May 2001

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

BIOMETRICS – TECHNOLOGIES FOR HIGHLY SECURE PERSONAL AUTHENTICATION

By Fernando L. Podio, Convergent Information Systems Division, Information Technology Laboratory, National Institute of Standards and Technology

Introduction

Biometrics are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, speaker verification, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification and keystroke dynamics are two examples of behavioral characteristics.

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

Biometric-based authentication applications include workstation/network/domain access, single sign-on, application logon, data protection, remote access to resources, transaction security, and web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures (trust in these electronic transactions is essential to the healthy growth of the global economy). Utilized alone or integrated with other technologies such as smart cards, encryption keys, and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives. For example, biometrics are used in various schools such as in lunch programs in Pennsylvania [1] and in a school library in Minnesota [2]. Examples of other current applications include verification of annual pass holders in an amusement park, speaker verification for television home shopping, Internet banking, and in users' authentication in a variety of social services.

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (*Capture, Process, Enroll*) followed by a *Verification* or *Identification* process.

Capture: A raw biometric is captured by a sensing device, such as a fingerprint scanner or video camera.

Process: The distinguishing characteristics are extracted from the raw biometric sample and converted into a processed biometric identifier record (sometimes called biometric sample or biometric template).

Enroll: The processed sample (a mathematical representation of the biometric – not the original biometric sample) is stored/registered in a storage medium for later comparison during an authentication. In many commercial applications, storing the processed biometric sample is all that is needed. The original biometric sample cannot be reconstructed from this identifier.

A *Verification* (or "1 to 1 matching") process implies matching the enrolled biometric sample against a single

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since November 1999

❒ *Acquiring and Deploying Intrusion Detection Systems*, November 1999

❒ *Operating System Security: Adding to the Arsenal of Security Techniques,* December 1999

❒ *Guideline for Implementing Cryptography in the Federal Government*, February 2000

❒ *Security Implications of Active Content*, March 2000

❒ *Mitigating Emerging Hacker Threats*, June 2000

❒ *Identifying Critical Patches with ICAT,* July 2000

❒ *Security for Private Branch Exchange Systems*, August 2000

❒ *XML Technologies*, September 2000

❒ *An Overview of the Common Criteria Evaluation and Validation Scheme*, October 2000

❒ *A Statistical Test Suite for Random and Pseudorandom Number Generators For Cryptographic Applications*, December 2000

❒ *What Is This Thing Called Conformance?* January 2001

❒ *An Introduction to IPsec (Internet Protocol Security)* March 2001 record. If the biometric-based recognition system requires that an individual present a claim of identity, for example, by entering a user name or user identification number, a password or presenting a token, the individual is recognized through biometrics in a "verification" mode. In this mode, a newly captured/processed biometric sample taken during, for example a login, is compared against a previously enrolled sample to determine whether the person is who they claim to be. It addresses the question "Are you who you claim to be?"

During enrollment, the processed biometric sample can be stored in a database or in a portable token such as a smart card. In many applications, storing the original biometric sample is neither needed nor desirable. Some applications, however, may be set up to store the original biometric input for reprocessing at a later date (for example, to generate processed samples with a different processing algorithm). The figure below illustrates the enrollment and the verification process.

An *Identification* (or "1 to N matching") implies matching a biometric sample against all records in a database of identifiers. In this mode, the individual does not claim an identity. The individual presents a biometric sample and the system tries to identify the individual from a database of stored biometric samples. This process intends to answer the question "Who are they?" This mode is sometimes associated with law enforcement applications but can also be used for other applications where the user voluntarily presents their biometric sample and expects to be recognized by the system.

