International·Biometric·Group

Research Consulting Integration

Biometrics Explained

- Key biometric terms defined and discussed
- Complete answers to the most commonly asked (and *least* commonly asked) questions in biometrics
- Addresses performance, accuracy, privacy, security, strengths, weaknesses, and costs

ONE BATTERY PARK PLAZA, NEW YORK, NY 10004
TEL: (888) IBG-8-IBG FAX: (212) 809-6197
WWW.BIOMETRICGROUP.COM

Table of Contents

What is the definition of Biometrics? Why is biometrics hard to define?

Because biometrics can be used in such a variety of applications, it is very difficult to establish an all-encompassing definition. The most suitable definition of biometrics is

> *The automated use of physiological or behavioral characteristics to determine or verify identity.*

To elaborate on this definition, *physiological biometrics* are based on measurements and data derived from direct measurement of a part of the human body. Finger-scan, iris-scan, retina-scan, hand-scan, and facial-scan are leading physiological biometrics.

Behavioral characteristics are based on an action taken by a person. *Behavioral biometrics*, in turn, are based on measurements and data derived from an action, and indirectly measure characteristics of the human body. Voice-scan, keystroke-scan, and signature-scan are leading behavioral biometric technologies. One of the defining characteristics of a behavioral biometric is the incorporation of time as a metric – the measured behavior has a beginning, middle, and end.

It is important to note that the behavioral/physiological distinction is slightly artificial. Behavioral biometrics are based in part on physiology, such as the shape of the vocal chords (voice-scan) or the dexterity of hands and fingers (signature-scan). Physiological biometric technologies are similarly informed by user behavior, such as the manner in which a user presents a finger or looks at a camera. However, the behavioral/physiological distinction is a helpful tool in understanding how biometrics work and how they can be applied in the real world.

Biometrics are a*utomated* inasmuch as the processes involved in sample acquisition, feature extraction, record retrieval, and algorithm-based matching are computerized or machine-based. The result is that biometric decision-making is very rapid, and in most cases occurs in real-time.

How else can the term "biometric" be used?

Biometric *(noun)* - one of various technologies that utilize behavioral or physiological characteristics to determine or verify identity. *"Finger-scan is a commonly used biometric."* Plural form also acceptable: *"Retina-scan and iris-scan are eye-based biometrics."*

Biometrics *(noun)* – Field relating to biometric identification. *"What is the future of biometrics?"*

Biometric *(adjective)* – of or pertaining to technologies that utilize behavioral or physiological characteristics to determine or verify identity. *"Do you plan to use biometric identification or older types of identification?"*

Biometric system - the integrated biometric hardware and software used to conduct biometric identification or verification.

What types of biometrics exist?

Primary disciplines include:

- Finger-scan (optical, silicon, ultrasound, touchless)
- Facial-scan (optical and thermal)
- Voice-scan (not to be confused with speech recognition)
- Iris-scan
- Retina-scan
- Hand-scan
- Signature-scan
- Keystroke-scan
- Palm-scan (forensic use only)

Disciplines with reduced commercial viability or in exploratory stages include:

- DNA
- Ear shape
- Odor (human scent)
- Vein-scan (in back of hand or beneath palm)
- Finger geometry (shape and structure of finger or fingers)
- Nailbed identification (ridges in fingernails)
- Gait recognition (manner of walking)

How hard is it to use biometric technologies?

Biometrics are much easier to use than one might expect. Here is a brief technology-by-technology summary of how one interacts with biometric systems.

Finger-scan. When prompted, the user gently places his or her finger on a postage-stamp sized optical or silicon surface. This surface, known as a platen, is built into a peripheral device, mouse, keyboard, or PCMCIA card. The user generally must hold the finger in place for 1-2 seconds, during which automated comparison and matching takes place. After a successful match, the user has access to programs, files, or resources. Typical verification time from "system ready" prompt: 2-3 seconds.

Facial-scan. User faces the camera, preferably positioned within 24 inches of the face. Generally, the system will locate one's face very quickly and perform matches against the claimed identity. In some situations, the user may need to alter his facial aspect slightly to be verified.
Typical verification time from "system ready" prompt: 3-4 seconds.

Voice-scan. User positions him or herself near the acquisition device (microphone, telephone). At the prompt, user either recites enrollment passphrase or repeats passphrase given by the system.
Typical verification time from "system ready" prompt: 4-6 seconds.

Iris-scan. User positions him or herself near the acquisition device (peripheral or standalone camera). User centers eye on device so he or she can see the eye's reflection. Depending on the device, the user is between 2-18 inches away. Capture and verification are nearly immediate.

Typical verification time from "system ready" prompt: 3-5 seconds.

Retina-scan. User looks into a small opening on a desktop or wall-mounted device. User holds head very still, looking at a small green light located within the device.
Typical verification time from "system ready" prompt: 10-12 seconds.

Hand-scan. User places hand, palm-down, on an 8X10 metal surface with five guidance pegs. Pegs ensure that fingers are placed properly, ensure correct hand position.
Typical verification time from "system ready" prompt: 2-3 seconds.

Signature-scan. User positions himself to sign on tablet (if applicable). When prompted, user signs name in tablet's capture area.
Typical verification time from "system ready" prompt: 4-6 seconds.

Keystroke-scan. User types his or her password or passphrase.
Typical verification time from "system ready" prompt: 2-3 seconds.

What is involved with a biometric enrollment?

Biometric systems convert data derived from behavioral or physiological characteristics into templates, which are used for subsequent matching. This is a multi-stage process whose stages are described below.

Enrollment - the process whereby a user's initial biometric sample or samples are collected, assessed, processed, and stored for ongoing use in a biometric system. Enrollment takes place in both 1:1 and 1:N systems. If users are experiencing problems with a biometric system, they may need to re-enroll to gather higher quality data.

Submission - the process whereby a user provides behavioral or physiological data in the form of biometric samples to a biometric system. A submission may require looking in the direction of a camera or placing a finger on a platen. Depending on the biometric system, a user may have to remove eyeglasses, remain still for a number of seconds, or recite a passphrase in order to provide a biometric sample.

Acquisition device – the hardware used to acquire biometric samples. The following acquisition devices are associated with each biometric technology:

Technology	Acquisition Device
Finger-scan	desktop peripheral, PCMCIA card, mouse, chip or reader embedded in keyboard
Voice-scan	microphone, telephone
Facial-scan	video camera, PC camera, single-image camera
Iris-scan	Infrared-enabled video camera, PC camera
Retina-scan	proprietary desktop or wall-mountable unit
Hand-scan	proprietary wall-mounted unit
Signature-scan	signature tablet, motion-sensitive stylus
Keystroke-scan	keyboard or keypad

Biometric sample - the identifiable, unprocessed image or recording of a physiological or behavioral characteristic, acquired during submission, used to generate biometric templates. Also referred to as *biometric data*. The following sample types are associated with each biometric technology:

Technology	Biometric Sample
Finger-scan	fingerprint image
Voice-scan	voice recording
Facial-scan	facial image
Iris-scan	iris image
Retina-scan	retina image
Hand-scan	3-D image of top and sides of hand
Signature-scan	image of signature and record of related dynamics measurements
Keystroke-scan	recording of characters typed and record of related dynamics measurements

Feature extraction - the automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template. The feature extraction process may include various degrees of image or sample processing in order to locate a sufficient amount of accurate data. For example, voice-scan technologies can filter out certain frequencies and patterns, and finger-scan technologies can thin the ridges present in a fingerprint image to the width of a single pixel. Furthermore, if the sample provided is inadequate to perform feature extraction, the biometric system will generally instruct the user to provide another sample, often with some type of advice or feedback.

The manner in which biometric systems extract features is a closely guarded secret, and varies from vendor to vendor. Common physiological and behavioral characteristics used in feature extraction include the following:

Technology	Feature Extracted
Finger-scan	Location and direction of ridge endings and bifurcations on fingerprint
Voice-scan	Frequency, cadence, and duration of vocal pattern
Facial-scan	Relative position and shape of nose, position of cheekbones
Iris-scan	Furrows and striations in iris
Retina-scan	Blood vessel patterns on retina
Hand-scan	Height and width of bones and joints in hands and fingers
Signature-scan	Speed, stroke order, pressure, and appearance of signature
Keystroke-scan	Keyed sequence, duration between characters

Template – a comparatively small but highly distinctive file derived from the features of a user's biometric sample or samples, used to perform biometric matches. A template is created after a biometric algorithm locates features in a biometric sample. The concept of the template is one of biometric technology's defining elements, although not all biometric systems use templates to perform biometric matching: some voice-scan system utilize the original sample to perform a comparison.

