Global Information Assurance Certification Paper

BIOMETRICS: AN OVERVIEW OFACCURACY, STANDARDS, AND TECHNOLOGY SELECTION CONSIDERATIONS

Judy Petsch
Version 1.4
28 March 2003

ABSTRACT
Biometrics is an up and coming technology that does personal identification based on the behavior or physical characteristics of an individual. As such, there is a vast market aimed at utilizing the individual's biometric as their ID. Accuracy is always a concern when authenticating an identity and biometrics can work well in this aspects. The only major concern with accuracy is in regards to technology selections. Vendors have varying methods for determining accuracy and this will be covered in this paper. Standards are another major concern of any industry when it comes to interoperability. Standards have been fought over and agreed to by other international forums but biometrics seems to have been lacking in this arena. Thanks to standards in the electrical industry, your 3-prong plug fits into the socket in any house in the United States. The biometrics industry is not new but the overwhelming push for usage is. Due to the lack of accepted standards, the implementation of biometric technologies has been very difficult. Consensus among the major vendors has been nonexistent and interoperability is a major concern. The general arrangement is for a vendor to promote its product as the best in the marketplace. But once implemented, the user may find desired results lacking and costs too prohibitive to switch to another product. The lack of standards can be seen as a contributing factor in causing biometrics to lag in "catching on" as a technological advancement for identity security.

What standards there currently are in the biometrics community, are in a state of flux. Due to the rapid development of biometric technology, proprietary standards have prevailed. To foster interoperability necessary for biometrics to become a user-friendly technology, the government and private industry have joined forces to advance standards. Also affecting standards is the fact that many companies are in the process of merging as a way of strengthening their market position. Standards have an effect on the peripheral hardware format, interface, and platform requirements of a vendor's product that can then greatly influence which biometric could be utilized in a specific scenario. This has a direct impact on technology selection.

This paper will cover accuracy, standards and technology selection to give the future biometric user a better understanding of the capabilities offered by biometrics for identity authentication and overall information assurance.

INTRODUCTION - WHAT ARE BIOMETRICS

Biometrics is identified as the measurable physical characteristics or a personal behavioral trait used to recognize one's identity or verify the identity one has claimed. To recognize one's identity, a one to many (1:N) search is done against a database. To verify the identity that one claims requires the use of a prior template or biometric sample which is then compared against a live sample (1:1). This is also called authentication. There are many biometrics in current use and this means there are

many companies with their own proprietary way to use the biometric. The most common, and therefore, well known biometrics include fingerprint, iris, hand geometry, facial recognition, and voice.

There are two basic methods of use with biometrics:

- Identification Mode: One-to-many
  - Example: ATM- one bank customer is checked against database of all customers

- Verification Mode: One-to-one
  - Example: The user is checked against only his/her own template while logging onto a PC

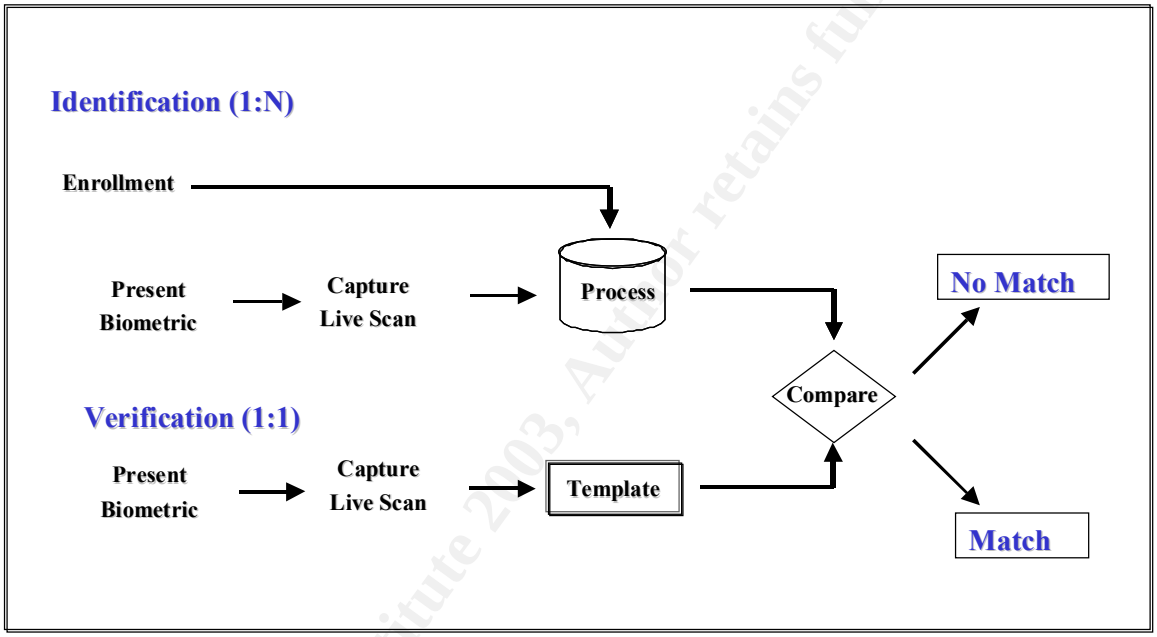

Figure 1. Identification/Verification Process

The majority of biometric applications are 'Verification' using a claimed identity.