Personal Authentication Through Biometrics

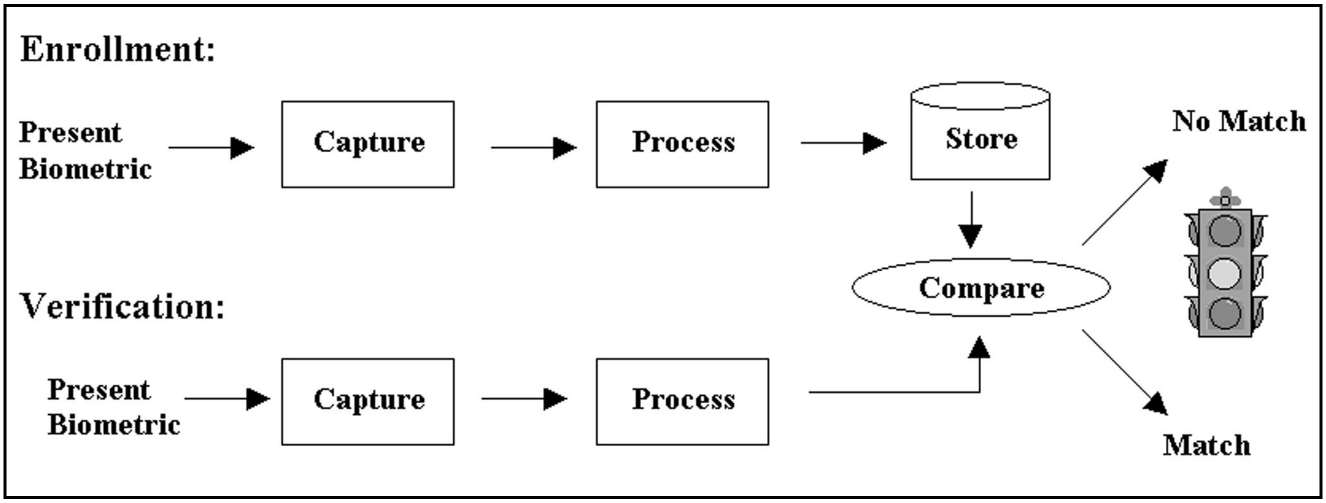
Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or personal identification numbers [PINs]). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember) and accurate (it provides for positive authentication), can provide an audit trail, and is becoming socially acceptable and inexpensive.

Biometrics is converging with other technologies, such as smart cards and Public Key Infrastructure (PKI), and provides for either verification or identification of an individual, as explained above. Smart cards can store transaction information, the biometric template, a public key, and process data. PKI ensures that the information is not intercepted and read (or altered) en route. Biometrics, therefore, may be used as a second factor for authentication for smart cards (token + biometric must be present). In this approach, a biometric can be used to authenticate the owner of a smart card and to unlock secrets on the card (e.g., private key, digital certificate, PIN, etc.). If the biometric identifier is stored on the card, the authentication of the individual is against the biometric data stored on the card. This is a popular application because it ensures that the user is the legitimate holder of a card, so lost/stolen cards that could contain personal records or allow for access to bank accounts are less of a problem. This solution is more secure than accessing a smart card with a PIN. For example, the Department of Defense (DoD) is testing biometric technologies in combination with smart cards for a number of DoD applications [3].

Biometrics are easier to use than PINs; the technology makes implementations easier. Biometrics, sometimes seen as a competing technology to PKI, can instead be complementary to PKI. Because PKI is totally dependent upon protection of the private key, issues such as confidentiality, integrity, and access control exist. Passwords and PINs are inadequate for this purpose. Biometrics can provide the means of strong authentication needed to 'release' the private key for use.

Biometric Consortium

The Biometric Consortium (BC) serves as a focal point for research, development, testing, evaluation, and application of biometric-based personal identification and verification technology. It currently has over 800 members from private industry, federal, state, and local governments, and academia. Fifty percent of the members are from industry. Over 60 federal agencies are represented in the consortium. The BC sponsors research and other technical industry and user activities as required (see a few examples below). The BC also sponsors technology workshops and standards activities and holds an annual conference that is open to members and the general public. An electronic discussion list is maintained for BC members. This electronic discussion list provides an online envi-



ronment for technical discussions among its members on all things biometric. NIST and the National Security Agency (NSA) co-chair the Biometric Consortium and co-sponsor most of the BC activities. Recently NIST and NSA have co-sponsored a number of biometric-related activities including the development of a Common Biometric Exchange File Format, the NIST Biometric Interoperability, Performance, and Assurance Working Group, a BioAPI Users' and Developers' Seminar, and the NIST BioAPI Interoperability Test Bed. NIST and NSA also provide advice to other government agencies such as the General Services Administration (GSA) Office of Smart Cards Initiatives and DoD's Biometric Management Office. The BC web site is http://www.biometrics.org.