Depending on when they are generated, templates can be referred to as enrollment templates or verification templates. Enrollment templates are created upon the user's initial interaction with a biometric system, and are stored for usage in future biometric comparisons. Verification templates are generated during subsequent verification attempts, compared to the stored template, and generally discarded after the comparison. Multiple samples may be used to generate an enrollment template – facial-scan, for example, will utilize several facial images to generate an enrollment template. Verification templates are normally derived from a single sample – a template derived from a single facial image can be compared to the enrollment template to determine the degree of similarity.

Just as the feature extraction process is a closely held secret, the manner in which information is organized and stored in the template is proprietary to biometric vendors. Biometric templates are not interoperable – a template generated in vendor A's finger-scan system cannot be compared to a template generated in vendor B's finger-scan system.

Do biometric systems result in exact, 100% matches?

One of the most interesting facts about most biometric technologies is that unique biometric templates are generated every time a user interacts with a biometric system. As an example, two immediately successive placements of a finger on a biometric device generate entirely different templates. These templates, when processed by a vendor's algorithm, are recognizable as being from the same person, but are not identical. In theory, a user could place the same finger on a biometric device for years and never generate an identical template.

Therefore, for most technologies, there is simply no such thing as a 100% match. This is not to imply that the systems are not secure – biometric systems may be able to verify identify with error rates of less than 1/100,000 or 1/1,000,000. However, claims of 100% accuracy are misleading and are not reflective of the technology's basic operation.

How do biometric systems determine whether two templates "match"?

Biometric decision-making is frequently misunderstood. For the vast majority of technologies and systems, there is no such thing as a 100% match, though systems can provide a very high degree of certainty. The biometric decision-making process is comprised of various components, as indicated below.

Matching - the comparison of biometric templates to determine their degree of similarity or correlation. A match attempt results in a *score* which, in most systems, is compared against a *threshold*. If the score exceeds the threshold, the result is a *match*; if the score falls below the threshold, the result is a *non-match*.

The matching process involves the comparison of the verification template, created upon sample submission, with the enrollment template(s) already on file. In 1:1 verification systems, there is generally a single verification template matched against an enrollment template. In 1:N identification systems, the single verification template can be matched against dozens, thousands, even millions of enrollment templates.

In most systems, enrollment and verification templates should never be identical. An identical match is an indicator that some sort of fraud is taking place, such as the resubmission of an intercepted or otherwise compromised template.

Score – a number indicating the degree of similarity or correlation of a biometric match. Traditional authentication methods – passwords, PINs, keys, and tokens - are binary, offering only a strict yes/no response. This is not the case with most biometric systems. Nearly all biometric systems are based on matching algorithms which generate a score subsequent to a match attempt. This score represents the degree of correlation between the verification template and the enrollment template. There is no standard scale used for biometric scoring: for some vendors a scale of 1-100 might be used, others might use a scale of –1 to 1; some vendors may use a logarithmic scale and others a linear scale. Regardless of the scale employed, this *verification score* is compared to the system's *threshold* to determine how successful a verification attempt has been.

Incidentally, many systems return a score during enrollment, referred to as an *enrollment score* or *quality score*. This score refers to how successful the extraction process was at finding distinctive features in the biometric sample. If the sample was rich in information, there will likely be a high enrollment score. This score is not used in the matching process, but might be used to determine whether a used can enroll successfully. A low quality score may indicate that the user cannot be reliable verified.

Threshold - a predefined number, often controlled by a biometric system administrator, which establishes the degree of correlation necessary for a comparison to be deemed a match. If the score resulting from template comparison exceeds the threshold, the templates are a "match" (though the templates themselves are not identical).

When a biometric system is set to low security, the threshold for a successful match is more forgiving than when a system is set to high security.

Decision – the result of the comparison between the score and the threshold. The decisions a biometric system can make include *match*, *non-match*, and *inconclusive*, although varying degrees of strong matches and non-matches are possible. Depending on the type of biometric system deployed, a match might grant access to resources, a non-match might limit access to resources, while *inconclusive* may prompt the user to provide another sample.

How are enrollment and verification templates compared - by looking at two numbers and seeing how close they are?

Biometric comparisons take place when biometric templates are processed by proprietary algorithms. These algorithms manipulate the data contained in the template in order to effect a valid comparison, accounting for variations in placement, background noise, etc. Without the vendor algorithm, there is no way to compare biometric templates – comparing the bits which comprise the templates does not indicate if they came from the same user. The bits must be processed by the vendor as a precondition of comparison.

Can biometric security levels be adjusted for specific transactions?

It is possible to vary the threshold from person to person and/or from transaction to transaction through *dynamic thresholding*. This automated process adjusts the verification threshold based on the specific conditions of a transaction. For instance, a score of 75 or higher might be sufficient to withdraw under $200 from an ATM, whereas a score of 90 or better may be required to withdraw $200 or more. Such dynamic thresholding allows systems to balance requirements for user convenience and system security.

What is the difference between identification and verification?

In day-to-day life most people with whom you do business *verify* your identity. You claim to be someone (your *claimed identity*) and then provide proof to back up your claim. For encounters with friends and family, there is no need to claim an identity. Instead, those familiar to you identify you, *determining* your identity upon seeing your face or hearing your voice.

These two examples illustrate the difference between the two primary uses of biometrics: identification and verification.

Identification (*1:N, one-to-many, recognition*) –the process of determining a person's identity by performing matches against multiple biometric templates. Identification systems are designed to determine identity based solely on biometric information. There are two types of identification systems: positive identification and negative identification.

Positive identification systems are designed to find a match for a user's biometric information in a database of biometric information. Positive identification answers the "Who am I?", although the response is not necessarily a name – it could be an employee ID or another unique identifier. A typical positive identification system would be a prison release program where users do not enter an ID number or use a card, but simply look at a iris capture device and are identified from an inmate database.

Negative identification systems search databases in the same fashion, comparing one template against many, but are designed to ensure that a person is *not* present in a database. This prevents people from enrolling twice in a system, and is often used in large-scale public benefits programs in which users enroll multiple times to gain benefits under different names.

Not all identification systems are based on determining a username or ID. Some systems are designed determine if a user is a member of a particular category. For instance, an airport may have a database of known terrorists with no knowledge of their actual identities. In this case the system would return a match, but no knowledge of the person's identity is involved.

Verification (1:1, matching, authentication) – The process of establishing the validity of a claimed identity by comparing a verification template to an enrollment template. Verification requires that an identity be claimed, after which the individual's enrollment template is located and compared with the verification template. Verification answers the question, "Am I who I claim to be?"

Some verification systems perform very limited searches against multiple enrollee records. For example, a user with three enrolled finger-scan templates may be able to place any of the three fingers to verify, and the system performs 1:1 matches against the user's enrolled templates until a match is found.

One-to-few. There is a middle ground between identification and verification referred to as one-to-few *(1:few)*. This type of application involves identification of a user from a very small database of enrollees. While there is no exact number that differentiates a 1:N from a 1:few system, any system involving a search of more than 500 records is likely to be classified as 1:N. A typical use of a 1:few system would be access control to sensitive rooms at a 50-employee company, where users place their finger on a device and are located from a small database.

What are the advantages and disadvantages of identification and verification? Is verification more accurate?

Deployers normally do not decide between identification and verification; instead, the objectives and operation requirements of a particular implementation mandate 1:1 or 1:N. Though identification systems do provide the maximum in user convenience, as they eliminate the need for a claimed identity, verification systems have several advantages. Verification is less expensive, more accurate, and faster than identification. However, certain types of deployments, especially public benefits programs, must utilize identification – the deployment would be nonsensical without positive and/or negative identification.

All biometric technologies are capable of verification. Identification systems can be based on finger-scan, facial-scan, iris-scan, and retina-scan, all physiological biometrics. Some of the differences between identification and verification deployments are as follows:

Processing Power: identification requires more processing power than verification, as identification systems execute large numbers of matches as opposed to one or two.

Accuracy: identification systems increase the likelihood of false matches - as more comparisons are being made, it is more likely that multiple users have similar physiological characteristics. In some environments, such as network or physical access, this can be a security risk, as a user may gain unauthorized access to a different user's account. False matches are not always problematic; if searching a database of known criminals returns three matches, one of which is correct, the effort involved in manually resolving the false matches is nominal.