There are also two major types of biometrics: contact and contactless. Contact biometrics is where the user actually touches a surface for interaction, such as a fingerprint reader. Many are familiar with it due to its usage within the law enforcement system. Usage outside law enforcement has grown as the costs for the devices and systems have crept downward so familiarity has increased. Contactless is identified as no requirement for the user to touch the device. Currently, the two biometrics most commonly used for contactless interface are the iris scan and facial recognition.

Biometric applications can include:

- Integrated Physical Access Control
- Logical access to IT resources
  - Logon (password replacement)

        - OS, E-mail, databases, applications
        - Web-based resource access
    - Document locking (Excel, Word etc.)
- Business Process Improvement
    - Faster, more efficient receipting, tracking and logging
    - Can be combined with a token, RFID, smart card, etc.

The commercial sector, especially in the European arena, has adopted biometrics as a means to increase security in projects such as:

- Banking
    - ATM, application process, network login
- Health Care – influenced by the federal Health Insurance Portability and Accountability Act (HIPAA)
    - Patient record access
- Time and Attendance
- Access control
    - Warehouses and high-value goods storage areas
    - Increasing number of commercial applications replacing passwords

The governmental sector has adopted biometrics for increased security in projects such as:

- Integrated Access Control
- Benefit Administration counter-fraud (State & Local systems)
- Border control (INS) & law enforcement (FBI)
- GSA's Government Smart Card
- DEERS /RAPIDS
- DoD Common Access Card

BIOMETRIC DEVICE ACCURACY

Biometric devices are frequently described in terms of a False Acceptance Rate (FAR) and False Rejection Rate (FRR). A false acceptance rate is the biometric device incorrectly identifying an individual; such as, saying user one matches to user three's template, or the failure to reject an imposter, someone not enrolled at all. A false rejection rate is a biometric device failing to identify or verify an enrolled individual who is authorized access. There is also the Equal Error Rate (EER), additionally called the Crossover Rate, which is described as the point on a chart where the FRR and FAR meet. This is where the risk for a FAR and a FRR are equal or the same. Many vendors will use this EER as the default point for setting the security threshold on their devices for measuring the FRR and FAR.

When considering the FAR and FRR and how they are reported, it is important to understand how the numbers were reached. There are two general methods used when calculating the FAR and FRR: one attempt versus three attempts. Many users will assume that an attempt to use the biometric device will register in the system as one FAR or FRR. This is not necessarily the case and care should be given to error rate comparisons. Many vendors will use three attempts to access the biometric device before an FAR/FRR is counted and this is how they arrive at their statistical data when rating their equipment capabilities. The three-to-one attempt could be viewed as

equivalent to the Windows NT default password policy: three invalid attempts and the user is locked out of the system. While there is no correct way to account for FAR/FRRs, consistency is the key when comparing data. Whereas a one to one attempt may give a truer measure of the device's performance, three attempts are more realistic for real world usage. It is not uncommon for a user to "fat finger" a password after a vacation and three attempts to get into their system is considered normal. Misplacement of a finger on the device or being distracted when using an iris reader could also be assumed to be normal usage considerations.

It must be noted that most biometric devices have thresholds that can be changed depending upon the administrator's wishes for security. The adjustable threshold settings allow system administrators to adjust the security policy of the devices (system) to affect false rejects and false accepts into the system. A balance needs to be struck between convenience and security. The threshold can be change to allow a stronger chance of false acceptances which would enable quicker response time for the device, i.e., the user can access the door quicker. It can just as easily be adjusted the opposite way to enable stronger security by increasing the likelihood of false rejects. This may lead to frustration of authorized users but security requirements may deem that this is better than risking access by an unauthorized person. It is also advisable to determine the needed setting of a device threshold and not just blindly accept the manufacturer's default setting.

Another issue affecting accuracy is the resolution and physical surface area of sensors. It is important to find out if changing the image capturing system's resolution affects the ability for user verification. As an example, the system administrator uses the default setting, 600 x 800 dpi, for capture of the iris image. If this setting is changed by the administrator, do previously enrolled users have difficulty? When using a fingerprint sensor, a small size for the sensor surface can decrease accuracy because a user will place their finger differently each time. This presents a slightly different area for comparison each time to the enrollment template, which may cause the system to reject the user and escalate your FRRs.