Biometrics Standards Activities

An indication of the current substantial growth and interest in biometrics is the emergence of biometrics industry standards and related activities. Standards have become strategic business issues. For any given technology, industry standards assure the availability of multiple sources for comparable products and of competitive products in the marketplace. Standards will support the expansion of the marketplace for biometrics. (The biometric industry represents a $500M market [4] with an anticipated revenue growth to 1.1B by the year 2003 [5]. The market for personal authentication through biometrics is much larger. For example, it is expected that 230M people will be conducting wireless transactions representing $100B/year with more than 1B transaction [6].) Biometric data interchange and interoperability standards are emerging. Some of them are independent of the biometric technology. Standards that are biometric technology-specific (e.g., fingerprints) have also been developed. NIST is involved in many capacities with industry and end-users in the development of these standards. A summary of these standards efforts follows:

Common Biometric Exchange File Format (CBEFF)

CBEFF describes a set of data elements necessary to support biometric technologies in a common way independently of the application and the domain of use (e.g., mobile devices, smart cards, protection of digital data, biometric data storage). CBEFF facilitates biometric data interchange between different system components or between systems, promotes interoperability of biometric-based application programs and systems, provides forward compatibility for technology improvements, and simplifies the software and hardware integration process. The data described by CBEFF includes: (1) the location of the biometric data within the CBEFF structure; (2) security options (digital signatures and data encryption); and (3) processing information such as identification of the biometric type (e.g., facial features), record data type (e.g., processed biometric data), the format owner (e.g., ID of an entity such as a vendor or organization) that defines one CBEFF biometric data format and the format type (biometric data format specified by the format owner). The International Biometric Industry Association (IBIA) [7] is the Registration Authority for CBEFF format owner and format type values for organizations and vendors that require them (http://www.ibia.org/formats). The CBEFF's initial conceptual definition was achieved through a series of three workshops co-sponsored by NIST and the Biometric Consortium. The Technical Development Team, formed as a result of these workshops, developed CBEFF in coordination with industry consortiums (BioAPI Consortium and TeleTrusT) and a standards development group (ANSI/ASC X9F4 Working Group). CBEFF is described in detail in NISTIR 6529, *Common Biometric Exchange File Format (CBEFF)*, January 3, 2001 [8]. A copy of NISTIR 6529 can be downloaded from the CBEFF web site: http://www.nist.gov/cbeff.

BioAPI Specification – BioAPI V1.1

The Biometric Application Programming Interface (API) specification was developed by the BioAPI Consortium, which consists of 80 organizations representing biometric vendors, Original Equipment Manufacturers (OEMs), major Information Technology (IT) corporations, systems integrators, application developers, and end-users. NIST holds membership in the Consortium and is a member of the Steering Committee. A Biometric Application Programming Interface is the interface between biometric technology modules and applications. The BioAPI V1.1 specification [9] promotes interoperability by defining a generic way of interfacing to a broad range of biometric technologies. The BioAPI Specification defines an open system standard API that allows software applications to communicate with a broad range of biometric technologies in a common way. As an "open systems" specification, the BioAPI is intended for use across a broad spectrum of computing environments to ensure cross-platform support. It allows for: (1) easy substitution among biometric technologies and easy integration of multiple biometrics using the same interface; (2) the utilization of biometric technology across multiple applications; and (3) rapid application development which increases competition and tends to lower costs. BioAPI specifies standard functions and a biometric data format which is an instantiation of CBEFF. It specifies basic functions (e.g., enroll user, verify asserted identity, discover user's identity) and primitive functions (e.g., create template, process, verify match, import). BioAPI supports a wide range of biometric technologies, and it is designed for use in a broad range of applications, extending from embedded devices (such as in cell phones) to large-scale identification systems (such as national ID systems), as well as user authentication applications associated with computer and network access. The specification and associated reference

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

implementation [9] are open source and can be downloaded from the BioAPI Consortium web site: http://www.bioapi.org. BioAPI compliance is required by DoD and GSA's Office of Smart Cards Initiatives.