Speed: identification systems will almost always take longer to process a request. Verification is expected to take place in seconds or fractions of seconds, while identification may take minutes, hours, even days.

User Convenience: It is generally easier for users to interact with an identification system since no user id is required.

How many users can be enrolled in a biometric system without encountering accuracy or performance problems?

The answer differs for verification and identification systems. Certain types of verification systems have no limits on potential growth. In a 1:1 system wherein matching takes place on a local PC or biometric reader, there is effectively no restriction on the number of users a system might incorporate. Spain has enrolled millions of users in its TASS program, allowing users to access government-related forms from finger-scan enabled kiosks. 1:1 systems in which matching takes place at a central server are more limited - there are few examples of central-matching deployments over 1,000 users. If a large number of authentication events are taking place at the same time, a possibility in a network access environment, the response time from the central verification server may be inadequate to meet user expectations. Biometric vendors have developed products capable of performing verification across multiple servers to address this issue.

Advances have been made in 1:N systems such that very large identification projects, some in the several tens of millions, are underway. These large-scale projects are generally based on finger-scan technology, although facial-scan is also capable of performing searches on large-scale databases. There are a number of steps that can be taken to increase the scalability of a 1-N system.

Binning is the process of separating biometric enrollments based on classifications inherent to the biometric data. In finger-scan systems, finger-scan templates with similar pattern types can be stored in a specific database segment, such that new templates with similar patterns only need be compared against this subset. This reduces the overall number of comparisons that need to be made. Similar processes, such as placing finger-scan classification data in the template's header file, allow for rapid large-scale searches.

Filtering is the process of using non-biometric information to limit the scope of a search. For instance, when a sample is submitted, the gender of the end user can be entered. This gender can be used as a filter to reduce the number of records that need be searched by half.

In large-scale 1:N systems, enrolling two fingers as opposed to one can increase maximum searchable database size from the tens of thousand to the tens of millions. The system can handle more enrollees, not only due to the increase in user-specific data, but to the ability to use more distinctive classification data.

In facial-scan, vendors often utilize more compact templates when conducting searches against very large databases, then employing a larger template when searching against a more manageable set of users.

What are common applications of biometrics?

Biometrics can be used anywhere keys, ID cards, PINs or passwords are currently used today. In addition, biometrics may be used where there are poor, manual or non-existent means of authentication. Biometrics can be used in a broad range of applications:

PC/LAN Logon - Many vendors have software which allows users to logon to PCs and local area networks, especially Windows NT. This reduces the user's need to remember and change passwords while reducing the administrator's need to frequently reset and manage passwords.

Application Logon - Biometrics can replace passwords required to access certain applications (e.g., email client). This automated logon process can be repeated for multiple applications and tied together with LAN logon, making biometrics the enabling technology in a 'single-sign-on' system.

Single sign on (SSO) - a process by which a single authentication is used to gain access to multiple applications or resources. The benefit of such a system is greater user convenience - not having to manage multiple passwords while reducing the time needed to access key applications. The drawback is that a single authentication event controls access to all applications and resources. Many companies are hesitant to use a simple password for single sign on, as the risk of compromise is significant. A biometric is a natural replacement for the password in a single-sign on implementation.

Some SSO applications provide partial sign-on functionality, for example to primary and network operating systems. These applications can be seen as reduced or consolidated sign on.

Time and Attendance - Hourly employees are often required to punch a time card when arriving and leaving work, as well as for breaks. A widespread problem, known as *buddy punching*, involves employees punching time cards for their friends who might be late or absent altogether from work. It is estimates that employers lose hundreds of millions of dollars annually to buddy punching. Adding a biometric to the time and attendance process effectively eliminates this type of fraud.

Access Control - Biometrics have long been used to protect a physical locations. In some cases entry to a facility is protected through a biometric at building entry. More frequently, specific rooms are secured with a biometric, as only certain employees have access to protected areas, and most building have areas considered semi-public.

Website Account Access and Purchasing - When considering the vast number of websites that require passwords, the value of transactions that take place through these sites, and the uncertainty involved in sending sensitive information over untrusted networks, it becomes clear that biometrics are a natural solution. Biometric logon reduces the need for users to remember multiple passwords for various sites (which can be difficult), using the same password for various sites (which can reduce security) or write down their passwords to various sites (which can significantly reduce security). In addition, for audit purposes, a biometric provides a very high degree of proof that an individual was indeed a party to a transaction. A transaction authorized with a password can be denied (*repudiated*) by a user stating that the password was guessed or stolen. Biometrics make repudiation significantly more difficult.

Double Dipping - For years public benefits disbursement programs have been plagued by people claiming benefits under multiple identities, a problem known as double dipping. Large-scale 1:N biometric systems can be designed to screen applicants to determine if they are already enrolled under a different name.

Verification to a token - with the increased storage and processing power available on smart cards, there is an increased need to verify that the bearer of the card is authorized to access its data. Biometrics can be used to verify that the person presenting a token is authorized to do so.

What is AFIS?

Automated Fingerprint Identification System (AFIS) is a biometric system that rapidly compares a one or more finger scan templates with a large database of templates. AFIS systems' most common use is in forensic applications, attempting to identify suspects out of local, state, or federal databases of known offenders. Civil AFIS is a type of rapid comparison system used in public service, as opposed to forensic, applications. AFIS describes a technology and a market.

How big is the biometric market?

The 1999 market size was approximately $58.4 million, and the expected 2003 market size is $594 million. These numbers do not include the forensic and AFIS markets, which are much larger.

The following chart illustrates the comparative market share of leading biometric technologies:

Source: International Biometric Group

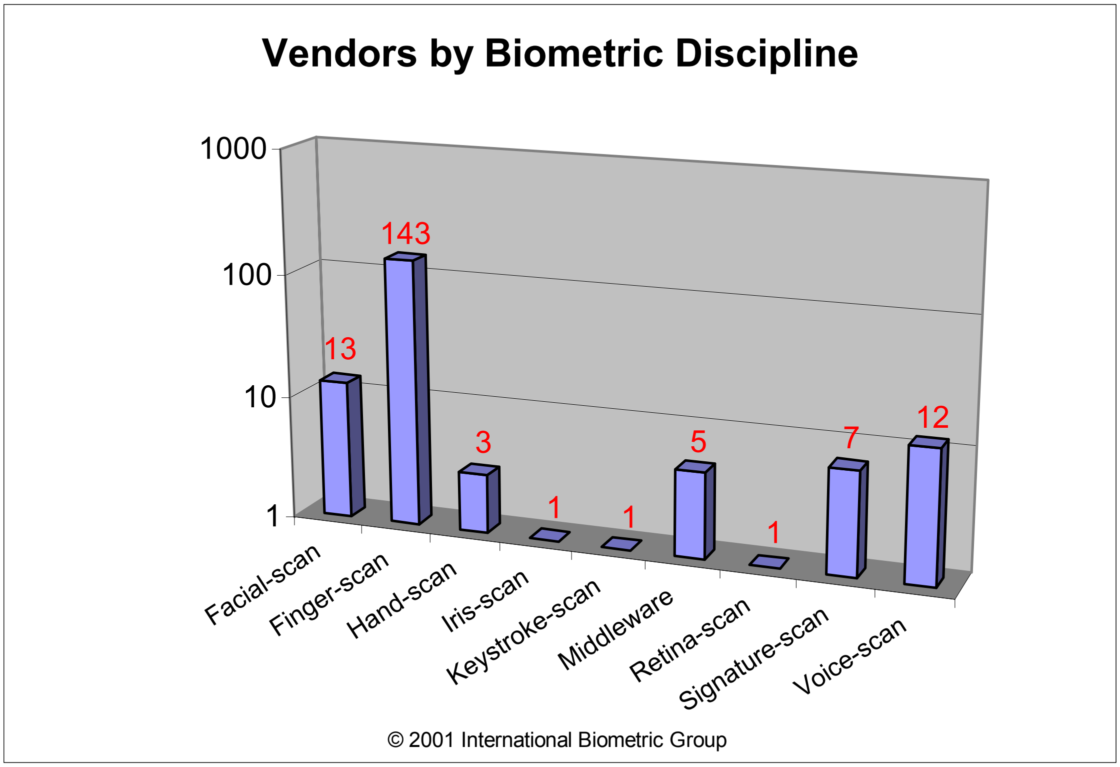
Technology	*2000*	*2001*
Finger-Scan	57.00	99.37
Facial-Scan	13.00	31.29
Hand-Scan	18.00	21.06
Middleware	11.50	24.20
Iris-Scan	9.00	12.64
Voice-Scan	6.00	8.78
Signature-Scan	3.00	5.46
Keystroke-scan	0.00	0.74
AFIS	282.00	320.35
Total	399.50	523.89

Source: International Biometric Group Market Report 2001-2005

How many biometric vendors are there?