When considering biometrics device algorithms accuracy, the government has conducted testing for fingerprint and facial recognition systems. In 2000 and 2002 the following tests occurred:

- Fingerprint Verification Competition 2000, http://bias.csr.unibo.it/fvc2002/
- Fingerprint Verification Competition 2002, http://bias.csr.unibo.it/fvc2002/
- Face Recognition Vendor Test 2000, http://www.frvt.org/FRVT2000/default.htm
- Face Recognition Vendor Test 2002 http://www.frvt.org/FRVT2002/Default.htm

NIST has requested iris images for doing a similar benchmark test for the iris.

STANDARDS

A standard, as defined by the Webster's II New College Dictionary is: "An accepted measure of comparison for quantitative or qualitative value." (Riverside, p. 1074). An accepted measure for comparison is very much needed by the biometrics community. Proprietary formats have flourished due to the specific uses of the biometric products. If a company needed the extra security afforded by biometrics, it was of little concern that they would have to stay with a particular product due to the proprietary differences

among the vendors. The biometric was being utilized in such a small area that interoperability was of no concern. With recent events, such as the September 11th terrorist attacks, biometrics has been forced to the forefront of overall security. As such, there now stands the need for the products to enter the mainstream market which requires interoperability for a more generalized use. Without standardization, costs alone could be prohibitive in the biometric selection. If a company chooses a certain type of biometric, such as fingerprint, then picks a vendor with their own proprietary format, the company would finds itself locked into that vendor's products. If a user-friendlier version of the biometric were to come to market, the fact that the company has already invested their funds in the one vendor's proprietary system, meaning template and method of using the template and database, would preclude them from switching. Changing in midstream could require starting over to rebuild a database and put in new readers. Standardization in other industries has allowed the public to benefit from the multitude of products available that can be used interchangeably. An example is the 3-prong plug that can fit into the socket in any house in the United States. Biometrics needs to have standards adopted that will allow it to become that plug – anyone's reader or database can utilized any template.

STANDARDS ORGANIZATIONS

The Biometric Consortium is an association of private industry, government from the federal, state, and local level, and academia. The primary focus of the Biometric Consortium is to foster cooperation between the industries providing technologies for using biometrics and the users in both the government and commercial sectors. The U.S. National Security Agency (NSA) and the U.S. National Institute of Standards and Technology (NIST) Information Technology Laboratory preside over the mechanism of the Consortium. While the Consortium has many activities of interest, standards for biometric technologies have become an essential issue. In examining just a small sampling of a popular biometrics, say fingerprint, one can find the following companies with their own proprietary method of using their templates:

- Autentec, Inc.
- Identix
- Precise Biometrics
- Sagem Morpho, Inc.
- Ultra-scan Corporation

The need for standards is reflected in this list. If a company wants to use fingerprints for the biometric identifier, then once they've invested in one company's technology it is financially challenging to change.

Due to the terrorist events of the past year, the President of the United States signed into law the requirement to develop technology standards to confirm identity. Biometrics falls under this requirement since it is used for identification and verification of identity. Leading the way for biometric standardization for the federal government is the National Institute of Standards and Technology (NIST). NIST has demonstrated a critical role in development of biometric standards for many years. The standardization work in fingerprint searches was done under NIST's auspice as well as biometric imaging. With the passage of the Enhanced Border Security and Visa Entry Reform Act of 2002, NIST has been charged with developing and certifying standards to be used for verifying the identity of those entering the US through the use of visas. Biometrics is expected to

play a vital role in visa and passport issuance and usage. As of January 2003, NIST has settled on the fingerprint and face as the chosen biometrics for use at border crossings.

The American National Standards Institute (ANSI) was founded in 1918 with the purpose of coordinating a voluntary system for standardization and conformity for the United States. ANSI is not a governmental agency but rather a non-profit, private organization with the mission to: "enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity." (ANSI, http://www.ansi.org:80/about_ansi/overview/overview.aspx?menuid=1) ANSI is an organization that gives interested U.S. parties a neutral venue to come together and work towards common agreements and standards. ANSI is the means to promote our US standards in the international forum and acts as an advocate for US policies and technical positions. ANSI also works to promote the use of international standards as US national standards to meet the needs of the user community.