Human Recognition Services (HRS) Module of the Open Group's Common Data Security Architecture (CDSA)

HRS is an extension of the Open Group's Common Data Security Architecture [10]. CDSA is a set of layered security services and a cryptographic framework that provides the infrastructure for creating cross-platform, interoperable, security-enabled applications for client-server environments. The CDSA solutions cover all the essential components of security capability, to secure electronic commerce and other business applications with services that provide facilities for cryptography, certificate management, trust policy management, and key recovery. The biometric component of the CDSA's HRS is used in conjunction with other security modules (i.e., cryptographic, digital certificates, and data libraries) and is compatible with the BioAPI specification and CBEFF. The web site is http://www.opengroup.org/security/cdsa/.

X9.84-2000, Biometrics Management and Security For The Financial Services Industry©

This American National Standards Institute (ANSI) standard was developed by the X9.F4Working Group of X9 [11], an ANSI-accredited standards organization that develops, establishes, publishes, maintains and promotes standards for the financial services industry. X9.84-2000 specifies the minimum-security requirements for effective management of biometrics data for the financial services industry and the security for the collection, distribution and processing of biometrics data. It specifies: (1) the security of the physical hardware used throughout the biometric life cycle; (2) the management of the biometric data across its life cycle; (3) the utilization of biometric technology for *verification/identification* of banking customers and employees; (4) the application of biometric technology for physical and logical access controls; (5) the encapsulation of biometric data; and (6) techniques for securely transmitting and storing biometric data. The biometric data object specified in X9.84 is also compatible with CBEFF. The web site is http://www.x9.org.

ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information - Fingerprint Standard Revision

On July 27, 2000, ANSI approved ANSI/NIST-ITL 1-2000 [12]. This is a revision, re-designation, and consolidation of ANSI/NIST-CSL 1-1993 and ANSI/NIST-ITL 1a-1997. The standard specifies a common format to be used to exchange fingerprint, facial, scars, mark and tattoo identification data effectively across jurisdictional lines or between dissimilar systems made by different manufacturers. NIST has published the document as NIST Special Publication SP 500-245. The revision began with a Fingerprint Data Interchange Workshop that was held in September 1998. This revision was performed in accordance with the ANSI procedures for the development of standards using the Canvass Method. All federal, state and local law enforcement data is transmitted using the ANSI-NIST standard. This standard is a key component in allowing interoperability in the justice community. NIST Special Publication SP 500-245 is available at: http://www.itl.nist.gov/iad/894.03/fing/fing.html#ANSI_NIST_ITL_1_2000.

ANSI B10.8 / AAMVA, Fingerprint Minutiae Format / National Standard for the Driver License/Identification Card DL/ID-2000

The purpose of the American Association for Motor Vehicle Administration (AAMVA) Driver's License and Identification (DL/ID) Standard is to provide a uniform means to identify issuers and holders of driver license cards within the U.S. and Canada. The standard specifies identification information on drivers' license and ID card applications. In the high-capacity technologies such as bar codes, integrated circuit cards, and optical memory, the AAMVA standard [13] employs international standard application coding to make additional applications possible on the same card. The standard specifies minimum requirements for presenting human-readable identification information including the format and data content of identification in the magnetic stripe, the bar code, integrated circuit cards, optical memories, and digital imaging. It also specifies a format for fingerprint minutiae data that would be readable across state and province boundaries for drivers' licenses. DL/ID-2000 is compatible with the BioAPI specification and CBEFF.

Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 11: Personal verification through biometric methods

This standard is developed as Part 11 of the ISO/IEC 7816 standard. The scope is specifying security-related inter-industry commands to be used for personal verification with biometric methods in integrated circuit cards (e.g., smart cards). It also defines data elements to be used with biometric methods. This standard is under development in the International Standards Organization (ISO) Subcommittee (SC) 17, Working Group 4.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our web site is http://www.itl.nist.gov/.

