INCITS M1/07-0185rev

InterNational Committee for Information Technology Standards
INCITS Secretariat, Information Technology Industry Council (ITI)
1250 Eye St. NW, Suite 200, Washington, DC 20005
Telephone 202-737-8888; Fax 202-638-4922
Email: incits@itic.org

Title: **Study Report on Biometrics in E-Authentication**

Source: **M1.4 Ad Hoc Group on Biometric in E-Authentication (AHGBEA)**

Date: **30 March 2007**

Version	Date	M1 Document #	Comments
0.1	28 Nov 2005	M1/05-0772	First base document
0.2	06 Feb 2006	M1/06-0112	First Working Draft
0.3	15 May 2006	M1/06-0424	Second Working Draft
0.4	28 June 2006	M1/06-0585	Revised Second Working Draft
0.5	21 August 2006	M1/06-0642	Third Working Draft
0.6	12 October 2006	M1/06-0693	Fourth Working Draft
0.7	1 November 2006	M1/06-0916	Fifth Working Draft (First Letter Ballot)
0.8	9 January 2007	M1/06-1027	Sixth Working Draft (Proposed Disposition of Comments)
0.9	6 February 2007	M1/06-1027rev	Sixth Working Draft Revised (Second Letter Ballot)
1.0	30 March 2007	M1/07-0185	Final approved report

Executive Summary

In December 2003, OMB issued M-04-04, "E-Authentication Guidance for Federal Agencies." Subsequently, in September of 2004, NIST issued SP800-63, "Electronic Authentication Guideline." This document, which forms the technical basis for the US government's e-authentication initiative, part of e-Gov, specifies the requirements, technologies, and protocols to be used at each of the four assurance levels defined in the OMB directive. However, it allowed for a very narrow usage of biometric authentication in this context. As a follow-on, NIST held a workshop on Biometrics in E-Authentication, which spawned a study group within INCITS M1 (consisting of representatives from industry, academia, and government) to investigate and make recommendations regarding how biometrics should be applied in a remote e-authentication environment. This report is the product of that group, which met over a period of 1.5 years.

Biometrics-based authentication offers several advantages over other authentication methods, prompting a significant surge in the use of biometrics for user authentication in recent years. It is important that such biometrics-based authentication systems be designed to withstand attacks when used in a remote e-authentication environment. This document outlines inherent strengths of biometrics-based authentication, identifies challenges and potential vulnerabilities in systems employing biometrics-based authentication, and presents solutions for eliminating these weak links. A threat model is presented and overlaid on several possible biometric authentication architectures which vary depending on the location where the biometric reference is stored and where the matching operation is performed.

An open discussion of some of the challenges (or critiques) of biometric authentication addresses topics such as integrity versus secrecy, compromise and revocation, sensor spoofing, entropy and strength of function, peer review, and privacy. Differences between biometric authentication and traditional authentication methods (such as passwords or cryptographic protocols) are also examined.

The major findings of this report are:

1. There is a role for biometric authentication at each of the four assurance levels defined in OMB M-04-04
2. Some additional challenges and threats accompany the use of biometric authentication, but countermeasures exist to address them
3. Biometric authentication can provide significant benefits in certain situations, not least of which is the tight binding of the authentication event to the physical presence of a human claimant
4. Biometrics present a different paradigm than traditional authentication methods where authentication data is always secret.
5. In general, integrity and authenticity are more critical than secrecy in a biometric authentication protocol/implementation, although many mechanisms exist to provide for the privacy of the biometric data.
6. In addition, some biometrics may be used to convey ancillary information, such as a secret (e.g., a password or PIN) or shared knowledge, by leveraging the ability of the user to control the manner in which the biometric is presented to the system
7. Recommended edits to SP800-63 are provided in Annex A of this report

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

As a result of the Workshop on Biometrics and E-Authentication over Open Networks held March 30-31, 2005 by NIST, the workshop participants recommended areas for further work related to biometric architectures and security requirements. These recommendations, developed by the participants of workshop breakout session 2, "Elements of Secure Biometric-Based Authentication Systems", included a request that INCITS Technical Committee M1 - Biometrics start a project for documenting, within an application profile, the use of biometrics for remote e-authentication and perhaps also initiate a study project to draft a technical report describing biometric architectures & security requirements. In addition to considering current related standards and other documents that have cited known issues with this architecture, the study attempts to look forward to potential applications as these standards find use in a broader commercial, civil, and international community.

1.2 Scope

The Ad Hoc Group on Biometrics and E-Authentication (AHGBEA) was chartered by INCITS M1.4 – Task Group on Biometric Profiles in June of 2005. The approved charter of this group was set out in its terms of reference to:

> Develop a technical report describing suitability of biometric architectures, security requirements and recommendations for the use of biometrics at each of the four authentication levels defined in Office of Management and Budget's Memorandum OMB M-04-04, E-Authentication Guidance for Federal Agencies (assuming biometrics would be allowed for each of these authentication levels).

1.3 Purpose

The ultimate goal of the ad hoc group and the document is to show how biometric technologies can be successfully used at the four (4) assurance levels of OMB 04-04 and NIST SP800-63 and further to make recommendations of future work to INCITS M1 and NIST on the use of biometrics in e-authentication.

1.4 Overview

1.4.1 Assumptions

It is assumed that biometric characteristics, although personalized to individual users, are not necessarily secrets. Latent and other residual data can be obtained by an individual without the user's knowledge. This classification is explicitly mentioned in the NIST SP800-63 statement, "Biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document."

1.4.2 Premise

The assertion going in to this report is that NIST did not fully utilize the benefits of biometric authentication in the original SP800-63 publication. M1 feels biometrics have merit in e-

authentication applications and the following paragraph is quoted to highlight the NIST acknowledgment of the usefulness of biometrics.

> **NIST SP 800-32 Section 2.2.4 in its entirety**
> … "Biometric authentication relies on a unique physical characteristic to verify the identity of system users. Common biometric identifiers include fingerprints, written signatures, voice patterns, typing patterns, retinal scans, and hand geometry. The unique pattern that identifies a user is formed during an enrollment process, producing a template for that user. When a user wishes to authenticate to the system, a physical measurement is made to obtain a current biometric pattern for the user. This pattern can then be compared against the enrollment template in order to verify the user's identity. Biometric authentication devices tend to cost more than password or token-based systems, because the hardware required to capture and analyze biometric patterns is more complicated. However, ***biometrics provide a very high level of security because the authentication is directly related to a unique physical characteristic of the user which is more difficult to counterfeit.*** Recent technological advances have also helped to reduce the cost of biometric authentication systems."…

1.5 Policy Boundaries

As with many modern day information technology environments, using biometrics for e-authentication is not strictly a technical issue. Management policies are needed to bridge the gap between people and technology. Some organizations may already have in place specific information security policies related to what data can enter and exit their network. The remote nature of the subject environment will demand the application of appropriate policies to the common procedures of a biometric system. Further recognized is the fact that some societies have inherent beliefs and customs which constrain the use of some or possibly all forms of biometric authentication.

2 Study Methodology

The general methodology for addressing the problem and goals of this study is defined below:

2.1 Current Guidance – Section 3

The current guidance is established in OMB M-04-04 and NIST SP800-63.

2.2 Frame the Problem – Section 3

At this step, an attempt is made to bind the problem such that it is understandable and addressable.

2.3 References – Section 4

Previous work is identified in the references and in the bibliography. This report includes and summarizes selected works and is not meant to be a holistic research report of past works.

2.4 Authentication Principles and Biometrics – Section 5

A review of authentication principles is covered as well as the authentication model proposed in SP800-63 and correlated with the biometric authentication process.

2.5 Biometric Authentication Architectures – Section 6

There are numerous ways to design and configure a biometric authentication system. To reduce the solution space, the basic biometric system architectures are reviewed and the most feasible identified for the purpose of this report and further study.

2.6 Challenges to Biometric Authentication – Section 7

It is necessary to identify the critiques of biometric technologies that exist to better understand why they are not currently viewed as an acceptable authentication mechanism in the remote e-authentication environment.

2.7 Threats and Vulnerabilities for Biometric Authentication – Section 8

The use of a particular technology within a given architecture must be analyzed in terms of the threats, vulnerabilities, attacks, and countermeasures that exist.

2.8 Recommend Guidance – Section 9

Once all architectures have been analyzed against categories of threats and specific security requirements have been identified; recommendations can be formed as to when and how the technology, architecture, mechanisms should be applied to the security levels in OMB 04-04 and NIST SP800-63.

2.9 Future Work – Section 10

Based on the complexity of the problem, it is not presumed that this study will be able to fully resolve all issues and considerations associated with the use of biometrics in an e-authentication

environment. As a result, a section has been included to identify those areas that are known to require further investigation.

2.10 Recommended Edits to SP800-63 – Annex A

Taking into consideration all of the detailed discussion included in the body of this report, specific recommended edits and changes to SP800-63 by section are described.