Another US entity involved in biometric standards is the InterNational Committee for Information Technology Standards (INCITS). They have established a technical committee, M1, to address biometric requirements. The purpose of M1 is to focus on an all-inclusive approach with a high priority towards the rapid development of generic biometric standards. This group was formed in November 2001 and has been successful in presenting and completing the INCITS fast track for Biometrics Applications Program Interface (BioAPI), which was approved in February 2002. M1 is also involved with the Common Biometric Exchange File Format (CBEFF) that was published in January 2001. An augmented version is in production for backward compatibility that will be submitted by M1 to INCITS for their fast track processing. M1 serves as the US Technical Advisory Group for both standards and will work towards fast tracking them as formal International Standards within the International Standards Organization (ISO). Another standardization that M1 is interacting with is for biometric templates. M1 actively interacts with other groups, both national and international, to attempt to limit conflict or duplication of standards development. To support the need for interoperability, scalability, and reliability, M1 is working towards the harmonization of generic international biometric standards with related standards-based applications and systems. INCITS/M1 also has five projects that are under development:

- Application Profile Verification & Identification of Transportation Workers
- Application Profile Personal Identification for Boarder Crossing
- Finger Minutiae Format for Data Interchange
- Finger pattern-Based Interchange Format
- Face Recognition Format for Data Interchange

These projects are to be sent into the International Standards Organization's Joint Technical Committee 1 Subcommittee 37 (ISO/IEC JTC 1 SC 37) for advancement and possible "fast tracking" for approval.

The Biometrics Management Office (BMO) is a Department of Defense (DoD) organization chartered by Congress through the Army, DoD's Executive Agent for biometrics. The BMO will lead, consolidate and coordinate the development, adoption and institutionalization of biometrics for the DoD. The aim of the technology is to

enhance Joint Services' security interoperability and the war fighter's operational effectiveness. The test and evaluation arm of the BMO is the Biometric Fusion Center (BFC). The BFC interacts with the military services, vendors, and academia to work towards establishing biometric standards. The BFC also does testing and performance measuring to evaluate biometric technologies for DoD usage. This will enable the BFC to provide technical implementation and integration support to the military services.

In the international arena, a group formerly known as the International Standards Organization's Joint Technical Committee 1 has been reformed as Subcommittee 37 (SC 37). There are approximately 20 countries involved in SC 37 through their own national standards bodies. Their purpose is to speed the development of biometric standards in a comprehensive manner for the international community. Areas within SC 37 with specific interest include technical interfaces, biometric vocabulary, and data interchange. For web-based usage, a group entitled Organization for the Advancement of Structured Information Standards (OASIS) is developing XML-based biometric standards.

Another international aspect affecting biometrics is the Common Criteria (CC) for Information Technology Security Evaluation. The CC came about from the Trusted Computer System Evaluation Criteria (TCSEC), developed in the US and the Information Technology Security Evaluation Criteria (ITSEC) developed in Europe based upon the TCSEC. The CC "defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems." (Common Criteria FAQ, p. 1). This allows for any country to then trust and use another country's product that has passed a CC evaluation since both countries will be basing the evaluation on the same testing and evaluation for security. This also opens the markets to developers from around the world while allowing for a better understanding of consumer requirements. The Common Criteria allows for countries to write protection profiles on explicit products that require that product to meet a set security level by addressing threats that exist in a specified environment. The Protection Profile provides "a reusable set of IT security requirements that can be certified as complete, consistent and technically sound." (Common Criteria Protection Profile, p. 1). Countries drafting their own biometric protection profiles in accordance with the Common Criteria include the US, the United Kingdom, Germany, and Canada. Copies of the most recently released drafts are available at: http://www.iatf.net/protection_profiles/biometrics.cfm.

APPROVED BIOMETRIC STANDARDS

Biometrics are still an emerging technology in an industry that is in flux and does not yet have comprehensive generic standards for usage and interoperability. As such, the Biometric Consortium along with the International Committee for Information Technology Standards (INCITS) and other groups are trying to move the industry to adopt some basic first-level standards to help continue with the field's growth. One of these standards is the Biometrics Applications Program Interface (BioAPI).

> "The BioAPI Specification provides for simple biometric application interfaces, standard access methods to biometric functions, algorithms, and devices; secured and robust biometric data management and storage; standard methods

> of differentiating biometric data and device types; and support for biometric identification in distributed computing environments…The BioAPI supports a wide range of biometric technologies including fingerprint imaging, speaker verification, facial recognition, iris scanning, dynamic signature, and hand geometry. 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."(Tilton, http://www.bioapi.org/BioAPI_news_press_files/press_files/PR01-001.html)

The Version 1.1 specification was released on March 20, 2001. On April 8, 2002, the BioAPI Consortium announced that the BioAPI Specification, Version 1.1 was approved and published by the INCITS as American National Standard Institute/International Committee for Information Technology Standards (ANSI/INCITS) 358. NIST worked with the BioAPI Consortium to help fast track this standard to the ANSI/INCITS. As a next step towards international interoperability, the M1 Technical Committee will continue to support the BioAPI's transition to an international standard through the International Organization for Standardization (ISO).