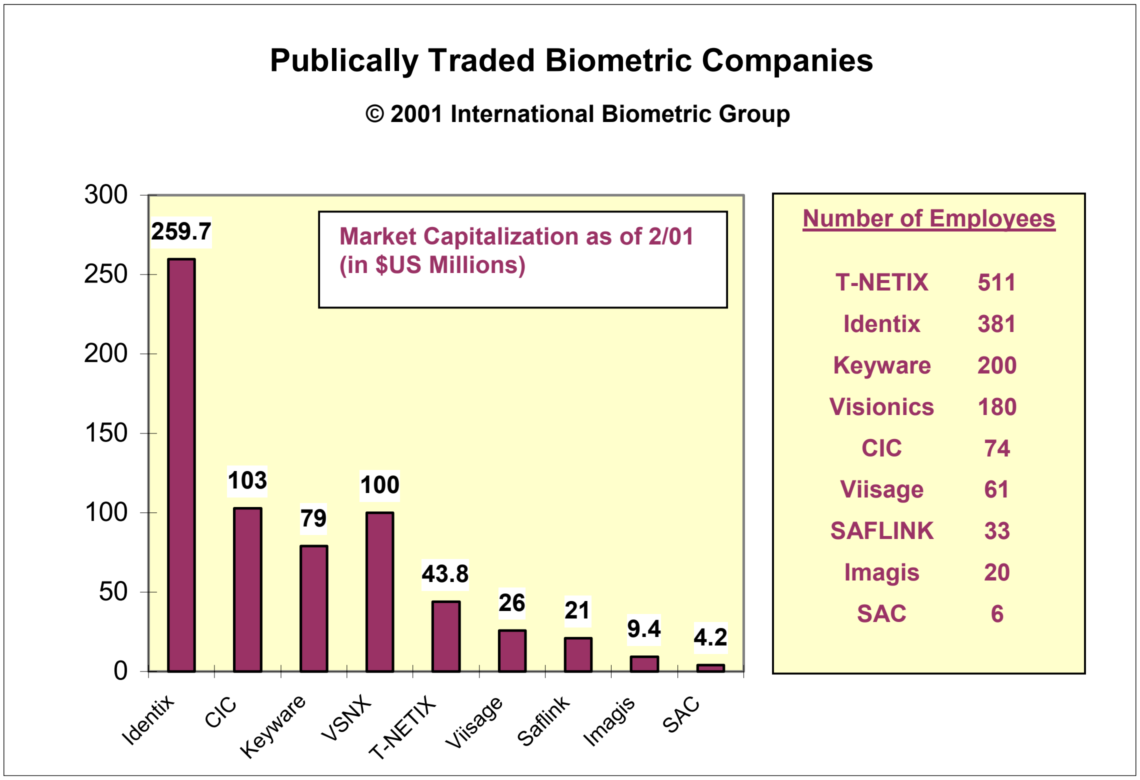
There are more than 200, depending on how one defines “vendor”. The broadest definition would be a company which manufactures or develops biometric hardware or software components. Companies such as Sony, Motorola and Fujitsu manufacture biometric readers, but clearly are not primarily biometric vendors. If one considers pure-play vendors whose primary business is selling biometrics, further definition is required. There are very small players developing technologies, some as small as one-man operations. The following chart represents the number of ‘substantial’ pure-play vendors, defined as a viable, ongoing operation dedicated to biometrics.

Note: many vendors fall into more than one category. These vendors have been classified by the category from which they derive the most revenue.



Are there any publicly traded biometric companies?

There are approximately 15 publicly trade biometric companies. When looking at these companies, keep in mind that not all of them are “pure-play” biometric vendors. Many sell non-biometric products and services and derive a large majority of their revenue for non-biometric sources. Also keep in mind that a number of very large companies sell biometrics but are not classifiable as biometric companies. The following chart represents the market capitalization and number of employees in 9 publicly traded biometric companies.


Publically Traded Biometric Companies

© 2001 International Biometric Group

Number of Employees	
T-NETIX	511
Identix	381
Keyware	200
Visionics	180
CIC	74
Viisage	61
SAFLINK	33
Imagis	20
SAC	6

What is a ‘middleware vendor’? What role do they play in the industry?

A middleware vendor produces software that lies between the core biometric technology, which performs sample capture, feature extraction, and biometric matching, and a given application, such as Windows NT, Novell, or a PKI system. Biometric middleware is designed to offer a deployer a variety of biometric and non-biometric authentication options, such that the deployer is not tied to a single core technology.

When will I see a biometric on every desktop?

Biometrics are slowly beginning to reach desktops in the form of very small and well-integrated scanners and sensors. Facial-scan technology works through standard peripheral cameras already shipping with PCs, voice-scan works through standard PC microphones, and finger-scan utilizes postage-stamp sized scanners integrated into keyboards, laptops, mice and PCMCIA cards. Major manufacturers such as Dell, Compaq, Toshiba, and IBM have started to ship biometrics as part of their systems.

Biometric technology is still unfamiliar to most, but is becoming more visible every day. Expect that by the end of 2005 there will be one or more biometric technologies shipped as a part of every new PC system.

What is the role of biometric in mobile and wireless commerce? Can I expect to see biometrics on mobile phones and PDAs?

As the value of transactions that can be accomplished on personal electronic devices increases, the demand for stronger authentication will start to increase. We are starting to see the first PDA add-on biometric components and should expect to see many biometrically enabled mobile devices by 2005. However, it is premature to suggest that m-commerce will be a very large growth area for biometrics. Biometrics must prove themselves in the comparatively less challenging area of standard PC-based e-commerce before companies can realistically consider deploying the technology in m-commerce environments.

What will be the driving force behind a widespread deployment of biometrics?

The answer differs for each type of biometric deployment. For physical access, less expensive devices which easily integrate into current building management systems will make biometric deployment more appealing. For e-commerce, increasingly visible security breaches will lead merchants to incorporate biometrics on their site as a way to draw more strongly authenticated customers. For internal IT security, similarly, an increased emphasis on best security practices will lead to a revision of authentication processes, currently one of the areas most susceptible to intrusion. Authentication, to this point, has been viewed as a secondary requirement in the enterprise, but as more resources are made accessible on internal and external networks, authentication demands will increase significantly. While the demand for biometric technology increases, the cost, ease-of-use, and accuracy are improving to the point where biometrics are not an “if” technology but a “when” technology.

What has been holding biometrics back from wide scale adoption?

Millions of people have used biometrics, and they are an everyday part of life for hundreds of thousands of employees, citizens, and purchasers. At the same time, biometrics are a very young technology, with most technologies having only recently reached the point where basic matching performance could be considered acceptable for real-world deployment.

There is also a great deal of skepticism regarding biometric technology: does it work? Can it track me? Is it worth deploying in place of existing systems? Will it crash my network or PC? Until very prominent successful deployments become known to potential deployers, the industry will face question on the viability of the technology.

Lastly, the question of need. Are biometrics necessary, or just overkill? Passwords have worked reasonably well for two decades; keys still open doors; fraud in large-scale systems can be reduced by non-biometric methods. Until there is a general consensus that biometrics are necessary as opposed to just new, biometrics will not be adopted on a large scale.

What are the benefits of using a biometric system?

There are many types of biometric systems, all of which are designed to offer improved authentication. Some of the primary benefits of using biometrics include the following:

<u>For employers</u>
Reduced costs – password maintenance
Reduced costs – no buddy punching
Increased security – no shared or compromised passwords
Increased security – deter and detect fraudulent account access
Increased security – no badge sharing in secure areas
Competitive advantage – familiarity with advanced technology

<u>For employees</u>
Convenience – no passwords to remember or reset
Convenience – faster login
Security – confidential files can be stored securely
Non-repudiation – biometrically transactions difficult to refute

<u>For consumers</u>
Convenience – no passwords to remember or reset
Security – personal files, including emails, can be secured
Security – online purchases safer when enabled by biometric
Privacy – ability to transact anonymously

For retailers (online and point-of-sale)
Reduced costs – biometric users less likely to commit fraud
Competitive advantage – first to offer secure transaction method
Security – account access much more secure than via password

For public sector usage
Reduced costs – strongest way to detect and deter benefits fraud
Increased trust – reduced entitlement abuse

When will we see biometrics in our day-to-day activities? Which biometric will it be?