NIST Biometric Interoperability, Performance and Assurance Working Group

NIST and the Biometric Consortium have established this Working Group [14] to support advancement of technically efficient and compatible biometric technology solutions on a national and international basis and to promote and encourage exchange of information and collaborative efforts between users and private industry in all things biometric. The Working Group consists of 80 organizations representing biometric vendors, system developers, information assurance organizations, commercial end users, universities, government agencies, National Labs and industry organizations. The Working Group is currently addressing development of a simple testing methodology for biometric systems as well as addressing issues on biometric assurance. In addition, the Working Group is addressing the utilization of biometric data in smart card applications by developing a smart card format compliant to the Common Biometric Exchange File Format (CBEFF). NIST's plans include validating the testing methodology and the CBEFF smart card format at ITL's Biometrics and Smart Cards Lab. The Working Group web site is http://www.nist.gov/bcwg.

Recent Research and Evaluation Activities

Research on biometric technologies such as fingerprint, face, hand features and speaker recognition, has taken place for decades in industry, government, and academia. A comprehensive description of these research activities is beyond the scope of this bulletin. A detailed summary of the research issues for the general problem of personal authentication (verification or identification) is provided in [15]. These include: (a) system design; (b) acquisition (of relevant biometric data); (c) representation (of salient features of the input biometric data); (d) feature extraction (from the raw biometric data to generate a biometric template of identifier); (e) matching (to quantify the similarity between two biometric identifiers); (f) search and scalability (applicable to identification systems such as maintaining a database of biometric identifiers); (g) evaluation (performance of the biometric system); (h) integration (utilization of more than one identifier or biometric technology to improve the authentication); and (i) prevention (of circumvention).

Industry

Industry is concentrating its efforts on developing solutions that are more accurate, less expensive, faster, and easy to use. Prices of biometric devices and authentication software have dropped substantially in the last few years. Many biometric solutions are expected to comply with open standards. Many personal authentication solutions also aim at integrating Public Key cryptography with smart cards and biometrics. Industry is integrating biometrics in mobile devices, keywords, cameras, and mice. The Biometric Consortium web site provides links to multiple examples of biometric systems [16]. In addition to the expected applications for biometrics (as described above), other innovative uses for biometrics include delivering medication to the correct patients, protecting digital content, and verifying that children are picked up (in a child care center) by the correct parent.

Academia

U.S. universities are very active in biometrics research. Examples include Michigan State University, West Virginia University, and San Jose State University (SJSU). The Michigan State University biometric program (http://biometrics.cse.msu.edu/) focuses on developing algorithms (e.g., fingerprint images, classification of fingerprints, fingerprint enhancement, face detection, integrated recognition with fingerprint verification, and speaker verification). West Virginia University (WVU) has a strong forensic identification initiative, which is a multidisciplinary research and education collaboration in areas related to forensic sciences. Two main programs available under WVU Forensics are the biometric systems and a latent fingerprint program. The web site is http://www.wvu.edu/~forensic/program.htm. Programs at SJSU (http://www.engr.sjsu.edu/biometrics/) include the study of mathematical concepts and equations that are the engines of biometric technologies and the utilization of biometrics in commercial driver's licensing systems. References to other private industry, government, and academic research activities can be found at the Biometric Consortium web site.