Another important standard for consideration is the Common Biometric Exchange File Format (CBEFF). The CBEFF defines a common set of data elements necessary to support multiple biometric technologies. This means that the CBEFF would help with the current limitations faced by companies switching to another vendor should a company decide a better deal can be had. The CBEFF makes possible the exchange of the biometric data between different components or systems. The CBEFF represents a standard biometric data record format specifically designed to facilitate biometric interoperability and utilization. A company would than be able to move from say, Indentix's fingerprint device to Precise Biometric's without the need to retool the current system in place. Development of the CBEFF includes endeavors to harmonize its data formats with the ANSI X9.84 (to be discussed later) and the BioAPI. Due to the growth of smart cards, the CBEFF will also work towards a smart card data format to work with existing ISO standards and keep a view towards future ISO developments. The CBEFF was published by NIST as NISTIR 6529 on January 3, 2001.

A standard accepted by the financial community, both nationally and internationally, is the ANSI X9.84. The full title for this standard is Biometric Information Management and Security. This standard states requirements for managing and securing biometric information such as customer identification and employee verification. It uses cryptographic message formats along with key management techniques to provide data integrity and authentication. Privacy of biometric matching and reference templates are also covered by this standard. This allows the financial community to use secure biometric information over the Internet. Since the binary formats used within X9.84 messages are very compact, they are suitable for use with smart cards, RFID (contactless) cards and other remote devices where a small message size is of utmost importance. An ongoing problem with X9.84, and biometric standards in general, is that many are not backwards compatible. When the X9.84 was first published in 2001, the BioAPI 1.0 was the expected standard for APIs, so X9.84 was harmonized with it. With the acceptance of ANSI/INCITS 385 (BioAPI 1.1), which is not backwards compatible with BioAPI 1.0, biometric data formats in these two standards can no longer be

mapped to each other. Another system that does not harmonize with X9.84 is the XML (eXtensible Markup Language). Many web applications can only send and accept information in the XML format. The XML Encoding Rules (XER) did not exist when X9.84 was originally published so there is no security requirements defined for processing XML formatted messages with biometric data. X9.84 has since undergone a revision to provide a common XML functionality that will include a common XML markup representation for X9.84 and BioAPI 1.1 biometric information to promote biometric information exchange. This will be based on the ASN.1 schema, as defined in X9.84 and the XER to provide data integrity, authentication and privacy services.

An e-ballot was issued by the Accredited Standards Committee X9 for X9.84 Biometric Information Management and Security in January 2003. On February 18, 2003, the ballot was closed and approved. The revision includes references for XCBF (defined below) and follows the XML encoding and cryptographic processing for the latest version of X9.73 Cryptographic Message Syntax (CMS).

The Organization for the Advancement of Structured Information Standards (OASIS) is one of the latest groups to join the biometric community. Their mission is to create an XML Common Biometric Format (XCBF) to "…provide a standard way for biometric functions to be done using XML." (Pace Picks Up for Biometrics Standards Development, ANSI Online, p.2).

The American Associate of Motor Vehicle Administrators (AAMVA) is an organization that the public would not generally expect to be involved in biometrics. AAMVA has been working on the ANSI standard B10.8, National Standard for Drivers License/Identification Card 2000-06-30 which contains the specifications for interoperability among different fingerprint vendors when comparing images and using the minutiae data gathered from the fingerprint for formation of a template. This format provides a uniform method for usage of the data in a template on a driver's license, which in turn, enables a uniform means of identifying the holder of the driver's license both across state lines and in Canada. This standard specifies which fingers are to be used, in an order of precedence, a minimum of two fingerprints will be taken, and compression requirements for the imaging. As expected, when there are current standards available, it is better to require conformance with them than attempt to create your own. The use of fingerprints has existed within the law enforcement community for many decades. As such, the AAMVA has required conformance with two of the law enforcement community's current standards: Criminal Justice Information Services CJIS/FBI IAFIS-IC-0110 Wavelet Scalar Quantization (WSQ) (http://www.itl.nist.gov/iad/894.03/fing/cert_gui.html) and CJIS-RS-0010, Electronic Fingerprint Transmission Specification (EFTS) (http://www.fbi.gov/hq/cjisd/iafis/efts_70.pdf) .

IAFIS-IC-0110 is the Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Specification and applies to fingerprint format and transmission standard used by the Criminal Justice Information Services (CJIS), Federal Bureau of Investigation. It was approved February 16, 1993. CJIS-RS-0010 is the specification that defines the interface between the Integrated Automated Fingerprint Identification system (IAFIS) and the States' systems.

> "Any changes to the data fields or formats within the EFTS must honor previously published protocols to ensure that the States' systems are not adversely affected. Since IAFIS and the States' systems are being developed independently, a process has been established which provides for coordinated enhancements within the various systems while maintaining reliable interoperability. This process is based in the tagged field structure defined in the 1993 ANSI standard, and a few "business rules"." (FBI website, http://www.fbi.gov/hq/cjisd/iafis/efts70/section1.htm)

For a copy of the AAMVA National Standard for Drivers License/Identification Card 2000-06-30, go to URL: http://www.aamva.org/Documents/stdAAMVADLIDStandrd000630.pdf.

