PKI NOTE

May 2001

Biometrics

The process of verifying that the person with whom a system is communicating or conducting a transaction is, in fact, that specific individual is called authentication. Authentication can be performed with three approaches: knowledge factor (something the individual knows), possession factor (something the individual has), or biometric factor (something physiologically unique about the individual). Biometric technology uses a measurable biological or behavioral characteristic to reliably distinguish one person from another. Biometrics can enhance PKI technology, and, symbiotically, PKI technology can secure biometric technology. These PKI Notes discuss the basics of biometric technology and its synergistic combination with PKI technology.

Acknowledgements

"Biometrics PKI Note" is a deliverable from the PKI Forum's Business Working Group (BWG). Several member organizations and individuals have contributed by providing content, editorial assistance and editorial reviews.

Author:

Jeff Stapleton
KPMG LLP

Table of Contents

Overview of Authentication

The ability to validate that an individual is actually the person with whom a system is communicating or conducting a transaction is called authentication. Authentication is accomplished using one or more of three validation approaches: knowledge factor (something the individual knows), possession factor (something the individual has), or a biometric factor (something physiologically unique about the individual).

- Knowledge factors are something an individual "knows," such as a Personnel Identification Number (PIN) or password. Both parties, the authenticator and the "authenticatee," must share knowledge of the PIN or password. For example, a person (authenticatee) types in a password to log on to a network server (authenticator). The server must know the person's password in order to verify it and therefore authenticate the individual. The security of the system relies on the fact that that password is known only by the authenticator and the authenticatee, and is kept secret from others. For example, a PIN entered at an ATM is encrypted and sent to the issuing financial institution for verification.

- Possession factors are something an individual "has," such as a door key, an employee badge, and a cryptographic key. When symmetric keys are used for authentication, typically the authenticatee creates a cryptically derived check value, called a Message Authentication Code (MAC), that the authenticator can verify using the same key. Thus, the authenticatee and the authenticator must share the symmetric key, but neither party actually knows what its unique property or identifier is. The security of the system relies on the fact that, unlike knowledge factors, the specific contents of a symmetric key are kept absolutely secret, even from the users of the key. This makes the initial generation and exchange of the symmetric key a bit tricky, which requires key management techniques that are beyond the scope of this particular paper.

  Asymmetric keys, often referred to as public-key cryptography, or Public-Key Infrastructure (PKI) technology, are another form of cryptography used as a possession factor. In this scenario, the authenticatee has possession of an asymmetric private key and the authenticator has possession of the corresponding asymmetric public key. The authenticatee creates a digital signature using the private key against a same key, and the security of the system relies on the fact that the private key is kept

Overview of Authentication *continued*

absolutely secret. Only the authenticatee has access to using the private key. In addition, the integrity and authenticity of the public key must be established and maintained using a technique called digital certificates, which requires certificate management techniques that are also beyond the scope of this paper.

- A biometric factor is something physiologically unique about an individual, such as a fingerprint, facial image, iris scan, voice pattern, and handwriting. Many other types of biometric technology have been developed. When an individual wants system access, a sample is taken of the authenticatee's biometric data, for example, a digitized signature. Then, the authenticator, using a previously enrolled version of the same biometric (called a template), can match the sample against the stored template to verify the individual's identity. Biometrics are not secret, as everyone leaves fingerprints everywhere they go, faces and eyes can be photographed, voices can be recorded, and handwriting samples can be obtained. The security of the system therefore relies on the integrity and authenticity of the biometric information, which can be accomplished using PKI once the individual has been enrolled.

The security of the [biometric] system therefore relies on the integrity and authenticity of the biometric information, which can be accomplished using PKI once the individual has been enrolled.

Overview of Biometrics

The single data representation of a biometric characteristic or measurement derived from an individual's fingerprint, voice, iris, face, or handwriting, which is captured or scanned by a biometric device, is called a *biometric sample*. The information extracted from one or more biometric samples is used to create a *biometric template*. An individual is authenticated when a current *biometric sample* is found equivalent to, or "matches," the *biometric template*. Both the *biometric sample* and the *biometric template* are called *biometric data,* or *biometric information*. An automated system capable of collecting, distributing, storing and processing biometric data, and returning a decision (match or non-match), is called a *biometric system*. A typical authentication process utilizing biometric technology consists of the following basic steps:

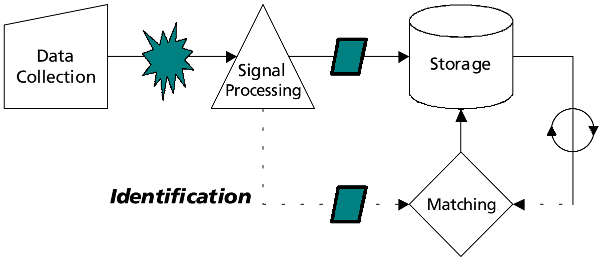
1. Capture the biometric data using a physical reader device;
2. Evaluate the quality of the captured biometric data and recapture if necessary;
3. Process the captured biometric data to create a biometric sample;
4. Match the biometric sample with a previously enrolled template, or templates, to determine if a match exists. This matching can be done as verification or identification.

