Statement by
Jeffrey S. Dunn
Fernando L. Podio
Co-Chairs, Biometric Consortium
Before the
Commission on Online Child Protection
9 June 2000
Washington, D.C.

Mr. Chairman and members of the Commission, we would like to thank you for the opportunity to speak today about biometric authentication technology. We believe this Commission's interest in biometric technology is very timely. Biometric technology is one means to achieve fast, user-friendly authentication with a high level of accuracy. Recent advances in biometric technology have resulted in increased accuracy at reduced costs.

Today, to address the Commission's interest in biometrics, we would like to discuss some of the terminology used by the biometric community, highlight some of the benefits of using biometrics for authentication, and give some examples of emerging applications and standards. We would also like to explain how the Biometric Consortium[1] is bringing together technologists from government and industry.

Introduction

Biometrics are automated methods of recognizing a person based on physiological or behavioral characteristics. Examples of human traits used for biometric recognition include fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins. During **Enrollment**, a sample of the biometric trait is taken, processed by a computer, and stored for later comparison. Biometric recognition can be used in **Identification** mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called “one-to-many” matching. A system can also be used in **Verification** mode, where the biometric system authenticates a person’s claimed identity from their previously enrolled pattern. This is also called “one-to-one” matching. In most computer access or network access environments, verification mode would be used. A user enters an account or user name as usual, but instead of entering a password, a simple touch with a finger or a glance at a camera would be enough to authenticate the user.

Biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions. Areas that will benefit from biometric

technologies include network security infrastructures, government IDs, secure electronic banking, investing and financial transactions, wireless communications, retail, and health and social services. Highly secure and trustworthy electronic commerce, for example, will be essential to the healthy growth of the global economy. Many biometric technology providers are already delivering biometric authentication for a variety of web-based and client/server based applications to meet these and other needs.

Advantages of Biometrics for Authentication

Using biometrics for identifying human beings offers some unique advantages. Only biometrics can identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys, and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember dozens and dozens of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites, and so forth. Biometrics hold the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications.

There is no one “perfect” biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that “no two fingerprints are alike.” Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have come into widespread use. Some newer biometric methods may be just as accurate, but may require more research to establish their uniqueness.

Another key aspect is how “user-friendly” a system is. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. Low cost is important, but most implementers understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware.

Biometric authentication for age verification

With the current state-of-the-art in biometric technologies, there are no means to determine the age of an individual based on a physical or behavioral characteristic. Given the wide variability of human characteristics, it seems unlikely any that such technologies will be available in the future.

The most likely benefit biometric technologies can provide is to enable quick and accurate authentication of authorized users. Three areas where biometrics might prove to be beneficial are:

1. **Workstation Access:** Biometric authentication could be used at workstations in homes, offices, schools, or other locations to ensure only previously authorized users have access to the workstation.

2. **Account Access:** Biometric authentication could be used to replace passwords for access to accounts provided by Internet Service Providers (ISP).

3. **Web access:** Biometric authentication could be required for access to specific web sites, for database access, or to download data.

The advantage biometric authentication provides is the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users. An indication of the biometric industry's substantial growth and maturity is the emergence of biometric industry standards and related activities.

Biometric industry standards

Biometric industry standards are now emerging. The development of industry standards are a sign of maturity in an emerging technology such as biometrics; industry standards assure the availability of multiple sources for comparable products and of competitive products in the marketplace. Standards have a major impact on our lives. They are vital to industry, commerce, the end users, and the Enterprise[2]. Standards promote understanding between buyers and sellers and facilitate mutually beneficial commercial transactions. They spur competition, expand markets, and increase user's confidence by promoting products that prevent the sole source lock-in. In a global economy, standards have become strategic business issues[3]. Current biometric standard activities include:

- Proposed Draft ANSI/NIST-ITL 1-1999, specifying a data format for the interchange of fingerprint, facial and scar, mark, and tattoo (SMT) information [4]. This standard is a revised version of ANSI/NIST-CSL 1-1993 Standard [5]. (A revision of ANSI/NIST-ITL 1-1999 is currently in progress.)