Biometric are being used by hundreds of thousands of people on a daily basis. Over the next decade, biometrics will grow to be a part of the everyday fabric of life. Biometric devices and systems will be available for your office, home, car, computer, and for retail and online purchases. Most technologies available today will find use in a variety of applications – no single biometric will supplant all others. However, it will be difficult for new biometric technologies to supplant those already developed and in use, unless they offer a highly compelling combination of cost, ease-of-use, and accuracy.

What happens when a biometric system rejects authorized users?

Depending on the nature of the deployment, the results of a false rejection can be minor or severe. Some systems reject (i.e. falsely declare a non-match) a modest percentage of users as a byproduct of extremely high security requirements. Many systems offer fallback authentication, whether to a live operator, a password, or another biometric method.

The odds of correctly guessing a PIN from a debit or ATM card are 1 in 10,000. Should I expect a PIN-replacement biometric to be more accurate?

A typical 4-digit pin code is typically thought to have a false accept rate of 1 in 10,000 (10x10x10x10=10,000). Some groups have used this as a basis for establishing minimum false acceptance rates for biometric technology, proposing that a biometric should not be any less secure than a PIN. This logic is flawed for several reasons. Most PIN numbers are not compromised through brute force attacks or random guessing. PIN numbers are written down and stored with cards, and are often stolen along with wallets. PIN numbers are also ascertained by shoulder surfing or by informed guesswork – date and month of birth, for example. Since PIN numbers can be shared, lost, and written in identifiable form, they simply do not provide a 1 in 10,000 false match rate in the real world.

Since biometrics cannot be shared or lost, they are much less susceptible to compromise than a 4-digit PIN code. Therefore, in terms of establishing accuracy requirements, setting a blanket standard for all ATM transactions seems counterintuitive. For low-risk transactions – less than $100 – there may be no need to have a false match rate as low as 1 in 10,000.

For better or worse, biometric usage brings security and accuracy not directly comparable to those involved in PIN usage. Using PIN-oriented criteria when evaluating biometric accuracy requirements is misleading and obscures more relevant issues.

Are biometrics privacy-invasive or privacy-protective?

Biometrics, like any technology, are defined by their usage. An analogy to databases is instructive. Databases can be used to link personal information from disparate sources without user consent and are the source of much of the privacy world's concern about information aggregation and misuse. Are databases privacy-invasive? No. It is the specific use to which they are put, and the systemic and operational controls (or lack thereof) which define whether databases are privacy-invasive. The same can be said for biometric technologies.

There is too broad a variety of biometric technologies, deployments, and systems to make any all-encompassing statements on the relationship between biometrics and privacy. In particular environments, the use of biometrics can be privacy-invasive, although a large number of intrinsic and extrinsic protections exist which significantly reduce the likelihood of biometrics being used in a privacy-invasive fashion. In many environments, biometrics are thought to enhance privacy.

What are commonly expressed fears regarding biometrics and privacy?

The basic classifications of privacy are *personal* and *informational*. It is rare that objections to biometric are expressed systematically: it is much more likely that objections to biometrics are called "slippery slope" or "Big Brother" without further elaboration.

Personal Privacy. For some people, the use of biometrics is seen as inherently offensive. Being required to verify one's identity through a finger-scan or voice-scan can be seen as intrusive, impersonal, or mistrustful. These objections to biometrics are based on *personal privacy*.

Informational Privacy. A more common objection to biometrics is based on informational privacy: how biometric data might be misused, tracked, linked, and otherwise abused. Potential privacy-invasive misuses of biometrics are as follows:

<u>Unnecessary or unauthorized collection</u> – gathering biometric information without the user's permission or knowledge, or gathering biometric data without explicitly defined purposes
<u>Unauthorized use</u> – using biometric information for purposes other than those for which it was originally acquired
<u>Unauthorized disclosure</u> – sharing or transmitting biometric information without the user's explicit permission
<u>Unique identifier</u> – using biometric information to track a user across various databases, to link different identities, and to amalgamate personal data for the purposes of surveillance or social control
<u>Improper storage</u> – storing biometric information in logical proximity to personal data such as name, address, social security number
<u>Improper transmission</u> – transmitting biometric information in logical proximity to personal data such as name, address, social security number

Forensic usage – using biometric information to facilitate investigative searches, which may be categorized as unreasonable search and seizure
Function creep – gradually using biometric data for a variety of purposes beyond its original intention and scope

Are biometrics unique identifiers?

No. Unique identifiers are exceptionally problematic from a privacy perspective, as they make possible the linking of information in separate databases. Social security and social identification numbers are used in this way, although they were not intended to be used as such.

Physiological characteristics such as fingerprints, iris patterns, and retinal patterns are thought to be unique – in theory, no two people share identical fingerprints, irises, or retinal patterns. They are also highly stable, changing only through wear and tear (fingerprints) or injury and disease (iris, retina). It comes as a surprise that the templates generated from these stable biometric samples vary from day to day, minute to minute, and second to second.

As opposed to being a consistently replicable string of data, such as a social security number, biometric templates vary with each biometric placement or recording: the same finger, placed over and over again, generates a different template each time. Without a matching algorithm to make sense of these templates, they would appear to be unrelated – a large percentage of the data changes with each placement. The idea that the same number (i.e. template) will exist in every biometric system in which a user enrolls is inconsistent with the technology's basic operations.

If biometrics were unique identifiers, there would never be false matches; however, every technology suffers false matches at some point. Because of the variance in template quality, there is always the possibility that a comparison of two templates will result in a false non-match. Oddly, the fact that biometric template generation is not perfect helps ensure that biometrics do not facilitate multi-database tracking.

Biometric templates, then, are highly reliable identifiers, but they are not unique identifiers. The more relevant question is whether biometrics can be used as semi-unique identifiers. At this point, such usage would be exceptionally difficult, but cannot be ruled out. In order for biometric data to be tracked across multiple databases (i.e. to function as a unique identifier), a single biometric vendor would have to supply all of the core technology; different finger-scan vendors' templates are not interchangeable or comparable. Assuming that only one biometric company provided the core matching technology for all systems, the companies managing the databases – employers, retailers, trusted third party providers - would need to access vendor source code in order to match templates. Even with the complicity of the biometric vendor and the companies responsible for storing and managing personal data, the ability to compare against large databases is limited by the enrollment quality and by the actual finger enrolled. A user who uses the left index at home and the right index at work renders even this theoretical risk moot.

All of this assumes that the biometric templates are stored centrally. There are many situations in which central storage is desirable or necessary, others where it is best to decentralize stored biometric data. Many deployments will give the users themselves control over data in the form of tokens or smart cards.

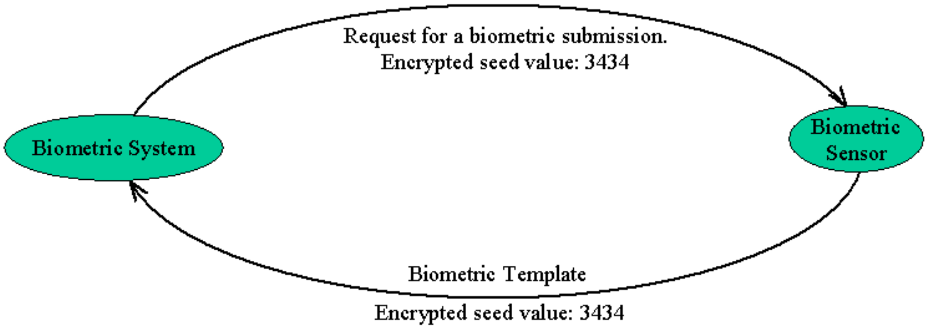
Are biometric templates secrets? If my template is compromised, does that mean that I can never use that biometric again?

Not in a well-designed system. If a criminal steals or guesses your password, it is very easy to have it changed. There is a fear, however, that if a criminal gets hold of a biometric template, the damage is irreparable - there is no way to change that part of your body. Although templates are often encrypted when in transit and storage in order to protect against such an occurrence, what happens if a template is compromised?

