



Biometric Glossary

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

Active Directory: Microsoft's LDAP compliant directory service.

Active Imposter Acceptance: Acceptance of a biometric sample submitted by someone attempting to gain illegal entry to a biometric system.

AFIS: Automated Fingerprint Identification System. A system originally developed for use by law enforcement agencies, which compares a single fingerprint with a database of fingerprint images. Subsequent developments have seen its use in commercial applications, where a client or customer has their finger image compared with existing personal data by placing a finger on a scanner, or by the scanning of inked paper impressions.

Algorithm: A sequence of instructions that tells a system how to solve a problem. Used by biometric systems, for example, to tell whether a sample and a template are a match. Cryptographic algorithms are used to encrypt sensitive data files, to encrypt and decrypt messages, and to digitally sign documents.

American National Standards Institute (ANSI): Established in 1918, ANSI is a voluntary organization that creates standards for the computer industry. The FBI commissioned ANSI to create an image standard for the exchange of fingerprint data between AFIS systems.

API: Application Program Interface. A computer code which is a set of instructions or services used to standardize an application. Any system compatible with the API can then be added or interchanged by the application developer.

ASIC: Application Specific Integrated Circuit. An integrated circuit developed for specific applications to improve performance.

Asynchronous Multimodality - systems that 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.

Attempt: The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.

Audit trail: In computer/network systems: Record of events (protocols, written documents, and other evidence) which can be used to trace the activities and usage of a system. Such material is crucial when tracking down successful attacks/attackers, determining how the attacks happened, and being able to use this evidence in a court of law.

Authentication: The action of verifying information such as identity, ownership or authorization. The preferred biometric term is verification.

Authentication Routine: A cryptographic process used to validate a user, card, terminal, or message contents. Also known as a handshake, the routine uses important data to create a code that can be verified in real time or batch mode. (see verification)

Automated Fingerprint Identification System (AFIS): A specialized biometric system that compares a single finger image with a database of finger images. In law enforcement, AFIS is used to collect fingerprints from criminal suspects and crime scenes. In civilian life, fingerprint scanners are used to identify employees, protect sensitive data, etc.

Automatic ID/Auto ID: An umbrella term for any biometric system or other security technology that uses automatic means to check identity. This applies to both one-to-one verification and one-to-many identification.

Behavioral Biometric: A biometric that is characterized by a behavioral trait that is learned and acquired over time, rather than a physical or physiological characteristic. (contrast with physical biometric)

Bifurcation: A branch made by more than one finger image ridge.

BioAPI: A programming standard published as an ANSI standard that defines a consistent interaction between biometric devices, algorithms and applications. Currently in final stages of review to become an ISO standard. The current version of the standard is 1.2, while the ISO standard will be defined as version 2.0. BIO*GATE depends on the BioAPI for interaction with biometric authentication modules.

Biometric: A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an enrollee.

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.

Biometric System: An automated system capable of capturing a biometric sample from an end user; extracting biometric data from that sample; comparing the biometric data with that contained in one or more reference templates; deciding how well they match; and indicating whether or not an identification or verification of identity has been achieved.

Biometrics: The automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic to a comprehensive database for purposes of identification.

Biopolicy: A set of one or many authentication type that are needed to unlock the requested resource.

BSP: Biometric Service Provider.

Capture: The method of taking a biometric sample from the end user.

CBEFF: Common Biometric Exchange File Format. CBEFF describes a set of data elements necessary to support biometric technologies in a common way.

CDSA : The Common Data Security Architecture is a programming interface standard that defines security and programming interactions for applications. The CDSA includes standard interfaces for Data Libraries, Certificate Services, Cryptography Services, Integrity Services, Authorization, Trust Policies and other interfaces which may be user defined. The CDSA was created by Intel and published through the Open Group (the holder of the UNIX patents). The standard and reference implementation is freely available for download.

Classification: A scheme for categorizing fingerprints according to their overall patterns. Some fingers do not fit into any of the classes, and some may have attributes of more than one class.

Coding: Image processing software for extracting minutiae features from the image.

Comparison: The process of comparing a biometric sample with a previously stored reference template or templates. (see one-to-many and one-to-one)

Contact/Contactless: In regard to chip cards: whether the card is read by direct contact with a reader or has a transmitter/receiver system which allows it to be read using radio frequency technology (up to a certain distance).

Crossover Error Rate (CER): A comparison metric for different biometric devices and technologies; the error rate at which FAR equals FRR. The lower the CER, the more accurate and reliable the biometric device.

Data Encryption Standard (DES): Data Encryption Standard, a block cipher developed by IBM and the U.S. Government in the 1970s as an official standard.

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. Either/or multimodality describes systems that offer multiple biometric technologies, but only require verification through a single technology.

Demographic Data: Census information about an individual, such as name, address, gender, race, and year of birth.

Digital Certificate: In the PKI environment, the data, equivalent to an identity card, issued to a user by a CA (Certificate authority), which he/she uses during business transactions to prove his/her identity.