3 Statement of the Problem

3.1 The Problem

"What is the role of biometric authentication at the various security levels and what architectures and surrounding security mechanisms are appropriate for use in the remote e-authentication environment?"

SP800-63 puts it well, "E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network, for the purpose of electronic government and commerce."

3.2 Office of Management and Budget (OMB), M-04-04

In December 2003, OMB issued the memorandum 04-04 with the subject "E-Authentication Guidance for Federal Agencies". This memorandum applies to remote authentication of human users of Federal Government Services for the purposes of conducting government business electronically (or e-government).

OMB M-04-04 defines four (4) assurance levels related to the degree of confidence in the validity of the asserted identity. It is a risk based approach based on potential impact and likelihood as defined in Federal Information Processing Standards 199 *Standards for Security Categorization of Federal Information and Information Systems.*

Table 1 below summarizes these four (4) assurance levels with examples from the guidance. Table 2 classifies the four (4) assurance levels based on potential risk impact.

Table 1 - OMB M-04-04 Maximum Potential Impacts for Each Assurance Level

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Table 2 - OMB M-04-04 Assurance Level Examples

Level	Confidence	Example
1	Little or none	An individual applies to a Federal agency for an annual park visitor's permit

2	Some	A beneficiary changes her address of record through the Social Security web site
3	High	A patent attorney electronically submits confidential patent information to the US Patent and Trademark Office
4	Very High	A law enforcement official accesses a law enforcement database containing criminal records

OMB M-04-04 does not mention biometrics. It does not identify which technologies should be implemented. Its scope is e-government, including individual user, business, or government entities.

In the OMB document, a credential is defined as an object that is verified when presented to the verifier in an authentication transaction. It also defines Credential Service Providers (CSPs) as those entities that issue electronic credentials.

Although the initial scope is limited to e-government, the security levels defined by M-04-04 are being used beyond just remote e-authentication. For example, The Federal Information Processing Standards (FIPS) 201 *Personal Identity Verification (PIV) of Federal Employees and Contractors*, which provides technical requirements for *Homeland Security Presidential Directive 12*, maps to similar levels.

3.3 NIST SP800-63

NIST Special Publication 800-63 *Electronic Authentication Guideline* was developed in direct response to the previously mentioned OMB M-04-04. SP800-63 interprets the high level requirements of OMB M-04-04 in defining the technical requirements for federal agencies implementing electronic authentication. The recommendations cover remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions.

3.3.1 Statements related to biometrics

Some of the statements in current version 1.0.2 of SP800-63 related to biometrics includes the following:

- "Biometrics are not used directly as tokens in this document."
- "Biometric characteristics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document."
- "This guidance addresses only traditional, widely implemented methods for remote authentication based on secrets."
- "NIST is continuing to study both the topics of knowledge based authentication and biometrics and may issue additional guidance on their uses for remote authentication of individuals across a network."
- "Biometric methods are widely used to authenticate individuals who are physically present at the authentication point, for example at the entry of a building or for accessing a computer."

- "In the local authentication case, where the claimant is observed and uses a capture device controlled by the verifier, authentication does not require that biometrics be kept secret."
- "The use of biometrics to "unlock" conventional authentication tokens and to prevent repudiation of registration is identified in this document."

3.3.2 Characterization of Assurance Levels from NIST SP800-63

In creating the correlation between SP800-63 and OMB M-04-04, requirements for different types of tokens were defined for each of the four (4) assurance levels in OMB M-04-04. Table 3 below shows the token requirements in SP800-63 mapped to OMB M-04-04 assurance levels. It should be noted that levels 1 and 2 require only one factor authentication while level 3 and 4 require two-factor authentication. Under the basic assumption of biometrics consisting of a single authentication mechanism; biometrics alone could only be used at levels 1 and 2 (though not allowed in the current version of SP800-63).

Table 3 - SP800-63 Token Mappings to OMB M-04-04 Assurance Levels

Token type	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

A brief description of the four assurance levels is provided below.

Level 1: Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 1 summary as it relates to biometrics: Assurance Level 1 does not currently allow for the use of biometrics for e-authentication. However, it is likely biometric technologies used alone would be stronger than the necessary security at this level.

Level 2: Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 2 summary as it relates to biometrics: Assurance Level 2 does not currently allow for the use of biometrics for e-authentication. There is a contention that biometrics cannot be considered secrets and therefore there is language in this assurance level that prohibits the sharing of secrets. This limitation can be overcome, however, if there are countermeasures put in place to mitigate the concerns about the sharing of authentication secrets. In particular, through liveness detection at the point of acquisition and the use of approved cryptographic techniques to protect transmission.

Level 3: Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or onetime password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the CSP, however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 3 summary as it relates to biometrics: Assurance Level 3 requires two-factor authentication and specifically calls out the use of biometrics as an option in order for the claimant to prove that he or she controls the token.

Level 4: Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only "hard" cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module, validated at FIPS 140-2 Level 2 or higher overall, with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

Level 4 summary as it relates to biometrics: Assurance Level 4 still requires two-factor authentication and does not prohibit the use of biometrics as an option in order for the claimant to prove that he or she controls the token.

4 References and Terminology

4.1 Reference Documents

- OMB M-04-04, E-Authentication Guidance for Federal Agencies, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
- NIST SP800-63, Electric Authentication Guidelines (v 1.02.2), http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

4.2 Baseline Standards

- ANSI INCITS 358-2002, The BioAPI Specification (Version 1.1), www.bioapi.org
- ANSI INCITS 398-2005/NISTIR 6529-A, Common Biometric Exchange Framework Format (CBEFF), www.nist.gov/biometrics
- ANSI X9.84, Biometric Information Management and Security, www.x9.org
- FIPS 140-2, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, http://csrc.nist.gov/piv-program/index.html
- ISO/IEC 19784-1 :2006, Biometric Application Programming Interface – Part 1: The BioAPI Specification (International Version, 2.0)
- ISO/IEC 19785-1:2006, Common Biometric Exchange Formats Framework (CBEFF) – Part 1: Data Element Specification
- ISO/IEC 19785-2:2006, Common Biometric Exchange Formats Framework (CBEFF) – Part 2: Procedures for the Operation of the Biometrics Registration Authority
- ISO/IEC 19795-1:2006, Information Technology – Biometric Performance Testing and Reporting – Part 1: principles and framework
- ISO/IEC FCD 24708, Biometric Interworking Protocol
    - This standard is being developed by ISOI/IEC JTC 1 SC 37 and ITU-T
- ISO/IEC JTC1 SC37 Standing Document 2, Harmonized Biometric Vocabulary (v7)
    - This standard is being developed by ISOI/IEC JTC 1 SC 37
- ISO 19092-1, Financial Services – Biometrics – Part 1: Security Framework
- NIST SP800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf

4.3 Common Terms

Where possible, the terms and definitions in this document are taken from OMB M-04-04 and NIST SP800-63. Basic biometric terminology is used in accordance with ISO/IEC JTC1 SC37 Standing Document 2 Harmonized Biometric Vocabulary. Alternatively, the ISO/IEC JTC1 SC37 Biometric Vocabulary Corpus available online at: http://www.biotown.purdue.edu/ecorpus/index.asp.

The following terms and definitions are inherited directly from NIST SP800-63 and used accordingly in this document:

- *Remote authentication mechanisms*: Combination of credentials, tokens, and authentication protocols
- *Credentials:* An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. The credential is presented to the verifier in an authentication transaction.
- *Credential Service Provider:* An entity that issues electronic credentials.
- *Electronic authentication (e-authentication):* The process of establishing confidence in user identities electronically presented to an information system.
- *Remote e-authentication:* Establishing identity over an open network such as the Internet

4.3.1 Biometrics

The definition of *biometrics* found in Section 4 of NIST SP800-63

> *Biometric*: "An image or template of a physiological attribute (e.g., a fingerprint) that may be used to identify an individual."

is not used in this document because it is not a broadly-accepted definition and because it contains inaccuracies. Instead, the ISO/IEC JTC1 SC37 Standing Document 2 definition is used:

> *Biometrics*: "Automated recognition of individuals based on their behavioural and biological characteristics"
>
> *Biometric:* "Of or having to do with biometrics"

Definitions of *biometrics* have encompassed the behavioral element of biometrics as far back 1987 when the first accredited ANSI Biometric Terminology standard defined it in manner similar to the definition provided above from Standing Document 2. The fact that the SP800-63 definition fails to acknowledge the behavioral element of biometrics is one of its failings.

> A *behavioral* aspect of a biometric measures data pertaining to a personal trait, learned over time, or to a learned action.

This document discusses biometric modalities with both behavioral and biological aspects. Biometrics with stronger behavioral aspects (e.g., keystroke, sign/signature, voice) utilize acoustics, pressure, and speed whereas those with stronger biological aspects (e.g., fingerprint, iris, hand geometry, vein) measure characteristics residing on or near the surface of the human body. Both behavioral and biological biometrics can be classified as "dynamic" if they include a temporal component. A more detailed description of content-bearing and dynamic biometrics is presented in Section 5.6.