The answer depends on how well a biometric system is designed. If a system allows a template to be inserted into the verification process without ensuring that this template came from an actual placement, a compromised template can pose a problem. However, a well-designed system will ensure that the information it is analyzing is not a recording but is in fact a new sample.

One way to assure that a new template is being submitted is to seed the request for a sample. This involves the biometric system sending an encrypted random number (known as a seed) to the biometric sensor. This number can be encrypted such that only the sensor itself can decrypt the message. When returning the biometric template, the sensor also sends the seed number back (encrypted). This ensures that the template being sent was created immediately after the request for the template (as opposed to an old template that has been recorded and played back).

The following chart illustrates a request for a biometric sample with a seed value of 3434.


Request for a biometric submission.
Encrypted seed value: 3434
Biometric System
Biometric Sensor
Biometric Template
Encrypted seed value: 3434

Note that biometric templates cannot be used to regenerate original biometric data.

Do systems check for live body parts?

Hollywood movies have illustrated many ways to defeat biometric systems. One such way involves stealing someone's body part (e.g., cutting off a finger or gouging out an eye) to attempt to circumvent the system. In reality, the various disciplines of technology have different ways to check for live samples. We should emphasize that the goal of live samples detection is not to check for dead body parts. Instead, live detection is designed to prevent use of a token – a sharable item such as a fake finger or mask capable of defeating biometric systems.

Finger-scan - There are many different ways that finger samples are acquired. Some systems rely on the unique conductive nature of a live finger. Others measure blood flow or ensure the ridges at the periphery of the print are arrayed as is normal in live finger placement.

Voice-scan - Some voice scan systems can generate a random sequence of numbers for each verification. This makes it difficult to utilize a pre-recorded voiceprint. Lower fidelity recording devices are also generally incapable of capturing the high and low frequencies necessary to verify.

Facial-scan - Facial-scan systems can require users to change their facial expressions (e.g., blink eyes or smile) in order for a template to be successfully generated.

Iris-scan - Iris-scan systems can vary the amount of light shone on the eye and record the dilation of the pupil.

Retina-scan - Within minutes of death, the vein structure of the retina would likely deteriorate to the point that a retina-scan would no longer authenticate a user.

Hand-scan - Hand-scan does not check for a live biometric sample. Theoretically, an amputated hand would be able to verify on a hand-scan system, although the fingers would need to be positioned such that they are placing pressure on the correct pegs.

Signature-scan - There is no way to generate a ‘dead’ signature.

Can biometrics systems be defeated?

Absolutely. Many claim that a well built biometric system cannot be broken into. This is untrue, and does a disservice to the biometric industry. Every biometric can be defeated if one allows a sufficient amount of time, money, and attempts. Employing biometrics raises the bar for potential thieves, imposters, and fraud perpetrators to the point where the costs of defeating the system may not justify the rewards. Biometrics are a part of an overall security philosophy, and without thoughtful deployment may be easier to defeat than existing systems.

Will biometrics still work if I have a cold or a cut on my finger?

An introduction to the IBG Strike System.

Biometric system performance varies according to sample quality and the environment in which the sample is being submitted. While it is not possible to definitely state if a biometric submission will be successful, it is possible to locate factors which can reduce affect system performance. The Strike System details, technology-by-technology, aspects that work against a successful verification. Some of these strikes are listed below.

Finger-scan

Cold finger
Dry/oily finger
High or low humidity
Angle of placement
Pressure of placement
Location of finger on platen (poorly placed core)
Cuts to fingerprint
Manual activity that would mar or affect fingerprints (construction, gardening)

Voice-scan

Cold or illness which affects voice
Different enrollment and verification capture devices
Different enrollment and verification environments (inside vs. outside)
Speaking softly
Variation in background noise
Poor placement of microphone / capture device
Quality of capture device

Facial-scan

Change in facial hair
Change in hairstyle
Lighting conditions
Adding/removing hat
Adding/removing glasses
Change in weight
Change in facial aspect (angle at which facial image is captured)
Too much or too little movement
Quality of capture device
Change between enrollment and verification cameras (quality and placement)
'Loud' clothing that can distract face location

Iris-scan

Too much movement of head or eye
Glasses
Colored contacts

Retina-scan

Too much movement of head or eye
Glasses

Hand-scan

Jewelry
Change in weight
Bandages
Swelling of joints

Signature-scan

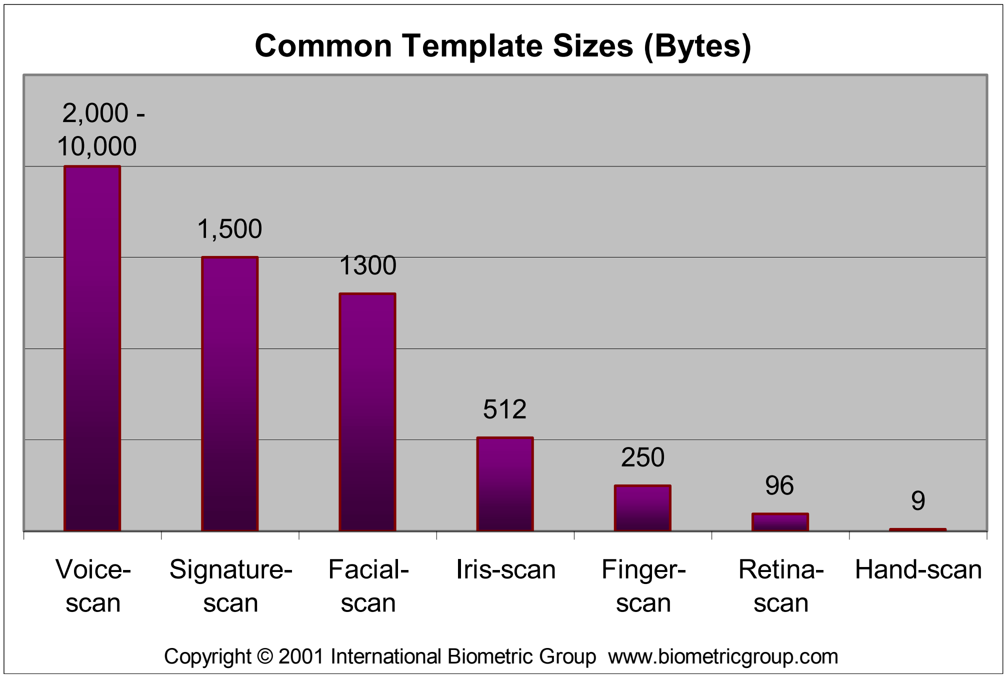
Signing too quickly
Different signing positions (e.g., sitting vs. standing)

In addition, for many systems, an additional strike occurs when a long period of time has elapsed since enrollment or since one's last verification. If significant time has elapsed since enrollment, physiological changes can complicate verification. If time has elapsed since a user's last verification, the user may have "forgotten" how he or she enrolled, and may place a finger differently or recite a passphrase with different intonation. For the most part, a single strike will probably not materially affect the performance of a given system. However, as you have more and more strikes for a given submission, your chances of a successful verification diminish.

These strikes do not include inherent characteristics such as age, ethnicity, or gender which can also affect system accuracy. The performance of many biometric systems varies for certain populations.

What is the size of a template?

The size of a template varies by technology and vendor. The chart below depicts the typical sizes for the leading biometric technologies. In some instances, specific vendors may utilize larger or smaller templates depending on the requirements of a given application. Template size can also vary depending on the size of the sample, such as the signature length and complexity, the length of a voice passphrase, or the number of characters in a typed password.



Should I use biometrics, smart cards or encryption?

In many enterprises, there is a role for all three technologies, as each plays a different role. Biometrics are primarily concerned with user authentication, smart cards with storage and portability of data, and encryption with data security and privacy. Instead of considering whether one or the other technology is appropriate for their needs, enterprises are increasingly considering combinations of biometrics, smart cards, and encryption to address their authentication needs.

There is a perception that these are competing technologies, as both smart cards and encryption (specifically Public Key Infrastructure) *implicitly* verify the identity of a party to a transaction. However, smart cards verify possession, not identity; when protected with traditional passwords and PINs they are as susceptible to compromise as a standard password/PIN methodology. PKI verifies the presence and match between a public and private key, but only does not verify the identity of the key owner. If strong user authentication is an important component of your data security processes, biometric technology is a necessity.

Why is proper enrollment so important?

The enrollment process creates the template against which all future verifications will take place. Poor submissions during enrollment can lead to a high False Rejection Rate during verifications. It is critical that the enrollment process is carefully conducted.