Another law enforcement standard that is applicable to biometrics is the ANSI/NIST-ITL-1-2000. This is the standard used for data format for the interchange of fingerprint, facial and scars, marks and tattoos (SMT) data across jurisdictional lines. This standard also provides the format for data exchange between dissimilar systems from different vendors. It was approved July 27, 2000 and stands as a key component in allowing interoperability in the justice community.

TECHNOLOGY SELECTION CONSIDERATIONS

There are a number of areas that will require standards for user interoperability. First let's start with data collection. How the device will interface, how the data is stored and what type of capture is done to prove liveness at the scan point are all aspects of data collection. When the template is transmitted, the compression and expansion methods need to be standardized to enable the interoperability of devices and software. This is also related to the way the signal is processed to enable feature extraction. Storage needs to be addressed, particularly in the security arena. The methods of protection, from hashing to digital signature to encryption need to be defined and standardized.

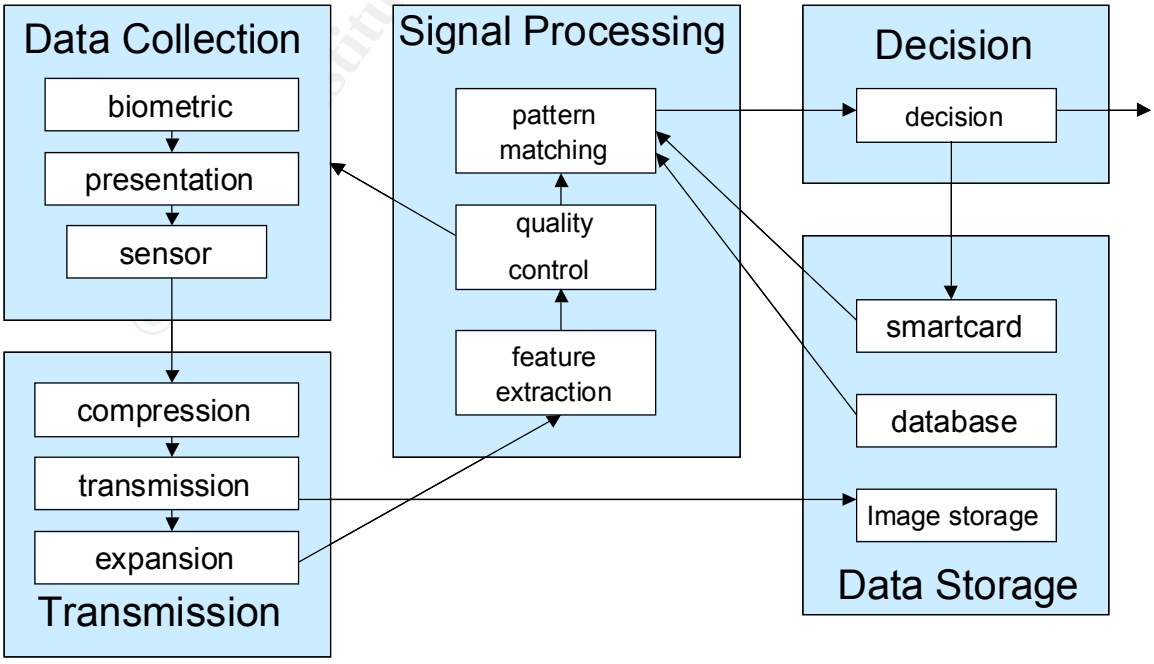

Figure 2. Generic Biometric System (Baumgardner, slide 5)

As stated in the Concepts in Biometric Systems & Information Assurance course offered by the West Virginia University: "An automated biometric system uses biological, physiological or behavioral characteristics to automatically authenticate the identity of an individual based on a previous enrollment event." For a characteristic to serve as a biometric it must have the following properties: uniqueness, permanence, universality, and collectability.

- Uniqueness – no two individuals possess the same characteristic, this uniqueness can be proven and is distinguishable.

- Permanence – the characteristic is not affect by time or is affect at such a slow rate that it can be compensated for. This property has a major impact on long-term usage of biometrics due to general population aging and is still being explored for effects on long-term storage.

- Universality – every person should possess this characteristic. Under this property are two concerns:
    - Genotypical – genetically linked, such as in the case of identical twins
    - Phenotypical – different on the same person, i.e., each finger has a different print

- Collectability – the property can be measured quantitatively. From the user's point of view, the intrusiveness of collection plays an important role.