4.3.2 Biometric Data

Biometric characteristics are represented as forms of biometric data. A distinction is made between the following:

> *Template*: Data collected during enrollment and stored as a reference for future matching. (Newer biometric vocabulary prefers the term "biometric reference data/sample".)
>
> *Sample*: "Live" data collected during authentication for immediate matching against the reference template. (Newer biometric vocabulary prefers the term "biometric recognition data/sample".)

[See Section 5.3.5 for further discussion of biometric data.]

4.3.3 Tokens

The definition of *tokens* found in Section 4 of NIST SP800-63

> *Token*: "Something that the claimant possess and controls (typically a key or password) used to authenticate the claimant's identity."

is not used in this document because it does not distinguish between physical and logical entities.

Instead, another commonly referred definition of tokens is used:

> *Token:* "Is a physical object controlled by the user such as a smart card."

This definition focuses on the common acceptance that tokens are something that is physically tangible. Passwords, as in the SP800-63 definition, are believed to be better classified as a secret and not a token.

4.3.4 Accuracy

4.3.4.1 False Match

The definition of *false match* found in *ISO/IEC JTC1 SC37 Standing Document 2 Harmonized Biometric Vocabulary*:

False match: "(A) matching decision of match for a presented biometric sample and a biometric reference that are not from the same source."

4.3.4.2 False Match Rate (FMR)

Currently, *ISO/IEC JTC1 SC37 Standing Document 2 Harmonized Biometric Vocabulary* does not contain a definition for *false match rate*. However; ISO/IEC 19795-1 Information Technology – Biometric Performance Testing and Reporting – Part 1: principles and framework defines the *false match rate* as "(A) proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template"

4.3.4.3 False Non-Match

The definition of *false non- match* found in *ISO/IEC JTC1 SC37 Standing Document 2 Harmonized Biometric Vocabulary*:

False non-match: "(A) matching decision of non-match for a presented biometric sample and a biometric reference that are from the same source."

4.3.4.4 False Non Match Rate (FNMR)

Currently, *ISO/IEC JTC1 SC37 Standing Document 2 Harmonized Biometric Vocabulary* does not contain a definition for *false non-match rate*. However; ISO/IEC 19795-1 Information Technology – Biometric Performance Testing and Reporting – Part 1: principles and framework defines the *false non-match rate* as "(A) proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample"

4.4 Acronyms and Abbreviations

AES	Advanced Encryption Standard
AHGBEA	Ad Hoc Group on Biometrics in E-Authentication
ANSI	American National Standards Institute
API	Application Program(ming) Interface
ASN	Abstract Syntax Notation
ATM	Automated Teller Machine
BIR	Biometric Information (Identification) Record
BSP	Biometric Service Provider
CA	Certificate Authority
CAPI	Cryptographic API
CBEFF	Common Biometric Exchange Formats Framework
cert	(digital) certificate
CRL	Certificate (or Credential) Revocation List
CSP	Credential Service Provider or Cryptographic Service Provider
DES	Data Encryption Standard
DLL	Dynamic(ally) Linked Library
DOS	Denial of Service
DNA	Deoxyribonucleic acid
FAR	False Accept(ance) Rate
FNMR	False Non-Match Rate
FMR	False Match Rate
FRR	False Reject(ion) Rate
FTE	Failure to Enroll
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HR	Human Resources
HSM	Hardware Security Module
HSPD	Homeland Security Presidential Directive
ID	Identity/Identifier
INCITS	International Committee for Information Technology Standards
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OEM	Original Equipment Manufacturer

OMB	(US) Office of Management and Budget
PC	Personal Computer
PCMCIA	PC Memory Card International Association
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PoP	Proof of Possession
RA	Registration Authority
RF	Radio Frequency
SIV	Speaker Identification and Verification
SOF	Strength of Function
SSN	Social Security Number
SSO	Single Sign-On
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTL	Time to Live
USB	Universal Serial Bus
UUID	Universally Unique Identifier
VPN	Virtual Private Network
VXML	Voice XML
XML	eXtensible Markup Language

5 Authentication Principles and Biometrics

5.1 Conventional Authentication Mechanisms

Currently, there are three common methods to achieve personal authentication:

- Something you know, normally a password.
- Something you have, normally a physical token.
- Something you are, formally known as biometrics.

Although all three of these methods can be used to achieve the same goal of secure authentication, the ways in which the methods maintain and reach this goal are very different. The first two methods of authentication listed above rely on a secretive element – i.e., the knowledge of the password, or the controlled possession of the physical token.

Biometrics is unique from the other two in that the characteristic being used for authentication is typically not considered a secret. This presents issues when trying to provide secure and accurate authentication over open networks primarily because the biometric characteristic by itself does not provide a complete solution as shown above in NIST SP800-63.

Another mechanism which is not normally under the direct control of the user is cryptographic module. FIPS 140-2 defines a cryptographic module as "the set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary."

Each authentication method has strengths and weakness. Table 4 below summarizes at a very high level some of the relative strengths (blue) and weakness (pink) for four method categories against nine areas of comparison [1].

> NOTE: With the permission of the original author, the descriptions in the table have been modified slightly to align with the purpose of the report. This is obviously not a rigorous analysis, but is provided only as a relative view and to identify some of the considerations in assessing the utility of an authentication metho3d.

Table 4 - Authentication Mechanisms Cross-Comparison

	Knowledge	Tokens	Biometric	Cryptographic
Entropy	low	low/medium	medium/high	high
Memory	forgetfulness	forgetfulness	cannot forget	secret
Discovery	smart guessing	counterfeit	faked	exhaustion
Manipulation	social engineering	social engineering	difficult	collusion
Usage	ubiquitous	commonplace	fairly common	unknown
Reliability	reliable	reliable	improving	reliable
Cost	cheap	costly	lowering	costly
Ergonomics	familiar	difficult	easy to use	complicated
Manageability	reset passwords	issuance	enrollment	subscription

- *Entropy* refers to the relative strength of function associated with the method (i.e., its resistance to a brute force attack).
- *Memory* addresses the reliance of the method on human memory capacity.
- *Discovery* is an indication of the ease at which the method is vulnerable to guessing or spoofing.
- *Manipulation* identifies the degree to which the mechanism is sharable and thus subject to social attack.
- *Usage* indicates how available, acceptable, and prevalent (proven) he technology is.
- *Reliability* refers to both the consistency with which the method performs as well as to the reliability of the components utilized in the method.
- *Cost* includes both procurement (hardware/software) and operating & maintenance (O&M)/lifecycle costs.
- *Ergonomics* relates to the ease of use of the method.
- *Manageability* addresses the administrative burdens incurred by use of the technology.

The prevailing techniques of user authentication involve the use of either user IDs (identifiers) and passwords or identification cards and PINs (personal identification numbers). Both of these two scenarios contain a secretive component which the user must enter into the authentication system. Passwords and PINs can be acquired by direct covert observation. Once an attacker acquires the user ID and the password, they have total access to the user's resources. In addition, there is no way to positively link the usage of the system or service to the actual user; that is, there is no protection against repudiation by the user ID owner. For example, when a user ID and password is shared with a colleague, there is no way for the system to know who the actual physical user is. A similar situation arises when a transaction involving a credit card number is conducted on the internet. Even though the data is sent over the internet using secure encryption methods, the systems are not capable of assuring that the transaction was initiated by the rightful owner of the credit card. In the modern distributed systems environment, the traditional

authentication policy based on a simple combination of user ID and password has become inadequate.

The reason why passwords, and secret or knowledge based authentication in general, are directly referred to and compared to in this report is because it is arguably the weakest link in current computer access control systems for the reasons described above. The use of biometrics to replace the password, particularly in the remote e-authentication environment, addresses these concerns.

Fortunately, biometrics in general can provide a much more accurate and reliable user authentication method. Biometrics is a rapidly advancing field that is concerned with electronically identifying a person based on his or her physiological or behavioral characteristics. Common examples of automated biometrics include fingerprint recognition, face recognition, iris recognition, voice recognition, and hand geometry. Because a biometric property is an intrinsic feature of an individual, it is difficult to duplicate and nearly impossible to share.

Biometric data, which range from several hundred bytes to over a megabyte, have the advantage that their information content is usually higher than that of a password or a pass phrase. Simply extending the length of passwords to get equivalent bit strength presents significant usability problems. Fortunately, biometrics can provide the security advantages of long passwords while retaining the speed and characteristic simplicity of short passwords.

Even though biometrics can help alleviate the problems associated with the existing methods of user authentication, there still are weak points in the system vulnerable to attack. Password systems are prone to brute force dictionary attacks. Biometric systems, on the other hand, require substantially more effort for mounting such an attack. Yet there are several new types of attacks possible in the biometrics domain. Many of these may not apply if biometrics is used as a supervised authentication tool. But in the remote unattended environment, imposters may have the opportunity to make several attempts, or even physically violate the integrity of a remote client, before detection. This document is intended to discuss these vulnerable points and make suggestions on how to take advantage of biometrics while alleviating inherent problems.