- X9F4 Remote Access to Financial Data Working Group is developing a standard that specifies the minimum security requirements for effective management of biometrics data for the Financial Services Industry (X9.84 – Biometric Information Management and Security) [6].

- ♣ The Human Recognition Services (HRS), an extension of the Open Group's Common Data Security Architecture (CDSA) is synchronizing the development of HRS with the BioAPI Consortium effort. CDSA provides a comprehensive and coherent set of security services covering the essential components of security capability [7].

- ♣ TeleTrusT, a non-profit organization in Germany is approaching standards and analyzing biometrics in security environments. TeleTrusT formed a Biometrics Identification Systems Working Group to address these issues [8].

- ♣ B10.8, Driver License and Identification Card Tasks Group's Biometric Task Force (Sub-Group) is developing a draft technical standard for Finger Minutiae Extraction and Format for One-to-One Verification (Authentication) Systems [9].

- ♣ The Biometric Consortium, NIST, and NSA are sponsoring the development of a Common Biometric Exchange File Format (CBEFF). CBEFF is a standard format that an application can utilize to recognize what type of biometric (software and devices) is available in a system, the version number, the vendor name, etc. A common format facilitates interoperability between different biometrics technologies [10].

- ♣ In addition to technical standards, industry practices on ethics and privacy are also being developed. The International Biometric Industry Association (IBIA) is plays a crucial role in the development of these standards [11].

Biometric APIs

An Application Programming Interface (API) defines the way for a software application to communicate with a technology service or module. The API defines the application request services and handles communications to and from these services or modules. They are usually composed of a set of function calls that include data and control parameters, and defined data structures.

A Biometric API standard defines a generic way of interfacing with a broad range of biometric technologies as well as defining a common method of interfacing with a particular biometric technology. In April 2000, the **BioAPI v.1** specification was released by the BioAPI Consortium, a group of over 50 organizations including biometric vendors, major IT corporations, system integrators, and users [12].

The BioAPI is an emerging global industry specification. The BioAPI Consortium plans include submitting the specification to a standards body for further standardization as a national and/or international standard. BioAPI allows for simple integration of multiple biometrics, the use of a

specific biometric technology across multiple applications, and easy substitution of biometric technologies.

BioAPI is planned as a public-domain multi-level API standard that allows for both verification and identification applications. The initial reference implementation will support Win32 operating systems.

BioAPI includes:

- simple biometric application interfaces
- standard modular access to biometric functions, algorithms, and devices
- secured and robust biometric data management and storage
- standard methods of differentiating biometric data and device types
- support for biometric identification in distributed computing environments

A key advantage of systems compliant to this specification is that applications can easily substitute one biometric technology for another without modification to the application. The BioAPI specification allows for simple integration of multiple biometrics in an application and the utilization of a specific biometric technology across multiple applications.

In addition to benefiting end-users and the Enterprise, a standard biometric API benefits system developers and the biometric industry. The common, top-level interface as defined in BioAPI v1.0 allows applications to be written once without risk of having to support different interfaces in the future. The standard also provides for flexibility of Biometric System Provider (BSP) implementation. As specified in v1.0, biometric vendors may implement a monolithic BSP, a layered BSP or special purpose objects and still comply with the standard. For those applications requiring control of biometric algorithms and devices, access to lower level functions is provided.

A common specification will hasten adoption of biometric technologies and biometric-based identification and verification solutions in multiple markets. In the near future, a large variety of BioAPI- compliant vendor biometric modules and applications are expected.

The BioAPI Consortium is currently developing a BioAPI reference implementation. A test suite for the reference implementation will follow.