These properties that make up the characteristics of the biometric are then tested for performance, user acceptance, and resistance to circumvention. Under performance, one must consider the accuracy requirements for the FAR/FRR; how will the biometric be used – for identification (one to many) or verification (one to one). Has the testing of the performance been done consistent with best practices? Some sources for best practices are the Biometric Consortium, www.biometrics.org, the United Kingdom's Communications-Electronics Security Group (CESG) Biometrics Working Group, www.cesg.gov.uk/technology/biometrics and the International Biometrics Group, www.biometricgroup.com. Also, in reference to the FAR/FRR above, what are the capabilities for adjusting the threshold on the biometric device? As stated before, security requirements affect the threshold adjustment in consideration of either convenience (more chances of FARs) or stronger security (higher possibility of FRRs). Another aspect of the threshold is the ease of accommodation for changing requirements, such as an increase in the security threat level.

The next criterion is user acceptance. Current research has found that user perception plays an extremely important role in acceptance of biometrics. There are some cultures where to touch a device after someone else just has is considered extremely dirty and unacceptable. Also the current perception of use, such as the law enforcement side to fingerprints, impinges upon the user's willingness to accept a more general practice. These can be dealt with by user education on the device along with possible utilization of direct feedback. Fingerprint readers do tend to get dirty with multiple uses so as a way to increase user acceptance, some type of scheduled maintenance or ability for the user to "clean" the reader before utilizing it may need to be included. As part of the

education process, positive feedback from prior demonstrations and installations could be included to allay user fears and concerns. The worse case would be to dismiss the user's perception of the technology as irrelevant. The best device could easily be dismissed by the user population as a whole if perceptions are left unaddressed, example – the beta format for tape was better than VHS (Video Home System) but the VHS addressed the customer's needs and perceptions on ease of use.

A final criterion to consider is the biometric device's resistance to circumvention. This would also tie directly into the performance requirements. If a risk assessment has been done, does the device meet requirements? Countermeasures need to be consider not only for the device itself, but also for the software that is being used with the device and any hardware that it connects to. The issue of spoofing is an ongoing concern within the biometrics community. How hard is it to fool the device? Along this avenue is the concept of liveness. Liveness is the conceptual issue that the biometric device can detect whether the biometric sample being presented is from a living, breathing person. Liveness means that the biometric device has the capability to detect that the biometric is alive, not recently removed from the authorized user's person. Two methods being explored for liveness include the electrical charge carried by the skin and the amount of moisture found in live tissue.

VENDOR ISSUES

Besides the above mentioned method of counting 3 attempts as one try, there are a number of issues related to vendors that need to be answered, preferably before the decision is made on which biometric device and vendor to utilized.

When selecting a vendor, the past performance and track record should be carefully examined. Are they responsive to inquiries? Will they still be in business next month? Biometric technology is evolving at an extremely fast pace and many companies are in the process of merging to better strengthen their market position. If this happens to the company that you are dealing with, what are the arrangements for product service, warranty issues, platform or device migration, etc? When considering the technical aspect of a vendor's product, be sure to examine the peripheral hardware format, interface, and platform requirements. What support is there for your current platform and where will that support be if you plan to migrate to another? In reference to the software development kit (SDK), be aware of required "system hooks" availabilities to meet platform requirements. As referred to above in the FAR/FRR section, questions to ask the vendor include the image that is used for the matching – is it the raw image or does the software "clean" it up? Due to possible security concerns, the system administrator will need to understand device contract/image control, confidence measure for access, and threshold access/adjustment for any particular system/device. Another very important issue relating to a vendor is the methods of testing – does the vendor endorse the best practices testing results being encouraged by the major biometric communities? What standards does the vendor currently use/support and what future ones are being considered? How is compliance with the standards shown? Is it self-compliance or are they involved with various biometrics communities who do independent testing?

CONCLUSION

The biometrics industry is working towards standards as the technology becomes more commonplace in the world. The events of the September 11, 2001 terrorist attack in the United States has helped to advance the federal government's involvement in biometrics as more than just a logical access security feature but as an overall access and identity authentication solution. Departments such as NIST, the Transportation Security Agency and the Department of Homeland Security require the advancement of standards to enable the certification of biometric devices and systems for governmental usage. Vendors are finding that interoperability created by standardization, not proprietary systems, is in their best interest if they want to be evaluated and certified to market to the federal government. And the federal government is not the only user of biometrics. The commercial sector has found that interoperability allowed by standardization enables it to move to biometrics as a continuing method of upgrading security. If a business is no longer locked into one biometric system due to retooling costs, then businesses will find they can consider biometrics across the spectrum for identity authentication needs.

Vendor certification also works to a company's benefit when dealing with the international community. The Common Criteria enables the vendor to have his product certified in an internationally understood methodology. This allows businesses to interact and employ any certified vendor from across the international community.

The growth of biometrics is not without its problems. Privacy issues still need to be addressed. With standardization, it will be easier for both the public- and the private-sector to address the taxpayer's/consumer's issues with privacy and general usage of biometrics and to then enhance the acceptance of this method for ensuring identity verification and increasing security.