5.2 Authentication Models

SP800-63 defines the traditional e-authentication model, which involves two processes – registration and authentication. During registration:

> "An *applicant* applies to a *Registration Authority (RA)* to become a *subscriber* of a *Credential Service Provider (CSP)* and, as a subscriber, is issued or registers a secret, called a *token*, and a *credential* that binds the token to a name and possibly other attributes that the RA has verified. The token and credential may be used in subsequent authentication events." [SP800-63]

During authentication, when the party to be authenticated (called a *claimant*) successfully demonstrates possession and control of a token to a *verifier* (the party verifying the identity) through an on-line *authentication protocol*, the verifier can verify that the clamant is the

subscriber. The verifier passes on an assertion about the identity of the subscriber to the relying party. The relying party can use the authenticated information provided by the verifier/CSP to make access control or authorization decisions.

Some features of this model:

- Tokens are always secrets and it is the responsibility of the subscriber to protect them.
- It is undesirable for verifiers to learn shared secrets unless they are a part of the same entity as the CSP that registered the tokens.

Figure 1 and Figure 2 depict e-authentication using the traditional process:

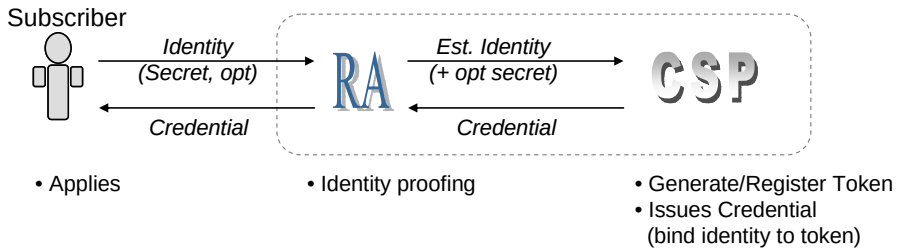

Figure 1 - Traditional Registration Process

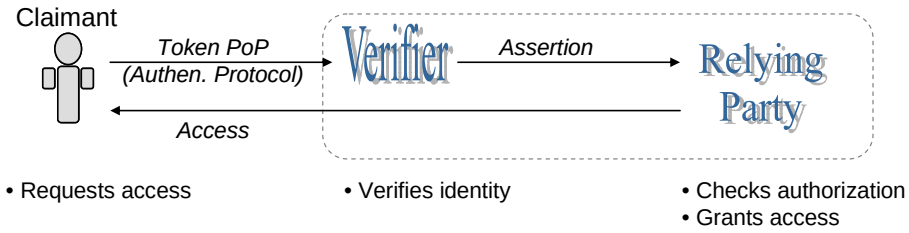

Figure 2 - Traditional Authentication & Authorization Process

In a biometric authentication model, during registration the applicant/subscriber enrolls (provides) their biometric data to the RA/CSP. The biometric reference data in this case is analogous to an authentication token except that:

a) It is not a secret known by the subscriber or a secret generated by the CSP – it is an inherent characteristic of the subscriber (though it may also incorporate knowledge-based content, see 5.5 below).
b) The reference biometric is bound to the identity by the CSP. The resulting credential (unless it is instantiated within a physical token) does not need to be issued to the subscriber since he retains the source of the biometric data (himself).

As a result, during authentication, the claimant presents a new biometric sample to the verifier, to be compared with that originally registered and incorporated into the credential.

a) For server-based matching:
    1. This requires that the verifier have knowledge of the registered biometric (credential) OR that a separate biometric authentication service be used. (The verifier would still handle the incoming live biometric sample; thus, if encrypted, keys would need to be shared with the biometric server.) It is noted that the verifier and the biometric authentication server may be the same entity.

2. A method to register the reference biometrics with the biometric server would be required (i.e., a relationship with the CSP is implied).

b) For local matching (e.g., on a physical token):
   1. The live sample is matched against the biometric credential stored locally, releasing a separate token for use in the traditional authentication protocol.

The biometric authentication model is shown in Figure 3 and Figure 4.

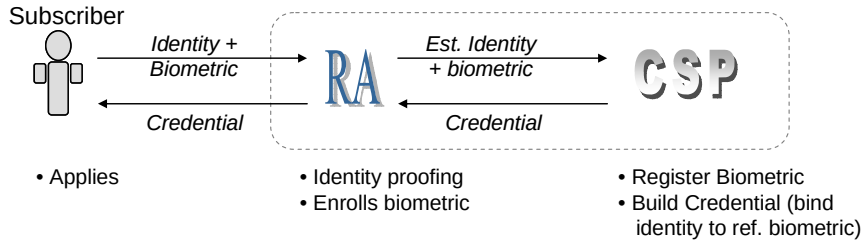

Figure 3 - Biometric Registration Process

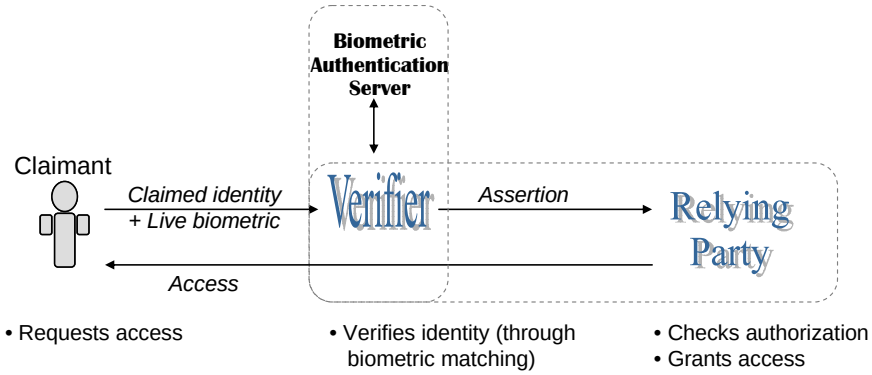

Figure 4 - Biometric Authentication Process (Server Based)

The main difference in these two models is that instead of proving possession of a CSP issued credential, the claimant proves he can present a biometric sample from the same source as that originally registered. The authentication protocol is therefore not engineered to verify proof of possession (PoP), but to ensure the integrity and authenticity of the live sample and to verify that it matches the registered biometric credential.

This is in some ways "backwards" from the traditional model in that:

- The biometric "token" is provided by the subscriber to the CSP rather than issued by the CSP to the subscriber.
- It is not the credential (issued token) that is provided for verification, but the credential that the provided biometric is verified against.

This is not to imply that either method is "better" than the other, but to highlight the fact that there are inherent differences in the technology that in turn drive differences in the associated authentication models and protocols. These differences are best recognized and accommodated (to ensure an effective and secure implementation) rather than attempting to either evaluate or employ biometric authentication by force fitting it into the traditional paradigm.

In summary, biometric authentication differs from the standard model in that:

- Biometric enrollment must occur during registration and results in the applicant providing the biometric to the RA/CSP.
- During authentication, it is a newly captured biometric sample that is compared to the registered biometric reference to verify identity. The claimant does not present the registered token/credential per se, but a biometric sample from the same source as that registered.
- For server-based matching, this requires that the verifier have knowledge of the registered biometric (credential).
- For non-server-based matching, this requires that a different token be sent to the verifier (or used to participate in an authentication protocol). This token may be bound to the same credential as the biometric or the biometric verification may be used to unlock the token from another binding.

5.3 Biometric Systems

5.3.1 Conceptual Diagrams

For purposes of consistency and demonstration, two documents are referenced as they relate to conceptual informational diagrams of biometric systems. ANSI X9.84-2003, *Biometric Information Management and Security for the Financial Services Industry*, provides a generalized biometric system model shown below in
Figure 5.

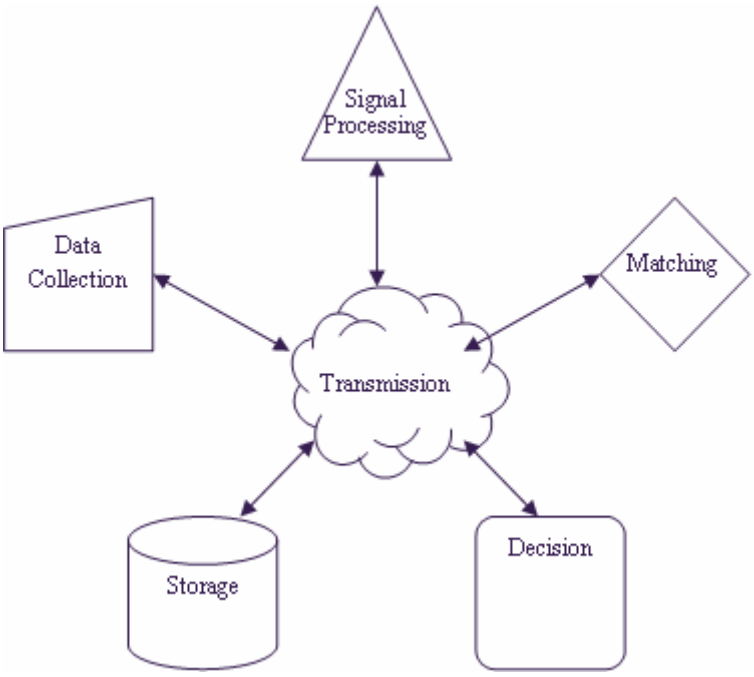

Figure 5 - ANSI X9.84-2003 Generalized Biometric Model

A more detailed reference model for a biometric system has been developed by ISO/IEC JTC1 SC37 as Standing Document 11, which is useful in describing the components, structure, and

general process flow of a biometric system. The Conceptual Diagram is provided below in Figure 6 for context.