Government

Many federal and state government agencies are involved in research, testing, and implementation of biometric authentication systems. The National Security Agency (NSA), for example, conducts one of the U.S. Government's leading research and development programs. As part of its Information Assurance mission, NSA conducts research on new technologies that may be used to protect information technology systems. For several years, NSA has been researching biometric technologies that may be useful to prevent unauthorized access to critical systems. The Department of Defense (DoD) established a DoD Biometrics Management Office (BMO) to ensure the availability of biometrics technologies within the Department of Defense [17]. Acting on behalf of the Secretary of the Army through the Army Chief Information Officer, BMO operates as the executive agent to lead, consolidate, and coordinate all biometric information assurance programs of the Department of Defense in support of Network Centric Warfare. The BMO is focused on providing the armed forces with a technological edge in all environments by providing proven, reliable, and effective biometrics access systems in support of garrison and combat operations. BMO established the Biometric Fusion Center in West Virginia to acquire, test, evaluate, and integrate biometrics. The Defense Manpower Data Center (DMDC) operates a large biometric database (fingerprints from all active-duty, reserve, and retired military personnel as well as survivors receiving a military annuity. The Immigration and Naturalization Service (INS) deployed a system based on hand geometry (INSPASS) in several U.S. airports (e.g., JFK, San Francisco, and Dulles) for frequent international travelers (e.g., U.S. citizens, U.S. legal residents, and citizens of Bermuda and Canada). Several states have implemented large-scale biometric applications in social services programs including New York, Texas, California, New Jersey, Connecticut, and Illinois [18].

Current NIST Involvement

NIST is involved in various aspects of biometric research and evaluation (e.g., interoperability, data interchange, Reference Databases, recognition algorithms, authentication architectures), metrology and standardization. Current projects support both the U.S. industry (e.g., biometric vendors, systems developers, IT major organizations) and end users such as the law enforcement community, other government agencies (e.g., Defense Advanced Research Projects Agency [DARPA], NSA, DoD's Biometric Management Office), financial, health care, and other commercial organizations.

In support of the law enforcement community, ITL's Information Access Division developed the first automated fingerprint system design and has developed evaluation methods for fingerprint matching and classification systems for over 20 years. NIST developed the evaluation protocols used in the Face Recognition Vendor Test (FRVT) 2000 and has designed most of the data collection methods in public use in the face recognition community. Work for Criminal Justice Information Systems (sponsored the FBI), includes all aspects of identification and communication of records and identification information. It currently includes the development of the ANSI/NIST-ITL 1-2000 standard described above, the development of software to manipulate images in a fingerprint Standard Reference Data CD developed by NIST, the development of a Law Enforcement web application (web site that allows submission of applicant's fingerprints for non-law enforcement applicants), development of a latent fingerprint workstation (to manipulate latent fingerprint images for forensic purposes), and research of compression algorithms for 1000 DPI fingerprint images. The HumanID project (cosponsored by DARPA and the National Institute of Justice) provides evaluation methods and test data for biometric systems that operate at long distances from the subject. It includes a HumanID data collection effort, development of statistical analysis of face recognition (new analysis method for face recognition experiment correlation), and FRVT 2000 report on the web. HumanID is a program designed to provide automated surveillance capability that can be used to protect U.S. installations from uncooperative subjects using data taken from distances of several hundred meters. It includes both new sensor technology and new recognition methods.

In the last few years, ITL's Convergent Information Systems Division has extended the biometric effort to address commercial applications of biometrics and the commercial marketplace. This work is addressing research, technology, and standards to support the advancement of technically efficient (required performance) and compatible biometric technology solutions. This effort (co-sponsored by NIST and NSA) facilitates solutions that promote interoperability and biometric data interchange with the required level of performance. ITL works with U.S. industry and user communities through industry consortiums, standards bodies, the Biometric Consortium (as described above), other organizations such as the Financial Services Technical Consortium, and other government agencies (e.g., NSA Information Assurance, GSA Office of Smart Cards Initiatives, DoD Biometric Management Office). The effort includes researching the integration of biometrics with other authentication technologies (e.g., smart cards, PKI, digital signatures, and advanced challenge-response techniques) for high performance personal authentication architectures, and developing performance metrics, interoperability, and data interchange tests. The project is currently researching a framework for biometric interoperability based on BioAPI and CBEFF and developing a BioAPI Interoperability and Performance Test Bed.