In many deployments, it is also important that the enrollment process includes a careful verification of the end users' identity. Biometrics can only verify claimed identities, and have no way of knowing if the person submitting enrollment samples is who they claim to be. If a fraudulent identity is claimed upon system enrollment, or a true identity is claimed fraudulently (identity theft), the imposter will be able to verify successfully from that point forward. 1-N systems can determine whether a person is already enrolled, but cannot determine which identity or identities is false. Systems which allow user anonymity are not concerned with establishing identity.

Can an enrollment template ever be updated?

Some systems are capable of updating enrollment templates after each successful verification. For instance, a signature sample might be close enough to the enrollment template to successfully match, but may also contain slightly altered features. These features can be incorporated back into the enrollment template to allow for more accurate matching on the next attempt. As time goes on, the slight changes made to the template may result in significant changes to the enrollment. In fact, it is possible that a signature verified at one point may not be verified years later after the enrollment template has incorporated many temporal changes.

What is the difference between forensic fingerprinting technology and biometric finger-scan technology?

Many people think of forensic fingerprinting as an ink and paper process. While this may still be done in some locations, most jurisdictions utilize optical scanners known as *livescan* systems. There are some fundamental differences between these forensic fingerprinting systems (used in *AFIS* systems) and the biometric finger-scan systems used to logon to a PC:

Response time - AFIS systems may take hours to match a candidate, while finger-scan systems respond with seconds or fractions of seconds.

Cost - an AFIS capture device can range from several hundred to tens of thousands of dollars, depending on whether it is designed to capture one or multiple fingerprints. A PC peripheral finger-scan device generally costs less than $200)

Accuracy - an AFIS system might return the top 5 candidates in a biometric comparison with the intent of locating or questioning the top suspects. Finger-scan systems are designed to return a single yes/no answer based on a single comparison.

Scale – AFIS systems are designed to be scalable to thousands and millions of users, conducting constant 1:N searches. Finger-scan systems are almost invariably 1:1, and do not require significant processing power.

Capture – AFIS systems are designed to use the entire fingerprint, rolled from nail to nail, and often capture all ten fingerprints. Finger-scan systems use only the center of the fingerprint, capturing only a small fraction of the overall fingerprint data.

Storage – AFIS systems generally store fingerprint images for expert comparison once a possible match has been located. Finger-scan systems, by and large, do not store images, as they are not used for comparison.

Infrastructure – AFIS systems normally require a backend infrastructure for storage, matching, and duplicate resolution. These systems can cost hundreds of thousands of dollars. Finger-scan systems rely on a PC or a peripheral device for processing and storage.

Can you recreate an image of the sample from a template?

Most vendors indicate that this is not possible. The template represents various measurements of the sample and is usually not a 'description' of the sample. However, it cannot be stated with absolute certainty that images cannot be rebuilt in some fashion – the rebuilt image may be a poor likeness, but it is possible that some features can be reverse-engineered with access to vendor source code.

Why would I want to use two or more biometrics? Does it increase my level of security?

A biometric system which offers more than one core technology for user authentication is referred to as multimodal (in contrast to monomodal). Many vendors suggest that multimodal systems can offer more security for the enterprise and convenience for the end user. There are three types of multimodality in the biometric world: synchronous, asynchronous, and either/or.

Either/or multimodality describes systems which offer multiple biometric technologies, but only require verification through a single technology. For example, an authentication infrastructure might support facial, voice, and finger-scan at each desktop and allow users to verify through any of these methods. A number of vendors have developed enabling middleware which allows for authentication by means of various biometrics. The benefit of this system is that biometrics, instead of passwords, can be used as a fallback. To have access to either/or multimodality, a user must enroll in each technology. To use finger, face, and voice, for example, one must become familiar with three devices and three submission processes. As a key performance indicator in biometrics is ease-of-use, requiring familiarity with multiple processes can be problematic.

Asynchronous multimodality describes systems which require that a user verify through more than one biometric in sequence. Asynchronous multimodal solutions are comprised of one, two, or three distinct authentication processes. A typical user interaction will consist of a verification on finger scan, then face if finger is successful. The advantage of added security – it is highly unlikely that a user will break two systems – is offset by a reduction in convenience. In addition to the time required to execute these separate submissions correctly (such verification can require 10 seconds of submission) the user must learn multiple biometric processes, as in either/or systems. This can be a challenge for both physical and logical access scenarios.

Synchronous multimodality involves the use of multiple biometric technologies in a single authentication process. For example, biometric systems exist which use face and voice simultaneously, reducing the likelihood of fraud and reducing the time needed to verify. Systems which offer synchronous multimodality can be difficult to learn, as one must interact with multiple technologies simultaneously.

A great deal of thought has gone into whether multiple biometrics are more or less accurate than a single biometric. Much of the debate fails to take into account the fact that the process flow of enrollment and verification are as relevant to real-world performance as the underlying statistical bases for performance. It is rare that multiple biometric technologies will be used at a single authentication point (i.e. a door, a desktop) within an enterprise. It is likely, however, that various technologies will be deployed in suitable environments – voice for telephony-based verification, finger for PC-oriented verification, etc.

What performance metrics should I look at?

There are almost as many performance metrics as there are biometrics. Unfortunately there is no single metric which indicates how well a system will perform. Analysis of multiple metrics is necessary to determine the strengths and weaknesses of each technology and vendor under consideration for a given application. It should also be noted that the processes unique to various applications have a great effect on performance metrics. Testing which generates system performance metrics is most valuable when it emulates real-world application environments.

Key performance metrics include the following:

Failure to Enroll (FTE) Rate - the probability that a given user will be unable to enroll in a biometric system due to insufficiently distinctive biometric sample(s). Users incapable of providing biometric data, such as amputees, are normally not counted in a system's FTE rate.

False Match Rate (FMR) - the probability that a given user's verification template will be incorrectly judged to be a match for a different user's enrollment template. Also referred to as false acceptance rate, terminology that does not always apply to 1:N systems.

False Non-Match Rate (FNMR) - the probability that a user's verification template will be incorrectly judged to not match that same user's enrollment template. Also referred to as false rejection rate, terminology that does not apply to 1:N systems. In a 1:1 system, FNMR is the probability that User 1 will not verify against his or her own template. In a 1:N system FNMR is the probability that a user whose enrollment template is located in a database will not be matched in a search.

All three metrics must be investigated as opposed to just one or two of them. Reliance on one or two metric without the third can be highly misleading. Using only selected performance metrics will generate a false sense of the system's actual capabilities. The three metrics are strongly related, such that as you raise or lower any one, the others will be affected. Decreasing the FMR, or making the system less susceptible to imposters, results in an increased likelihood that legitimate users will be rejected (false non-match rate). Decreasing the FTE by allowing a higher percentage of subject to enroll successfully leads to higher FNMR, as users with low-quality biometric samples have an increased presence in the system. These metrics also change when system thresholds are adjusted.

The following are derived metrics, generated from analysis and comparison of FMR, FNMR and FTE.

Equal Error Rate (EER, crossover) - the rate at which the FAR is equal to the FRR. If a system's thresholds are set to the Equal Error Rate, the exact same number of people will be falsely rejected as falsely accepted. If such performance is important to your application, then the EER will be a vital statistic. In reality, it tends to oversimplify the balance between FAR and FRR and should be used with caution. There are few applications in which a system administrator has an identical need for security and convenience.

Receiver Operator Curve (ROC) - a visual representation of FAR and FRR rates at varying thresholds.

Ability to Verify (ATV) - see below.

Ease of Use – Though not a traditional performance metric, ease of use is affected by performance-related adjustments. Steps taken to improve performance tend to decrease the ease of use. Requiring multiple submissions, or compelling the user to submit more carefully, will each increase system performance. They also serve to make the system more tedious and cumbersome to use.

What percentage of my user population will be able to use a given biometric system?

Exception processing is the method of authentication employed for users incapable of successful biometric authentication. Exception processes can be secondary biometric technologies, passwords, PINs, or live verifications. Some deployments can afford a high exception processing rate, whereas others would be rendered inoperable if a large percentage of users required alternative verification. In any case, it is absolutely certain that some percentage of users – perhaps 0.5%, perhaps 10% - will be incapable of using a system successfully. Proper system design accounts for these users without reducing overall system security or penalizing users for being unable to verify with a specific piece of biometric technology.