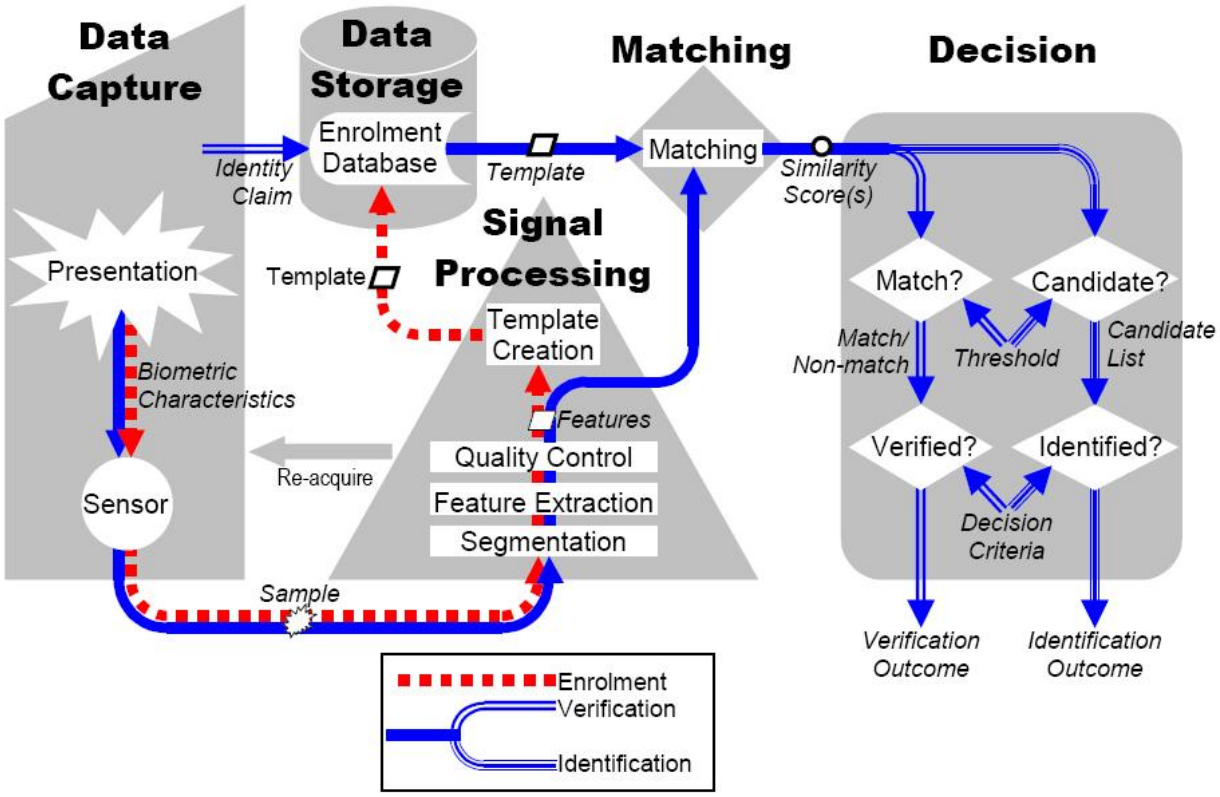

Figure 6 - ISO/IEC JTC1 SC37 SD11 Concept Diagram

NOTE: The above figure uses the term "template" generically. See Section 5.3.5 for a more detailed explanation regarding this terminology.

5.3.2 Biometric Subsystems

The following subsections describe each of these subsystems in more detail. It should be noted that, in any real biometric system, these conceptual components may not exist or may not directly correspond to the physical components.

Data capture subsystem: The data capture subsystem collects an image or signal of a subject's biometric characteristics that they have presented to the biometric sensor, and outputs this image/signal as a biometric sample.

Transmission subsystem: The transmission subsystem (not always present or visibly present in a biometric system) will transmit samples, features, and/or templates between different subsystems. Samples, features or templates may be transmitted using standard biometric data interchange formats. The biometric sample may be compressed and/or encrypted before transmission, and expanded and/or decrypted before use. A biometric sample may be altered in transmission due to noise in the transmission channel as well as losses in the

compression/expansion process. It is advisable that cryptographic techniques be used to protect the authenticity, integrity, and confidentiality of stored and transmitted biometric data.

Signal processing subsystem. The signal processing subsystem extracts the distinguishing features from a biometric sample. This may involve locating the signal of the subject's biometric characteristics within the received sample (a process known as segmentation), feature extraction, and quality control to ensure that the extracted features are likely to be distinguishing and repeatable. Should quality control reject the received sample/s, control may return to the data capture subsystem to collect a further sample/s.

In the case of enrollment, the signal processing subsystem creates a (reference) template from the extracted biometric features. Often the enrollment process requires features from several presentations of the individual's biometric characteristics. Sometimes the template comprises just the features.

Data storage subsystem. Templates (references) are stored within an enrollment database held in the data storage subsystem. Each template is associated with details of the enrolled subject. It should be noted that prior to being stored in the enrollment database, templates may be re-formatted into a biometric data interchange format and/or packaged as a BIR. Templates may be stored within a biometric capture device, on a portable medium such as a smart card, locally such as on a personal computer, in a local server, or in a central database.

Matching subsystem. In the matching subsystem, the features extracted from the captured biometric image are compared against one or more enrollment templates and similarity scores are passed to the decision subsystem. The similarity scores indicate the degree of fit between the features and template/s compared. In some cases, the features may take the same form as the stored template. For verification, a single specific claim of subject enrollment would lead to a single similarity score. For identification, many or all templates may be compared with the features, and output a similarity score for each comparison. Where the comparison occurs can affect the risks of attack and system manageability.

Decision subsystem. The decision subsystem uses the similarity scores generated from one or more attempts to provide the decision outcome for a verification or identification transaction. In the case of verification, the features are considered to match a compared template when the similarity score exceeds a specified threshold. A claim about the subject's enrollment can then be verified on the basis of the decision policy, which may allow or require multiple attempts. In the case of identification, the enrollee identifier or template is a potential candidate for the subject when the similarity score exceeds a specified threshold, and/or when the similarity score is among the highest k values generated for a specified value k. The decision policy may allow or require multiple attempts before making an identification decision.

Template-adaptation subsystem. The template-adaptation subsystem modifies a template using new data gathered from a successful verification or identification. Adaptation is generally employed by biometric systems to counteract factors external to the user, such as differences in telephone device/channel attributes, background noise. It may also be used for other purposes, such as to perform incremental enrollment or to attenuate the potential effects of template aging.

Unsupervised adaptation is performed automatically on a pre-determined schedule, such as after every verification/identification or on every 3rd verification/identification and generally requires a high matching determination. Supervised adaptation is usually invoked by the application and is based on application-specific criteria. For example, it may be called when the biometric matching score is not high but other factors clearly support the claimed identity.

> NOTE: Conceptually, it is possible to treat multi-biometric systems in the same manner as uni-biometric systems, by treating the combined biometric *samples/templates/scores* as if they were a single *sample/template/score* and allowing the decision subsystem to operate score fusion or decision fusion as and if appropriate.

Administration subsystem (Not portrayed in diagram). The administration subsystem governs the overall policy, implementation and usage of the biometric system, in accordance with the relevant legal, jurisdictional and societal constraints and requirements. Illustrative examples include:

- providing feedback to the subject during and/or after data capture;
- requesting additional information from the subject;
- storage and format of the biometric templates and/or biometric interchange data;
- provide final arbitration on output from decision and/or scores;
- set threshold values;
- set biometric system acquisition settings;
- control the operational environment and non-biometric data storage;
- provide appropriate safeguards for end-user privacy;
- interact with the application that utilizes the biometric system.

Interface (Not portrayed in diagram). The biometric system may or may not interface to an external application

5.3.3 Biometric Functions

Functional lifecycles (process) models for enrollment and verification are shown below in Figure 7 and Figure 8. These, particularly the verification diagram, form the basis of the architecture and threat modeling discussions which follow in Section 8.