NIST is participating with the General Services Administration in a cooperative effort in support of the Government Smart Card (GSC) Program administered by GSA (which has a biometric requirement). ITL's Computer Security Division is providing advice to GSA and developed the technical requirements for GSA's "Smart Access Common ID Card" RFP. ITL's Convergent Information Systems Division and the Biometric Consortium supported this effort by providing advice on the biometric interoperability requirements. (Utilization of biometrics in smart cards under the GSA Government Smart Card program requires compliance to the BioAPI specification and CBEFF.) Through this program, ITL is helping the U.S. Government to effectively use standards and is working with GSA and leading IT developers to promote smart card and biometric standardization and conformance testing. ITL's Computer Security Division, with the Software Diagnostics and Conformance Testing Division and the Statistical Engineering Division, is developing a smart card interoperability and conformance testing program to support this GSA program.

Conclusion

Biometric technologies are ideally suited to provide highly secure identification and personal verification solutions. Biometric-based personal authentication has multiple applications in commerce, the federal, state and local governments, in the military and in commercial applications. Biometrics has a high priority in the government sectors and also in the business world, especially in fast-growing sectors such as mobile appliances and e-commerce. Open system standards increase users' confidence by preventing the sole source lock-in and are vital for the growth of the global economy. The biometrics industry's maturity is demonstrated by its commitment to the development of the required biometric standards. ITL has played a major role in the development of these standards. Industry, academia, and government agencies have been conducting evaluation and research in biometrics for many years. Evidence of the growing acceptance of biometrics is the availability in the marketplace of biometric-based authentication solutions that are becoming more accurate, less expensive, faster and easy to use.

For More Information

[1] “*Fingerprint Technology Speeds School Lunch Lines*”, http://www.eschoolnews.com/showstory.cfm?ArticleID=2146, eSchool News online, April 26, 2001.

[2] *“Best Practices – Technology: This Minnesota High School Gives Fingerprint Scanning a Whorl”,* http://www.eschoolnews.com/showstory.cfm?ArticleID=1277, eSchool News online, April 26, 2001.

[3] G. Sellers, *“The Details are in the Bio*”, Federal Computer Week, April 30, 2001, p46.

[4] B. Ruttenbur, Morgan Keegan and Co., Inc., “*Biometrics Overview*”, BC 2000 Conference, Sept. 2000

[5] S. Nanavati, IBG, ”*Comparative Biometric Testing for IT Security and E-Commerce*”, Biometric Summit 2001, February 26, 2001.

[6] Dr. J. Atick, Visionics, “*Biometrics at Mass Market Level; Today’s Trends that will Affect Tomorrow’s Adoption*”, Biometric Summit 2001, February 27, 2001

[7] International Biometric Industry Association, http://www.ibia.org

[8] F. Podio, J. Dunn, L. Reinert, C. Tilton, Dr. L. O'Gorman, M. P. Collier, M. Jerde, Dr. B. Wirtz*, Common Biometric Exchange File Format (CBEFF)*, NISTIR 6529, January 3 2000.

[9] BioAPI Consortium, *BioAPI specification v1.1 and BioAPI Reference Implementation*, March 15, 2001.

[10] “*Common Data Security Architecture*” http://www.opengroup.org/security/cdsa/

[11] X9. F4 Working Group, ANSI/ASC X9.84, *Biometric Information Management and Security*, April 2001.

[12] NIST, ANSI/NIST-ITL-1-2000*, Data format for the Interchange of Fingerprint, Facial and SMT Information*, July 2000.

[13] ANSI B10.8 / AAMVA, Fingerprint Minutiae Format / National Standard for the Driver License/Identification Card DL/ID-2000.

[14] NIST Biometric Interoperability, Performance and Assurance Working Group: http://www.nist.gov/bcwg

[15] A. Jain, R. Bolle, S. Pankanti, Biometrics, *Personal Identification in Networked Society*, Kluwer Academic Publishers (Norwell, Massachusetts, 1999), p20-34.

[16] Biometric Consortium web site: http://www.biometrics.org

[17] Department of Defense (DoD) Biometrics Management Office (BMO), http://www.c3i.osd.mil/biometrics/

[18] J. D. Woodward, K. W. Webb, E. M. Newton, M. Bradley, D. Rubenson, *Army Biometric Applications, Identifying and Addressing Socio-cultural Concerns*, RAND Arroyo Center, May 2001, p99.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

1901-2001

NIST CENTENNIAL

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8901
Gaithersburg, MD 20899-8901