Digital Signature: The encryption of a message digest with a private key. The number derived by performing cryptographic operations on the text to be signed. This operation, or hash function (also called hash algorithm), is performed on the binary code of the text. The result is known as the message digest, and always has a fixed length. A signature algorithm is applied to the message digest, resulting in the digital signature.

Direct Fingerprint Reader (DFR): A device capable of scanning finger images directly from an individual's fingers.

DSA: Digital Signature Algorithm. Presented in 1991 by the NIST and patented in 1993. A publicly available one-way algorithm used to generate or verify digital signatures of a text to be signed (not to encrypt/decrypt information). As input, DSA needs; the message digest of the message to be signed; the signer's private key; a random number. Its output is a pair of numbers (often referred to as r and s) which together, make up the digital signature. To verify a digital signature, DSA needs as input; the message digest of the text to be verified; the signer's public key; the value s from the signature. DSA then makes a computation, the output of which is called v, for example. If $v = r$, then the signature verifies.

DSS: Digital Signature Standard. Developed by FIPS (U.S. Federal Information Processing Standard). Adopted the DSA in the early 1990s.

eDirectory: Novell's LDAP compliant directory service.

Electronic Benefits Transfer (EBT): Electronic Benefits Transfer enables automatic benefits distribution. It is currently implemented in WIC and Food Stamps programs.

Encryption: The scrambling of data so that it becomes difficult to unscramble or decipher. Scrambled data is called cipher text, as opposed to unscrambled data, which is called plaintext. Unscrambling cipher text is called decryption. Data encryption is done by the use of an algorithm and a key. The key is used by the algorithm to scramble and unscramble the data. The algorithm can be public (for scrutinization and analysis by the cryptographic community), but the key must be kept private. Encryption does not make unauthorized decryption impossible, but merely difficult. Time, and the power (ever increasing) of computers are the factors involved in the feasibility of decryption.

End User: A person who interacts with a biometric system to enroll or have his/her identity checked.

Enrollee: A person who has a biometric reference template on file.

Enrollment: The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

Enrollment Station: A workstation at which an individual's biometrics (fingerprint, voiceprint, etc.) and personal information (name, address, etc.) can be entered into a bioidentification system

Enrollment Time: The time a person must spend to have his/her biometric reference template successfully created.

False Acceptance Rate (FAR): The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. Also known as the Type II error rate.

False Rejection Rate (FRR): The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of

an enrollee. Also known as the Type I error rate.

Feature Extraction: The automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template.

Finger Image: (see image database)

Fingerprint Identification Unit (FIU): A biometric system capable of capturing, storing and comparing fingerprint data for the purposes of verifying an individual's identity.

Fingerprint Template: A description of all the detected minutiae in a fingerprint pattern. The template contains each minutia's x/y coordinate, slope, and type, thus summarizing the characteristics of the fingerprint for purposes of matching the fingerprint against candidates.

Furrow: The lower parts of the fingerprint (see Ridge)

GINA: Graphical Identification and Authentication.

GUI: Graphical User Interface.

Hand Geometry: Measurement of the layout of the physical characteristics of the hand. A lesser used biometric technology.

Identification (id): A one-to-many comparison of an individual's submitted biometric sample against the entire database of biometric reference templates to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity within a database, rather than verify a claimed identity. (contrast with verification)

Identification Algorithm: The algorithm used for making a one-to-many search for user identity.

Identification: The process by which the biometric system identifies a person by performing a one-to-many (1:n) search against the entire enrolled population.

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.

Image Database: The database that contains all fingerprint templates in the system. The image database can contain images of the fingerprints, as well as photograph and signature images.

International Standards Organization (ISO): The major international standards-setting organization for cards of all types.

Iris Recognition: The technique of measuring the veins in the Iris to identify a person. This biometric technology is exceptionally accurate.

Key: A string of bits used widely in cryptography, allowing people to encrypt and decrypt data; a key can be used to perform other mathematical operations as well.

Key Management: The various processes that deal with the creation, distribution, authentication, and storage of keys.

Live Capture: The process of capturing a biometric sample by an interaction between an end user and a biometric system.

M1: INCITS standards group responsible for the biometric working group. It is the US section of the ISO SC37 biometrics standards group

Match/Matching: The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.

Minutiae: Points corresponding to the ridge endings, deltas, and bifurcations of a finger pattern. Minutiae are described in a fingerprint template.

Minutiae Database: The database that contains all fingerprint templates in the system. The minutiae database is contained within the image database.

MMC: Microsoft Management Console provides a consistent interface architecture for configuration management of Windows products.

NMAS: Novell® Modular Authentication Service is a component of Novell eDirectory that offers you an easy way to centrally manage multiple authentication methods across your network. With Novell Modular Authentication Service you can implement stronger forms of authentication and authorization to secure your critical corporate resources. While removing the complexity of directory-based authentication, Novell Modular Authentication Service allows you to create a variety of flexible security options and helps remove the administrative overhead involved with maintaining password information throughout your organization. With Novell Modular Authentication Service, users can authenticate to the network via something they know (for example, a password), something they have (for example, a smart card), or something they are (for example, a fingerprint). And by supporting smart cards, proximity cards, Kerberos, tokens, biometrics and digital certificates, Novell Modular Authentication Service provides a way to centrally and easily manage all of your authentication methods.