- **Biometric Enrollment**. *The process of collecting a biometric sample(s) from an individual, and the subsequent construction and storage of a reference template(s) and associated data representing the individual's identity.*
    - Considerations: In enrollment, a transaction by a subject is processed by the system in order to generate and store an enrollment record for that individual. The enrollment record will consist of the biometric reference (a stored sample, template or model) for the individual and perhaps other information, such as a name. At the time of enrollment, the veracity of this other information must be ascertained from external source documentation, such as birth certificates, passports or other trusted documents. The use of biometrics does not obviate the need for care in ascertaining the validity of these documents at the time of enrollment.
    - Biometric enrollment almost always involves a face-to-face meeting (i.e., it is not a process which is normally executed remotely), so that the enrollment biometric

data capture can be witnessed and so that the external source documentation that establishes a claimed identity can be checked by a human. A remote biometric enrollment is possible, with the resulting decrease in the level of trust of the binding of the claimed identity to the biometric data. Section 7 of NIST Special Publication 800-63, Electronic Authentication Guideline describes a registration and identity proofing process. The identity proofing process during a biometric enrollment is quite similar to the described registration process although the in-person versus remote identity proofing requirements described in Section 7.2 of NIST Special Publication 800-63 will differ because of the importance of a witnessed biometric capture.

- Enrollment is the first process of any biometric system and also where the reference template is created. In order for the template to have any value for later use, it must be associated with some sort of identifier. This places great emphasis on properly authenticating the user being enrolled before the introduction of biometrics. Furthermore, the person administering the enrollment of the new user must be properly authenticated and also authorized to enroll others into the system. If these steps are not closely adhered to, a bad seed can be planted causing future problems. An optional step to perform an identification search of the enrollment database may be performed to ensure that the person is not already enrolled in the system (duplication check).

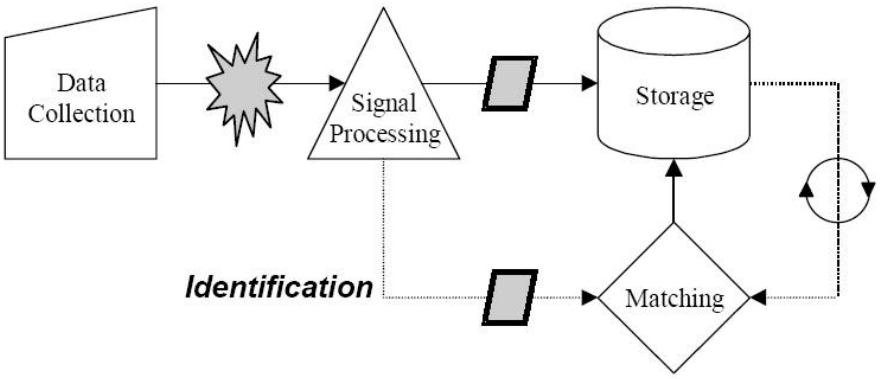

Figure 7 - Enrollment Process Model

- **Biometric Verification**. *A one-to-one comparison of an individual's biometric sample with a single biometric reference template in order to validate an explicit positive claim of identity.*
  - Considerations: Verification (the process most often used in biometric authentication) involves the capture of a sample, the processing of that sample for matching, retrieval of the corresponding reference template from the enrollment database (based on a claimed identity), the matching of the processed live sample (recognition data) against the enrolled template, and making a decision regarding the results of that match which is provided to an application (or relying party). Optionally, if the verification is successful, the new sample may be used to update the enrollment data for that individual (a process known as adaptation).
    When addressing the remote nature of the environment, it is important to note the lack of supervision for both genuine and imposter users. Attackers are much

more able to set up hill climbing, replay type or spoofing attack with decreased physical monitoring of their behavior. It is important to not provide detailed feedback relating to the authentication attempt. Rather, incremental feedback should be used to prevent against these attacks. This capability exists in the BioAPI framework, but currently is not mandatory.

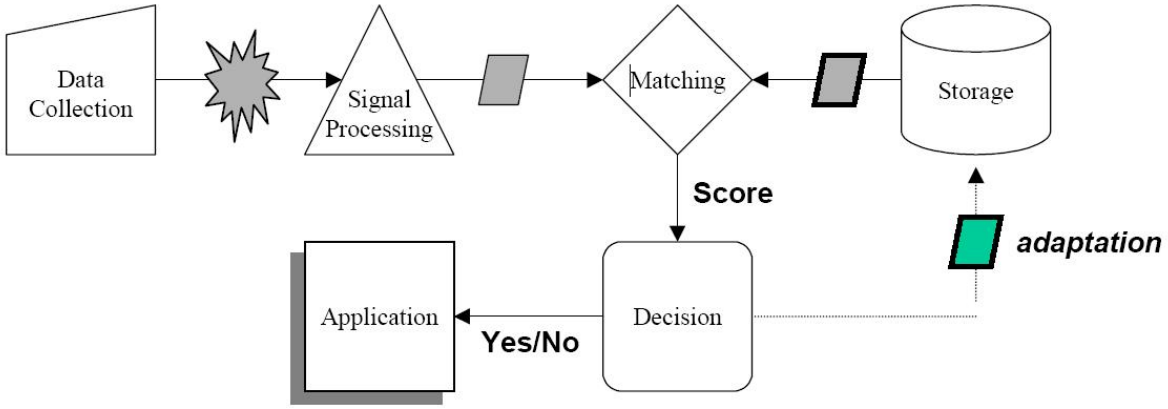

Figure 8 - Verification Process Model

- **Biometric Identification**. *The one-to-many process of comparing a submitted biometric sample against all or a specified subset of the biometric reference templates on file to determine whether it matches any of the stored templates and, if so, the identity of the enrollee whose template was matched.*
    - Considerations: Simply using biometrics to identify someone is only using one form of authentication; therefore this factor alone wouldn't allow level three and four to be obtained in compliance with the NIST document. Although identification-based authentication may have limited use in applications requiring a claimed identity and/or multiple authentication factors, it offers some capabilities that are uniquely valuable in some situations. As part of the enrollment process, an identification search can be performed to determine whether an enrollment already exists for the applicant in the database. This eliminates duplicate enrollments and can prevent the establishment of fraudulent identities. Small-set identification (sometimes referred to as "one-to-few") is used when a small number of individuals have the same identifier. For example, banks often use account number as the identifier/identity claim even for jointly-owned accounts. Consequently, small set identification would examine the biometric templates of the set of owners for that account. Identification also offers an opportunity for "anonymous authentication" in applications where the mere existence of an enrollment in the database (or designated subset of the database) confers a privilege or benefit, without the need to record any personal identifying information. The authentication system need only confirm that the person is in the database or database subset in order to authorize the privilege associated with enrollment. Finally, identification is essential in "watch list" applications. Here the presence of an enrollment record in the database indicates the individual is "of interest" due to previous activity, or perhaps is to be denied some benefit because it has already been received at the time of enrollment.

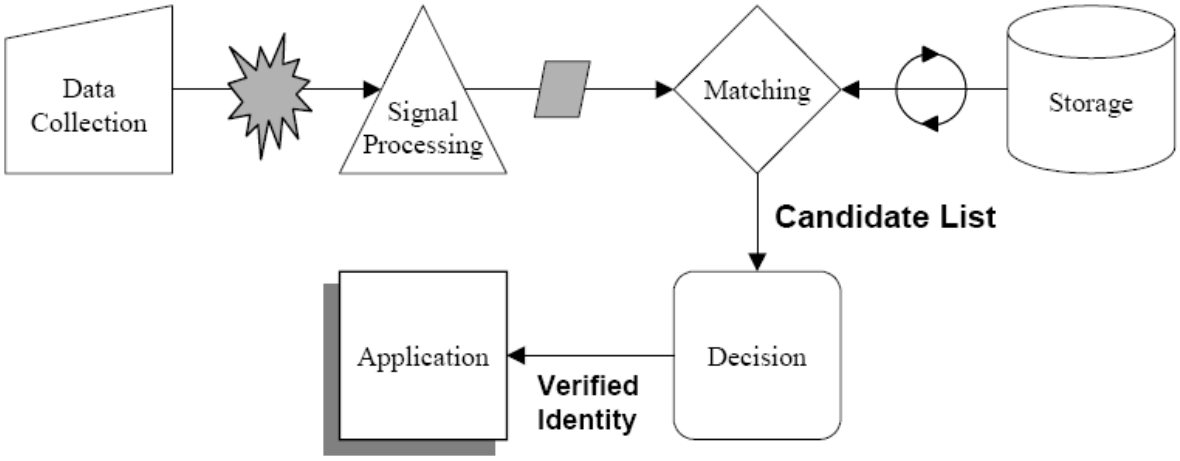

Figure 9 - Identification Process Model

5.3.4 Biometric Algorithms

At the heart of a biometric system is a comparison function (*biometric algorithm*). There are primarily two types of biometric algorithms, as described below. Prior to the usage of these algorithms, it is essential that the data collection system capture high quality biometric data samples for processing by the biometric algorithms.

