeguard the data.

When should biometrics be implemented?

Biometric authentication technology is here today, with many choices of devices, architectures, and integrated solutions. Enterprises that require strong user authentication can deploy this technology as part of their end-to-end security architectures, but they should consider business requirements and existing infrastructures when selecting specific components. Implemented properly, biometrics can provide a cost-effective tool that offers numerous benefits to the security-conscious enterprise. 

Cathy Tilton is the vice president for Standards & Emerging Technologies at Daon, an identity assurance software company specializing in enterprise

¹ For more information about the INCITS Technical Committee M1, visit www.incits.org/tc_home/m1.htm.

² For more information about ISO/IEC JTC1 SC37, visit www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMIID=5537&scopelist=PROGRAMME.

³ For more information about BioAPI, visit www.bioapi.org.

⁴ For more information about the Code of Fair Information Practices, visit www.epic.org/privacy/consumer/code_fair_info.html.

solutions benefiting from an open, multi-modal, Web-based identity infrastructure. She is very active in the development of national and international biometric standards and currently serves as the head of the U.S. delegation to the ISO/IEC JTC1 SC37 subcommittee on biometrics. She also chairs the BioAPI Consortium and is an officer of the INCITS M1 technical committee on biometrics. Cathy has 25 years of engineering and management experience, including 12 years in the field of biometrics. She has a B.S. in Nuclear Engineering from Mississippi State University and an M.S. in Systems Engineering from the Virginia Polytechnic Institute and State University.

FOR MORE INFORMATION

Ashbourn, Julian, Nicholas M. Orlans, and Peter T. Higgins.
Biometrics: Advanced Identify Verification: The Complete Guide. Springer, 2000.

Avanti: The Biometric Reference Site:

www.jsoft.freeuk.com

Biometric Consortium:

www.biometrics.org

European Biometrics Forum:

www.eubiometricsforum.com

Find Biometrics:

www.findbiometrics.com

International Association for Biometrics:

www.iafb.org.uk

International Biometric Industry Association:

www.ibia.org

Jain, Anil K., Ruud Bolle, and Sharath Pankati, eds. *Biometrics: Personal Identification in Networked Society*. Kluwer, 1999.

Nanavati, Samir, Michael Thieme, and Raj Nanavati. *Biometrics: Identity Verification in a Networked World*. Wiley, 2002.

UK Communications Electronics Security Group

Biometrics Working Group: www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&displayPage=4

Wayman, James, Anil Jain, Davide Maltoni, and Dario Maio, eds. *Biometric Systems: Technology, Design and Performance Evaluation*. Springer, 2005.

Woodward Jr., John D., Nicholas M. Orlans, and Peter T. Higgins.
Biometrics: Identity Assurance in the Information Age. McGraw-Hill/Osborne, 2003.