One-to-Many: Fingerprint search that compares the minutiae from a candidate fingerprint image against the fingerprint minutiae database to determine whether or not the candidate exists in the database. (synonym for identification.)

One-to-One: Fingerprint search that compares the minutiae from an individual's live fingerprint image against fingerprint minutiae stored on a card or in a specific database record to determine whether or not the individual is who he or she claims to be. (synonym for verification.)

Password Bank: A database for storing username, password and other personal information, to be released upon verification of an individual's identity.

Personal Identification Number (PIN): A security method whereby a series of letters and/or numbers number are entered by an individual to gain access to a particular system or area.

Physical/Physiological Biometric: A biometric that is characterized by a physical characteristic rather than a behavioral trait. (contrast with behavioral biometric)

Privacy-Protective - A privacy-protective system is one used to protect or limit access to personal information, or which provide a means for an individual to establish a trusted identity.

Privacy-Sympathetic - A privacy-sympathetic system is one that limits access to and usage of personal data and in which decisions regarding design issues such as storage and transmission of biometric data are informed, if not driven, by privacy concerns.

Privacy-Neutral - A privacy-neutral system is one in which privacy is not an issue, or in which the potential privacy impact is slight. Privacy-neutral systems are difficult to misuse from a privacy perspective, but do not have the capability to protect personal privacy.

Privacy-Invasive - A privacy-invasive system facilitates or enables the usage of personal data in a fashion inconsistent with generally accepted privacy principles.

Reference Template: Data that represents the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.

Registration: Process of registering biometric data with a Fingerprint Identification Unit (FIU) or other biometric system.

Rejection/False Rejection: When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee. Also known as a Type I error.

Response Time/Processing Time: The time period required by a biometric system to return a decision on identification or verification of a biometric sample.

Retina Scanning: Scanning the veins at the back of the eye (on the retina) - usually for use in an identification or verification algorithm.

Ridge: The raised skin areas which make up a fingerprint

SAS: Secure Action Sequence – A series of key press in Windows that begins a security operation. The SAS most well known to Windows users is the Ctrl, Alt, and Del keys begin pressed simultaneously.

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 that 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.

Single Error Rates - Error rates state the likelihood of an error (false match, false non-match, or failure to enroll) for a single comparison of two biometric templates or for a single enrollment attempt. This can be thought of as a "single" error rate.

Software Developer's Kit (SDK): A programming package that enables a programmer to develop applications for a specific platform. Typically an SDK includes one or more APIs, programming tools, and documentation.

SSL: Secure Sockets Layer is a network communications protocol that provides secure messaging using various encryption techniques.

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 pass phrase in order to provide a biometric sample.

Synchronous Multimodality: 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.

Smart Card: A card-shaped portable data carrier that contains one or more integrated circuits for data storage and processing. A typical smart card chip includes a microprocessor or CPU, ROM (for storing operating instructions), RAM (for storing data during processing) and EPROM (or EEPROM) memory for nonvolatile storage of information.

Template: A mathematical representation of biometric data. A template can vary in size from 9 bytes for hand geometry to several thousand bytes for facial recognition.

Threshold: The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

Type I Error: The failure of a fingerprint identification system when it does not match a candidate fingerprint pattern with its mating fingerprint pattern (in other words, a failure to make a match that should have been made).

Type II Error: The failure of a fingerprint identification system when it matches a candidate fingerprint pattern with a non-mating fingerprint pattern (in other words, making a match that should not have been made).

Validation: The process of demonstrating that the system under consideration meets in all respects the specification of that system.

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.

Verification Algorithm: The algorithm used to check whether a user is who he says he is. Each biometric device will have an associated verification algorithm.

Wiegand: Wiegand is the trade name for a technology originally developed by HID Corporation used in card readers and sensors, particularly for access control applications. A Wiegand card looks like a credit card. It works according to a principle similar to that used in magnetic-stripe cards, such as those used with bank automatic teller machines (ATMs). Instead of a band of ferromagnetic material, the Wiegand card contains a set of embedded wires. The wires are made of a special alloy with magnetic properties that are difficult to duplicate. The set of wires can contain data such as credit card numbers, bank account numbers, employee identification information, criminal records, and medical history. The card is read by passing it through, or bringing it near, a device called a Wiegand sensor. Wiegand effect occurs over a wide range of temperatures. Therefore, access control devices using this technology can function in hostile environments. Other assets include rapid response time and portability. These properties make Wiegand cards and readers ideal for use in the field.

VMWare: A software application that allows a user to run virtual instances of an operating system from within another running OS. This will allow a client instance of BIO*GATE to run inside an instance of the BIO*GATE server.

JANUS is a certified, woman-owned small business. Please call 203.251.0200 to speak with an Information Security Specialist about how your organization would benefit from our information security services.

JANUS Associates, Inc. 9 West Broad Street Stamford, CT 06902

www.janusassociates.com