- Feature extraction (template generation) algorithms
  - The first function of the algorithm is the processing or feature extraction of the sample presented to the system. Template generation then takes place where a digital representation of one's biometric is created and stored for matching purposes in the future.
- Matching algorithms
  - The second function of the algorithm is matching (or comparison). In this process an estimation, calculation or measurement of similarity or dissimilarity between a biometric sample(s) and a biometric reference(s) is (are) made. This comparison process and the subsequent provision of the result of the comparison are the main functions that biometric algorithms provide.
  - Considerations: It is clear that a biometric algorithm on its own does not provide assurance that:
    - The biometric sample was properly captured by the biometric system (in other words, the algorithm cannot guarantee the quality, the liveness or other properties of the biometric sample);
    - The biometric reference has not been modified or tampered with;
    - The biometric reference is properly linked with the system identifier by which the individual is known to the system.

5.3.5 Biometric Data

Biometric data can be stored and/or transmitted alone or encapsulated in a data structure that contains metadata about the biometric data (e.g., BIR). The diagram in Figure 2 and the following clauses use the word "template" as a generic term representing any form of biometric

data including "processed" or “encapsulated" data. There are several categories and representations of biometric data within a biometric system. Some characterizations are as follow:

5.3.5.1 Processing level

Biometric data exists in various forms as it evolves from the initial capture through storage and matching. Three levels have been defined as follows:

- *Captured biometric sample (raw) data*. This data is as acquired by the biometric sensor, prior to any processing. Examples include digital images (e.g., of an iris, face, or fingerprint) or a digitized audio waveform.
- *Intermediate data*. Biometric data that has been partially processed, but is not yet suitable for matching.
- *Processed data*. Biometric data which has been fully processed (e.g., via feature extraction) and is suitable for matching.

5.3.5.2 Purpose

Biometric data is generally collected for a specific purpose, related to the functions described in Section 5.3.3:

- *Reference data*. Data collected during enrollment and stored as the reference for subsequent matching.
- *Recognition data*. “Live” data collected during an authentication operation, intended for immediate matching against reference data.

The term “template” is sometimes use to refer to any fully processed data, but is usually used to refer to reference data. When used in this report, the latter meaning is intended. Strictly speaking, a biometric “sample” refers to any biometric data; however, when used in this report, it generally refers to recognition data.

5.3.5.3 Encapsulation

Biometric data is usually formatted with metadata describing it. Standard data formats exist for each major biometric modality which describes the content and structure of this data. *Common Biometric Exchange Formats Framework* (CBEFF) standards ISO 19785-1:2006 and INCITS 398:2005 promote interoperability of biometric-based applications and systems by specifying standard structures for *biometric information records* (BIRs) and a set of abstract data elements and values that can be used to create the header part of a CBEFF-compliant BIR. A biometric information record (BIR) is an encoding in accordance with a CBEFF patron format (below). It is a unit of biometric data for storage in a database or for interchange between systems or parts of systems. A BIR always has at least two parts: a standard biometric header (SBH) and at least one biometric data block (BDB). It may also have a third part called the security block (SB). CBEFF places no requirements on the content and encoding of a BDB except that its length shall be an integral number of octets; the several parts of ISO/IEC 19794 and INCITS biometric data interchange format standards specify standardized BDB formats for a number of biometric types. In addition to providing the means for identification of the formats of the BDBs, some of the required or optional data elements contained in the CBEFF Header as well as allowing for the existence of a Security/Signature Block provide features that can be used to support biometrics

and e-authentication (requirements such as time stamp, creator of the biometric data, validity period and whether the data is encrypted or signed) are features specified in the CBEFF BIR header A CBEFF patron format is a full bit-level specification of encodings that can carry some or all of the abstract values of some or all of the CBEFF data elements defined in the CBEFF standards (possibly with additional abstract values determined by the CBEFF patron), together with one or more biometric data blocks (BDBs) containing biometric data. The BioAPI standards ISO 19784-1:2006 and INCITS 358-2002 define instantiations of the CBEFF BIRs. Both BioAPI BIRs include the mandatory data elements specified in the CBEFF BIRS but they are not exactly the same (the international version of the BioAPI BIR includes some data elements not specified in the national version of BioAPI (e.g., Creation Date and Validity Period). The X9.84 standards and its international equivalent 19092 include specification of CBEFF BIRs. Implementers are encouraged to examine in detail these standards and the CBEFFs standards. Specific features of these BIRs in support of e-authentication with biometrics will be referred to in other clauses of this report.

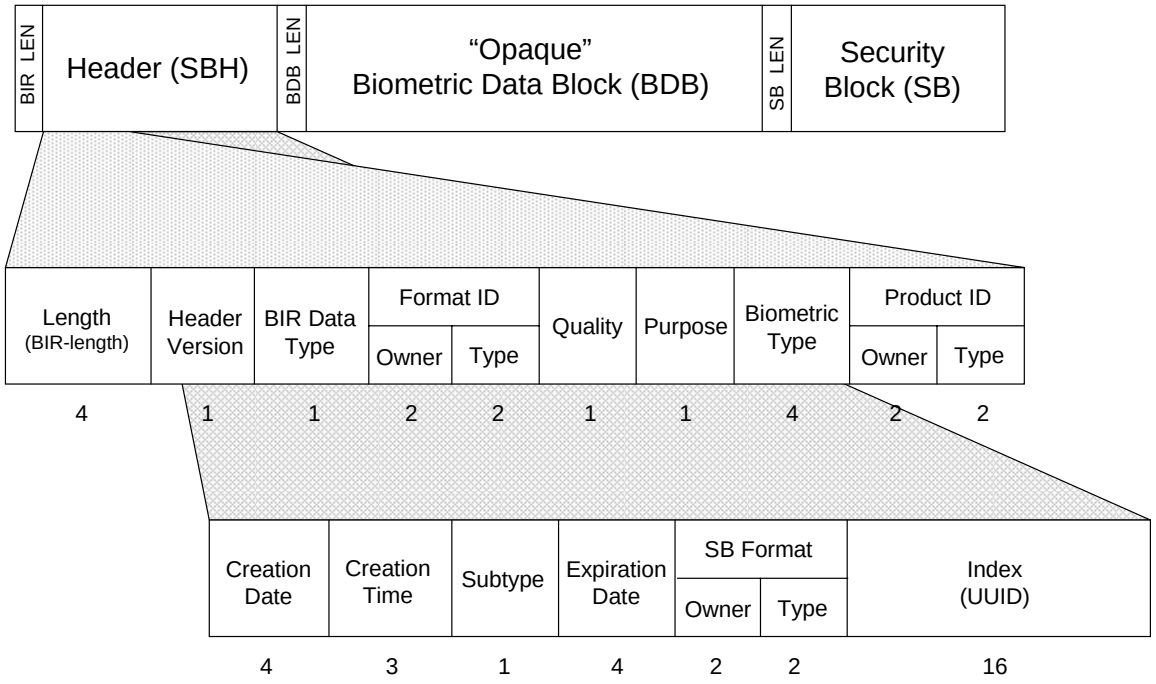

Figure 10 - Biometric Identification Record (BIR) Structure

NOTE: Reference to different types of biometric data in this report, except where noted, does not imply its format or packaging (i.e., does not imply the lack of BIR packaging.)

The topic of biometric data is critical to any discussion of biometric authentication. Each function and component within a biometric architecture/system creates or acts upon this data. Therefore, the use and protection of this data is addressed throughout this report.

5.3.6 Biometrics and authorization

As stated above, a biometric system's role in an overall security system is simply to validate that the biometric sample matches a previously acquired sample, and to output the match result to the

security system. The biometric system cannot and does not assess the rights and privileges of the user. The rights and privileges of the user are associated with an identifier by which the user is known to the security system. Therefore, even though the biometric system may provide a match result, this does not presume that the security system will afford the user any rights or privileges. As such, any revocation of rights and privileges will occur at the security system level. Figure 11 below presents the interaction between the biometric system and the security system.

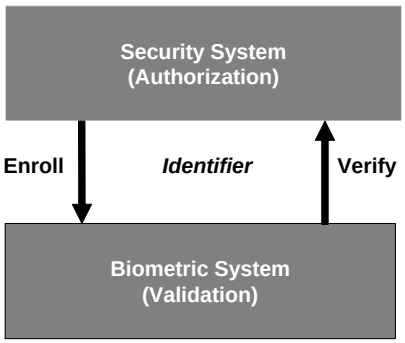

Figure 11 - Biometric and Security System Relationship

5.3.7 Secure Biometric System

An ideal biometric system should also integrate solutions to insure the three common security principles of Confidentiality, Integrity and Availability within the entire biometric transaction and lifecycle by:

- Prevent biometric sensor attacks;
- Prevent digital biometric sample modification and/or injection attacks;
- Provide mutual authentication between all connected system components;
- Insure the authenticity of the critical data elements in the system.
- Liveness detection: to ensure a living biometric sample is introduced at the point of biometric sample acquisition;
- Restriction of access to the input/output of the biometric algorithm to prevent injecting digital biometric samples at a system point behind the biometric capture device (in other words tampering with the matching algorithm results or substituting one reference template for another);
- For verification systems: restrictions on the number of live biometric samples able to be submitted for a comparison against a single biometric reference at one time (in other words, place restrictions on the number of failures to verify before the user must either re-begin the process or talk to an administrator to reset the ability to attempt verification against the biometric reference);
- Mutual authentication between the biometric system components (i.e., biometric capture device, matching server or engine software, etc): to ensure all components receiving or passing data are authorized to do so;

In following all of these protocols, it is clear that biometrics is only a part of the overall security system. A detailed discussion of vulnerability, threats and countermeasures is contained in Section 8.