Biometric Consortium

The Biometric Consortium was chartered as a Working Group on 7 December 1995 by the Facilities Protection Committee, a committee that reports to the Security Policy Board established by the President. Quoting from the Biometric Consortium charter,

> "The Consortium will serve as a Government focal point for research, development, test, evaluation, and application of biometric-based personal identification / authentication technology."

The Biometric Consortium now has over 700 members from government, industry, and academia. Over sixty different federal agencies participate in the Biometric Consortium. The main benefit of the organization is to share information about biometric technology among the members. This is done through conferences and workshops, through an electronic mail list, and through the Biometric Consortium's web site on the Internet.

Biometric Consortium World Wide Web Homepage

The Biometric Consortium web site at http://www.biometrics.org/ is open to everyone and contains a variety of information on biometric technology, research results, federal & state applications, and other topics.

Summary

There is great demand for the fast, accurate authentication that biometric systems can provide. Continued improvements in technology will bring increased performance at a lower cost. Biometric authentication, however, is not a magical solution that solves all authentication concerns. A complete systems approach that addresses a variety of security, functional, operational, and cost considerations is always necessary. The growth of biometric technology will place greater demand on both biometric system developers and users to work together to address a number of issues including privacy, testing, infrastructure, and standards. The Biometric Consortium provides a forum to facilitate this work.

Certain company names or specific biometric technologies that may have been identified in order to adequately describe the subject matter in no way imply endorsement by the Biometric Consortium, the National Institute of Standards and Technology, or the National Security Agency, nor does it imply that companies identified are the only providers of the biometric technologies referred to in this statement.

References

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

[2] M. A. Breitenberg, Office of Standards Code and Information, Office of Product Standards Policy, National Institute of Standards and Technology, *The Abc's Of Standards-Related Activities In The United States,* NBSIR 87-3576, May 1987.

[3] Robert B. Toth, Editor, Office of Standards Services, National Institute of Standards and Technology, *Profiles of National Standards-Related Activities,* NIST SP 912.

[4*] Draft ANSI/NIST ITL 1-1999, Data Format for the Interchange of Fingerprint, Facial, & Scar, Mark & Tattoo (SMT) Information,* http://www.itl.nist.gov/iaui/894.03/fing/stand2.html

[5] *ANSI/NIST-CSL 1-1993, Data Format for the Interchange of Fingerprint Information,* http://www.itl.nist.gov/iaui/894.03/fing/stand1.html

[6] *ANSI X9,* http://www.x9.org

[7] *Open Group CDSA web site:* http://www.opengroup.org/security

[8] *Teletrust web site:* http://www.teletrust.de

[9] *AAMVAnet, Inc. Standards Development web site:* http://www.aamva.org/aamvanet/indexStandards.html

[10] *Common Biometric Exchange File Format web site:* http://www.nist.gov/cbeff

[11] *International Biometric Industry Association (IBIA) web site:* http://www.ibia.org

[12] *BioAPI Consortium web site:* http://www.bioapi.org

Fernando Podio, Co-Chair Biometric Consortium

Fernando Podio has been involved in information technology development, measurements, and standards development efforts for many years. He is a member of the National Institute of Standards and Technology (NIST), Information Technology Laboratory. He is currently the Program Manager for NIST's Biometrics and Smart Cards Program. This program is conducting research into the interoperability and performance of biometric subsystems, devices and applications, and the integration of biometrics and smart cards. Mr. Podio serves on the BioAPI Consortium Steering Committee and chairs the BioAPI Consortium's External Liaisons Working Group

Jeff Dunn, Co-Chair Biometric Consortium

Jeff Dunn is Chief of the Identification and Authentication Research Branch at the National Security Agency. This group is researching new technologies to protect access to computer systems in the Department of Defense and other critical systems. During his 20-year career at NSA, he has held a variety of program manager and management positions. He is a graduate of the Agency's Management Development Program and certified as an Acquisition Professional. Mr. Dunn has provided consultations on biometric technologies to a wide range of Government organizations.