The likelihood that a deployment will require a great deal of exception processing can be determined by referencing a technology's *Ability to Verify* rate. This is not a commonly used metric within the biometric industry, but is very helpful in understanding real world system performance. The ATV rate represents the percentage of users who will have to be handled with a special fall back process. The rate is simply a combination of the FTE and the FNMR:

ATV = (1-FTE)(1-FNMR)

This metric can be thought of as representing the group of users who cannot enroll (FTE) along with users falsely rejected by the system (FRR). No system has a 100% ATV rate, but in general, a high ATV rate will make for a more effective system. When balanced with an acceptable False Match Rate, ATV can be extremely useful because it is has an impact on three key aspects of biometric deployments:

1) <u>Cost</u>. One of the most expensive aspects of a biometric system is the cost involved with exception processing. Any user unable to be processed by the biometric needs to be processed by a 'fall-back' procedure, meaning that dual systems must be maintained. Whether an alternate biometric, a password, or a live verification, there is a need for a separate enabling and support infrastructure.

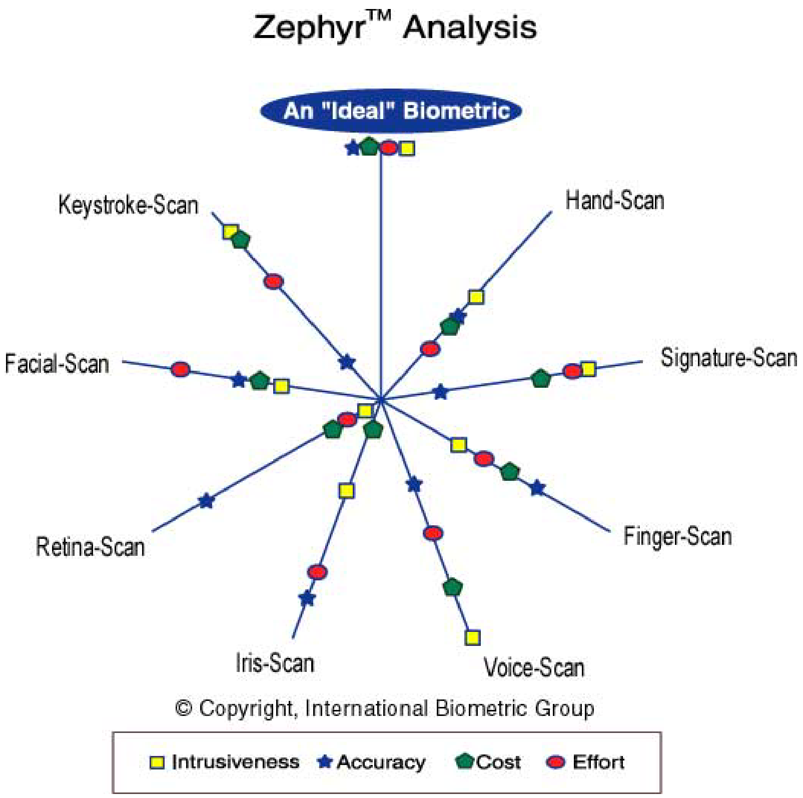
2) <u>Security</u>. A low ATV means that a substantial percentage of users are not being verified by your system. The security provided by a system which can only verify 90% of its users may be acceptable for some deployments, but can be problematic in many others.

3) <u>Convenience</u>. A low ATV may be a reflection of a difficult to use system. In situations in which user convenience is paramount, adjustments to enrollment and verification settings may be required to maximize the ATV rate.

Which is the best biometric?

Despite vendor claims, there is no best biometric technology. If one specifically defines an application, it may be possible to describe the most accurate, easiest to use, easiest to deploy, or cheapest biometric for that particular deployment, but no one biometric technology or set of criteria is right for all situations.

The following Zephyr^{TM} chart is a general comparison of biometric technologies in terms of ease-of-use, cost, accuracy, and perceived intrusiveness. Symbols represent the relative capabilities of each technology; a perfect biometric would have all symbols at the periphery, while a poor biometric would have symbols near the center of the Zephyr chart.



© Copyright, International Biometric Group

Is DNA a biometric?

DNA differs from standard biometrics in several ways:

1) DNA requires a tangible physical sample as opposed to an impression, image, or recording.
2) DNA matching is not done in real-time, and currently not all stages of comparison are automated.
3) DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples.

Regardless of these basic differences, DNA is a type of biometric inasmuch as it is the use of a physiological characteristic to verify or determine identity.

Whether it should or will find use beyond its current use in forensic applications is uncertain. Intelligent discussion on how, when, and where it should and should not be used, and who will control the data, and how it should be stored, is necessary before its use begins to expand into potentially troubling areas.

DNA matching is used today; taking an ostrich approach and wishing it away is counterproductive. Instead, conditions under which its usage, collection, storage, and disposal are acceptable must be defined and enforced. These definitions will vary by application: it illogical to suggest that the usage of DNA in public benefits programs should be viewed as an equivalent to the use of DNA in a criminal investigation. Thinking about the role of DNA as a biometric is helpful as it underscores the tremendous variety of biometric technologies available, and makes clear that blanket statements about biometrics are misleading.

Are biometrics safe to use?

Biometrics based on behavioral characteristics are, of course, safe to use.

Among physiological biometrics, finger-scan systems use light, plastic, glass, and silicon, and have not been shown to be unsafe in any way. Hand-scan readers use metal, plastic, and infrared light to measure reflections and hand structure, and have not been shown to be unsafe in any way. Iris-scan uses infrared illumination just beyond the visible spectrum, and has been declared safe by leading ophthalmologists. Retina-scan shines light through the pupil to read retinal blood vessel patterns, and has not been shown to be unsafe.

To our knowledge, no one has ever been injured or adversely physically affected by any biometric system. Further testing with technologies which require contact or illumination is necessary to make any conclusive statements.

Who are the parties relevant to biometric deployments?

Deployer - the organization using (and normally purchasing) biometric technology.
OEM - the original equipment manufacturer, may be a supplier of biometric technology to the integrator or vendor
Biometric Vendor - the company whose core biometric technology is being deployed. There may be several biometric vendors involved in a deployment supplying hardware and middleware.
Integrator - the company responsible for making the vendor technology and system work with the deployer's technology and systems.
Enroller – the person who enrolls end users into the system.
End-User - the person who actually submits their sample to the biometric system and is verified or identified in the system
System Operator – person responsible for overseeing verification events (relevant to public service deployments where supervision is necessary to ensure cooperation with the system)

System Administrator – person responsible for overall operation, resolving system problems, adjusting thresholds, determining verification and fallback procedures
System Auditor – person responsible for ensuring that the system performs as intended, verifies compliance with best privacy and security practices

Are there biometric standards?

The biometric industry has a number of standards, some of which are complementary, some competing.

Application Programming Interfaces (APIs) simplify the process of application development, offering a standard set of function calls for various biometric devices. An analogy to another class of peripheral devices may help illustrate the point. In the past, an application required customization in order to work with new printers as they were released: a time consuming task for developers. By having a standard API for printers, application developers could simply write applications that adhered to the API, and their application would work with any printer that also adhered to the API.

The API standards field is the most contested area in biometric standards. BioAPI and BAPI are the two prominent standards, each of which has gained degrees of acceptance. BioAPI is the work of a coalition comprised of biometric and non-biometric companies, and has been made a standard for a large-scale government smart card program. BAPI was developed by I/O Software, and is to be incorporated into versions of the Windows operating system. The two standards share many elements in common, and it is not impossible that the two could be made compatible in some fashion.

Other standards efforts, such as CBEFF and X9.84, are concerned with file format and encryption standards. Their acceptance will be extremely important to the future of the biometric industry.

What are some high profile applications of biometrics?

Prominent biometric applications include the following:

- Civil AFIS applications in New York, Texas, California, Connecticut
- Large-scale biometric programs underway or beginning in the Philippines, Nigeria, Hong Kong, Argentina
- Facial-scan application in Illinois, West Virginia
- Over 500,000 users enrolled in facial-scan check-cashing system
- U.S. Army established Biometric Management Office to research biometric technology for armed forces
- U.S. General Services Administration requires biometric compatibility for its $1.5b smart card project
- INSPASS program speeds border crossing at U.S. and Canada airports through hand geometry
- Iris-scan used in pilot application in U.S. and international airports

Most of the larger uses of biometrics are in the public sector. The private sector is testing, piloting, and assessing biometrics, but have been hesitant to adopt on a large scale.