ACRONYMS

AAMVA	American Associate of Motor Vehicle Administrators
ANSI	American National Standards Institute
ASN	Abstract Syntax Notation
ATM	Automated Teller Machine
BFC	Biometrics Fusion Center
BIOAPI	Biometrics Applications Program Interface
BMO	Biometrics Management Office
CBEFF	Common Biometric Exchange File Format
CC	Common Criteria
CESG	Communications-Electronics Security Group
CJIS	Criminal Justice Information Services
CMS	Cryptographic Message Syntax
DEERS/RAPIDS	Defense Eligibility Enrollment Reporting System/Real-Time Automated Personnel Identification System
DOD	Department of Defense
EER	Equal Error Rate
EFTS	Electronic Fingerprint Transmission Specification
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FRR	False Rejection Rate
GSA	Government Services Agency
HIPAA	Health Insurance Portability and Accountability Act
IAFIS	Integrated Automated Fingerprint Identification System
INCITS	InterNational Committee for Information Technology Standards
INS	Immigration and Naturalization Service
ISO	International Standards Organization
ISO/IEC JTC 1 SC 37	International Standards Organization's International Technical Commission Joint Technical Committee 1 Subcommittee 37
ITSEC	Information Technology Security Evaluation Criteria
NSA	National Security Agency
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OS	Operating System
RFID	Radio Frequency Identification
SC 37	Subcommittee 37
SDK	Software Development Kit
SMT	Scars, mars and tattoos
TCSEC	Trusted Computer System Evaluation Criteria
VHS	Video Home System
WSQ	Wavelet Scalar Quantization
XCBF	XML Common Biometric Format
XER	XML Encoding Rules
XML	eXtensible Markup Language

REFERENCES

American National Standards Institute, “About ANSI.” ANSI Online Standards Store. URL: http://www.ansi.org:80/about_ansi/overview/overview.aspx?menuid=3 (3 Mar 2003)

American National Standards Institute. “Pace Picks Up for Biometrics Standards Development.”6 Nov 2002. URL: http://www.ansi.org/public/news/2002apr/biometrics_standards.htm

Baumgardner, James. "Common Access Card-Biometrics Working Group – Standards Team." DoD Biometrics Management Office (11 Nov 01): slide 5.

BioAPI Consortium, “Press Releases”, June 7, 2002. http://www.bioapi.org/

Biometric Management Office, “Mission Statement.” Biometrics Department of Defense About Us. URL: http://www.c3i.osd.mil/biometrics/ (3 Mar 2003)

Common Criteria FAQ “Frequently Asked Questions,” December 9, 2002. URL: http://www.commoncriteria.org/faq/faq.html

Common Criteria Protection Profiles “Protection Profiles ,” December 9, 2002. URL: http://www.commoncriteria.org/protection_profiles/index.html

Connecticut Department of Social Services “Biometric ID Project”, Biometric Vendors/Consultants, URL: http://www.dss.state.ct.us/digital/divend.htm

Department of Justice Federal Bureau of Investigation, “Electronic Fingerprint Transmission Specification “, CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) ELECTRONIC FINGERPRINT TRANSMISSION SPECIFICATION, URL: http://www.fbi.gov/hq/cjisd/iafis/efts70/section1.htm

Hornack, Larry; Cukic, Bojan; Schuckers, Michael; Shank, Robert. “5-Day Short Course: Concepts in Biometric Systems & Information Assurance.” CITer, West Virginia University (2002): 1-7 to 1-9, 2-45 to 2-57, 2-59 to 2-60, 3-33.

International Biometric Group. “Biometric Standards.” Teleconference of January 9, 2003.

National Institute of Standards and Technology, U.S. Department of Commerce and the Biometrics Consortium “CBEFF Common Biometric Exchange File Format,” January 3, 2003. http://www.itl.nist.gov/div895/isis/bc/cbeff/

National Institute of Standards and Technology, U.S. Department of Commerce “CBEFF Common Biometric Exchange File Format,” NISTIR6529, January 3, 2001. http://www.itl.nist.gov/div895/isis/bc/cbeff/CBEFF010301web.PDF

Poldio, Ferando. “Status of Biometric Standardization (Updated).” Biometric Consortium. Undated.

Riverside. Webster's II New College Dictionary. Boston, MA: Houghton Mifflin Company, 1995.

Tilton, Cathy. "BioAPI Consortium Announces Release of Final Specification and Reference Implementation." 20 Mar 2001. URL: http://www.bioapi.org/BioAPI_news_press_files/press_files/PR01-001.htm (2 Jan 2003).

X9 Accredited Standards Committee, "ANNOUNCEMENT TO MEMBERS X9.84 REVISION." 24 Feb 2003. URL: http://list.oasis-open.org/archives/xcbf/200206/doc00001.doc

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event