An automated system capable of collecting, distributing, storing and processing biometric data, and returning a decision (match or non-match), is called a biometric system.

These steps utilize three fundamental biometric applications: Enrollment, Verification, and Identification.

Enrollment

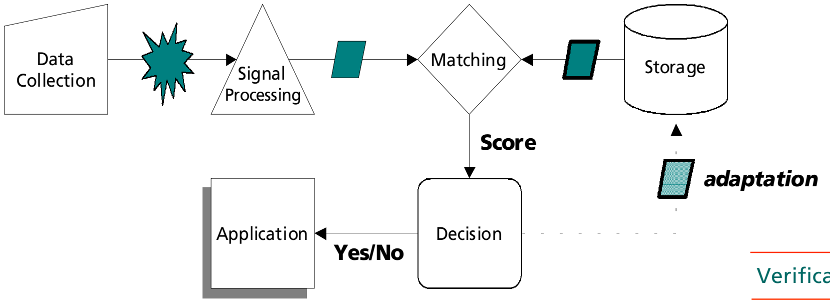
Enrollment is the process of entering a new biometric template and identifier into the database. This data is usually entered along with other information about the individual, which links the individual to an organization, an account, or a set of privileges. Enrollment can incorporate *identification* to make sure that the individual is not already in the database, perhaps under another name. If no match is found, the biometric template, the identifier and its associated information can be added to the database.



Enrollment

Verification

Verification involves a "one-to-one" comparison of a current biometric sample with a *particular*, previously generated biometric template, stored in a database or on an ID card, in order to ensure the correctness of the user's "claimed identity." The biometric template is retrieved from the database using the user's claimed identity, indicated by the user ID, user name, etc., or it is assumed based on the user's possession of the ID card containing the biometric template. If the biometric sample matches the previously generated biometric template, then the claim of identity is verified.



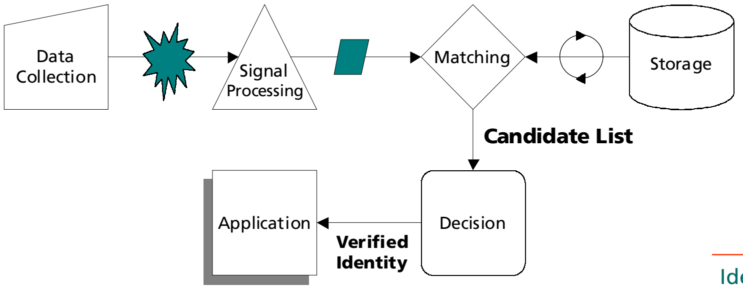
Verification

A typical authentication process utilizing biometric technology employs three fundamental biometric applications:

- Enrollment
- Verification
- Identification

Identification

Identification is the process by which a biometric sample is compared with *all or a specified subset* of the enrolled biometric templates, or a subset based on search algorithms, in the database. This "one-to-many" comparison is done in order to find a matching template and thus identify the person who provided the biometric sample. Unlike verification, the user does not provide a "claimed identity" but instead is identified strictly on the basis of the biometric sample matching one of the biometric templates in the database. The technique can be used for recognition or to confirm that the person being identified is not known under a different name.



Identification

Biometric Requirements

By its very nature, biometric information cannot be kept secret. Individuals leave fingerprints, show their faces, use their voices and leave samples of handwriting behind. Thus, an authentication system should not rely on the confidentiality of biometric information because confidentiality of biometric information cannot be achieved. However, where biometrics are linked to individual identity, privacy requirements may require that such data is encrypted to prevent its disclosure to those who are not authorized.

An authentication system based on biometrics relies on the integrity and authenticity of that biometric information. Thus, biometric information must be protected against unauthorized modification and substitution. Furthermore, the source and destination of the biometric information must be protected to prevent biometric data from being "injected" into the system. Such protection should include temporal information to eliminate falsified or replayed data. Accordingly, the primary requirements are to establish and maintain the integrity and authenticity of biometric information during transmission and in storage.

An authentication system based on biometrics relies on the integrity and authenticity of that biometric information. Thus, biometric information must be protected against unauthorized modification and substitution.

Authenticity and integrity of biometric information can be achieved using physical protection where no transmission is involved and all biometric components reside within the same tamper resistant unit. When transmission occurs, cryptographic mechanisms are the only viable alternative, since physical protection is typically not practical.

Other considerations for managing and securing biometrics systems include metrics such as the failure to enroll rate, false match rate, false non-match rate, and various types of threats such as identity theft, hill-climbing attack and synthetic attack, all of which are beyond the scope of this paper.

Synergy of Technologies

This section describes the interaction between PKI and biometric technology.

PKI Securing Biometrics

The integrity and authenticity of biometric information can be maintained and verified using a digital signature. Biometric templates created during enrollment can be digitally signed to create an unquestionable binding between the biometric information and some type of identifier (e.g., name, account number). In this manner, the authentication system can rely on the biometric template, whether the template is kept in a central repository, mirrored in distributed data bases, or singularly stored in a portable medium such as a smart card.

Biometric samples obtained using a biometric device (such as a fingerprint reader, camera or microphone) can also be digitally "signed" to maintain the integrity of the biometric information and provide authenticity of the biometric device. In this manner, the biometric applications (enrollment, verification, and identification) can rely on the biometric sample.

Furthermore, when privacy is necessary, the biometric information can also be encrypted during transmission. The management of symmetric keys used to encrypt the biometric information can be accomplished using PKI.

Biometrics' Uses with PKI

Non-repudiation, which can be achieved by using digital signatures, is a combination of integrity and authentication that can be proven to a third party. The relative strength of digital signatures, notwithstanding the strength of the underlying asymmetric cryptography, relies on the access controls established and maintained over the private key. Biometrics can enhance the access controls over the individual's private key. Unlike a PIN, which the user can forget, the device or mechanism protecting the private key can authenticate the user using biometric data to activate the private key to be used for generating a digital signature. Users and developers of this technology have also recognized the need for biometric standards. Some work is completed; others are in progress.

ANSI X9.84-2001 Biometric Information Management and Security

This standard defines the requirements for managing and securing biometric information for use in the financial industry (e.g., customer identification and employee verification). Furthermore, the standard identifies techniques such as digital signatures and encryption to provide integrity and maintain privacy of biometric data. The standard also provides a comprehensive set of control objectives suitable for use by a professional audit practitioner to validate a biometric system.

X9.84 was developed in conjunction with other organizations, including the BioAPI Consortium, the NIST/ITL CBEFF initiative, and the International Biometric Industry Association (IBIA). The ANSI standard has been submitted to the ISO Technical Committee 68 for international standardization. More information about the X9 Committee and the standard is available at http://www.x9.org.

The authentication system can rely on the biometric template, whether the template is kept in a central repository, mirrored in distributed data bases, or singularly stored in a portable medium such as a smart card.

Standards and Initiatives

BioAPI Specification

The BioAPI Specification was developed by the BioAPI Consortium, which was formed to develop a widely available and widely accepted Application Programming Interface (API) that serves for various biometric technologies. This specification defines the API and Service Provider Interface (SPI) for a standard biometric technology interface. It is beyond the scope of this specification to define security requirements for biometric applications and service providers, although some related information is included by way of explanation of how the API is intended to support good security practices. It covers the basic functions of Enrollment, Verification, and Identification, and includes a database interface to allow a Biometric Service Provider (BSP) to manage the Identification population for optimum performance. It also provides primitives which allow the application to manage the capture of samples on a client, and the Enrollment, Verification, and Identification on a server. Further information on the BioAPI Consortium and the specification is available at http://www.ibia.org.

CBEFF NIST Publication

The National Institute for Standards and Technologies (NIST) Information Technology Laboratory (ITL) initiated the Common Biometric Exchange File Format (CBEFF) workshops, which resulted in the Common Biometric Exchange File Format For Biometric Interoperability, NIST Publication, NISTIR 6529. This effort was coordinated with the BioAPI Consortium and the X9F4 working group. For more information, visit http://www.nist.gov/cbeff.

ANSI/NCITS Driver's License / Identification Standard

The B10.8 working group, operating under the National Committee for Information Technology Standards (NCITS) with jurisdictional representation from the American Association of Motor Vehicle Administrators (AAMVA), developed the ANSI Driver's License and Identification (DL/ID) Standard. This standard allows for the use of biometrics as an identification mechanism. For more information, visit http://www.aamva.org.

ISO/IEC JCT1 Subcommittee 17

The ISO/IEC Joint Technical Committee One (JTC1) Subcommittee 17 is chartered to develop standards for Passports and Identification Cards. Several of the working groups are reviewing the ANSI DL/ID standard, the ANSI X9.84 standard, and the BioAPI specification. More information about JTC1 is available at http://www.jtc1.org.

Copyright Statement

About PKI Forum

The PKI Forum is an international, not-for-profit, multi-vendor and end-user alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI).

The PKI Forum advocates industry cooperation and market awareness to enable organizations to understand and exploit the value of PKI in their e-business applications.

Web:	http://www.pkiforum.org
e-Mail:	info@pkiforum.org
Phone:	+1 781 876 8810