5.4 Biometric Authentication Principles

5.4.1 Human issues

Knowledge based authentication is affected by a major issue in its real world applications as well, which is the relative ease of guessing or discovering other people's passwords when they are chosen and managed by their owners using average human abilities. This issue has more to do with real-life constraints (such as people's limited ability to invent and remember many complicated passwords) than with cryptographic algorithms and protocols, and its importance is often underestimated when comparing biometrics to passwords and cryptography.

In today's applications of password-based authentication, people are often requested to create tens of passwords for use with many different services, and are asked (as security rules of thumb) to make those passwords hard to guess, make them all different, change them frequently, not reuse them, not write them down in places where they can be seen or found by others, and remember them all. However, most people are unable to do all these things well and tend to give up on one or more of them. The higher the number of different services that require a password to be created and managed by a user of the service, the harder it will be for an individual to follow the security rules of thumb mentioned above. This issue can be described as an issue of scalability in the dimension of multiple services used by a given individual, which is that the degree of identity assurance provided by password-based authentication to decrease, on average, as the number of services increases. Some Single Sign-On (SSO) systems attempt to lessen these issues; however, by using one password to unlock many different applications, the potential damage from a successful password attack is significantly increased, so this effect should be carefully considered when deploying these systems with a single form of authentication.

Biometric authentication (in general) does not suffer from this scalability issue because it does not depend on secrecy of credentials, and thus the same credential can be used with multiple services with no degradation of the identity assurance.

5.4.2 Assumptions

One of the assumptions of password-based authentication ("secrecy") is that you are the only person who knows your password. Password-based authentication does not work if the assumption of secrecy does not hold, or ceases to hold for any reason. Secrecy is a technical requirement of this authentication technology, not a privacy-related requirement. In password-based authentication, knowledge of the credential is what ties the credential to its owner. If someone else (human or machine) gets to know your password, then they can also become associated with that password, and use that credential in place of the intended user.

In contrast, in biometric authentication there is no assumption (in general) that the subject is the only person who knows their biometric characteristic. (Actually, they may not know it at all - most people would not be able, for example, to visually recognize their own fingerprints or irises.) It is certainly possible to use biometrics as an authentication technology even with those biometric characteristics that are very easy to "steal" and share (such as fingerprints, voice, and face), which indicates that there is no assumption of secrecy in biometric authentication in general. In biometric authentication, the link between the credential and its owner is either entirely physical, or a combination of a physical component and a “secret” or "knowledge"

component. In both cases, the credential (biometric characteristic) is subject to measurement, and is actually measured in each authentication operation.

There are some biometric modalities that can associate (or embed) subject-managed information with (or within) a biometric sample, exploiting a subject's ability to generate such information at will, replay it at will under controlled circumstances, and keep it secret at all other times. Such subject-managed information (content) may be, for example, a "secret sign" associated with signature/sign recognition, a password associated with keystroke recognition, a phrase associated with voice recognition or a user-defined sequence of fingerprints are presented. The subject-managed information may either be treated as an integral part of the biometric information (sample or template) inseparable from the rest of the information (i.e., be “content-bearing”), or may be coupled with a biometric sample or template, and stored or transmitted along with it.

The assumptions of biometric authentication are different from those of password-based authentication. The following statement expresses a typical set of assumptions: In a normal verification operation (consisting of a capture sub operation, a process sub operation, and a match sub operation) performed by a "biometric system", there is a reasonable certainty that the biometric sample being input into the biometric system has been produced during the capture sub operation by a real sensor measuring a certain biometric characteristic of a real person.

The less confident we are that there is a real sensor that has performed a fresh measurement of a real person and has just provided a sample to the biometric system, the less we trust the result.

Below is a partial list of assumptions of biometric authentication, which includes a summary of the assumptions expressed by the above statement as well as others:

- There is a real subject, whose biometric characteristic has been measured.
- There is a real sensor, which has provided input to the biometric system.
- The sample being input into the system is a fresh sample, captured during the time interval in which the biometric system was expecting a capture to take place.
- The biometric characteristic used in the capture sub operation is sufficiently distinctive over the given population.
- The biometric characteristic remains intimately tied to the individual for long periods of time.
- The biometric characteristic is relatively stable for each individual (does not change significantly over space, time, environmental conditions, physiological conditions, etc.)
- For any biometric characteristic whose measurement requires active cooperation from the subject, the subject is capable of providing that cooperation under normal circumstances.
- The measurement technology (comprising both hardware and software) does not significantly affect the variability of the measurements.
- The extraction, matching and communication processes are not tampered with during any stage of the process.

Likewise, here is a partial list of assumptions of password-based authentication:

- The subject is the only individual who knows his password
- The subject has chosen his password in such a way that the probability of it being guessed by other individuals of the same population is very low

- The password is chosen in such a way that the probability of it being guessed by a malicious software program within a reasonable time is very low
- The subject remembers the password
- The subject retains the ability to enter the password into the system upon request

These lists are not intended to be exhaustive, but they show how different the assumptions of these two authentication technologies are. For both technologies, an uncertainty on whether an assumption is verified in a given case directly affects the degree of trust in the result of an authentication operation.

5.5 Comparison of Cryptographic and Biometric Philosophies

NIST SP800-63 has, as its roots, the cryptographic algorithms and protocols and the public key infrastructure (PKI) upon which NIST has already standardized. While SP800-63 makes some statements about biometrics in the context of e-authentication (see Section 3), it does so from the perspective of the cryptographic community. Consequently, it is both interesting and relevant to consider the similarities, differences, and biases between the cryptographic community, which fostered and nurtured those standards, and the biometric community. This comparison is summarized in Table 5 below.

Table 5 - Comparison of Cryptographic and Biometrics Communities

Category	Issue	Cryptographic Community	Biometrics Community
Assumptions	Data	The strength is in the data (key), not the algorithm. Therefore, share the algorithm and maybe the implementation with everyone.	Biometric data is unique to each individual.
	Computational Complexity	Only a concern for embedded devices.	Only limited by implementation performance considerations.
	Devices	Hardware implementations can be implemented securely.	Biometric capture can be done and be made secure.
	Privacy	Not applicable.	Enrolled biometric data must be protected at the system level using conventional best practices.
	Secrecy	All cryptographic mechanisms depend on the secrecy of the data (key).	Although there is debate over how secretive biometric data really is, biometric technologies do not rely on maintaining secrecy.
	Business Incentives	Primarily at the infrastructure level and not at the algorithmic level.	At all levels of the technology and deployment.

Category	Issue	Cryptographic Community	Biometrics Community
	History	Established history of best practices with cryptography (see, for example [FIPS1402]).	Some biometrics have a long history of usage are considered mature. Other biometrics are newer and still establishing their viability. There is on-going research.
Technological Characteristics	Dependency on Human Interactions	None.	Very dependent. All input data originates with the live capture of a person's biometric data.
	Algorithmic Approaches	Completely deterministic, at least mathematically.	Effectively only statistical approaches are used. Can be based on a wide variety of algorithms.
	Key Generation	Determined by algorithm.	Template generation is determined by algorithm
	Key Storage	Stored key must be protected against unauthorized access at the system level to ensure secrecy of the key.	Enrolled biometric data must be protected against tampering at the system level to ensure integrity of the biometric data.
	Repeatability	Deterministic - Based on principles alone, a cryptographic algorithm should be 100% repeatable.	Probablistic – Matches determined based on similarity. Repeatability varies by modality and is influenced by intrinsic and extrinsic factors.
	Strength	Directly proportional to key length and tested robustness of algorithm.	Modality specific. Raw accuracy is measured by 3rd party testing and is one factor of overall strength of function (see section 7.5).
Peer Review	Philosophy	Open reviews with open and even confrontational discussions of results.	No peer review of algorithms, which usually are proprietary. The biometric engine and its enclosed algorithms are treated as black boxes and tested accordingly (see below).
	Methodology	Theoretical algorithm analysis and experimental cracking techniques.	Performance tests by independent bodies/agencies.
Data Compatibility	Key Formats	Keys are either ASCII strings or arbitrary 8-bit binary data. No compatibility issues or interoperability issues.	INCITS M1.3 and ISO/IEC SC 37 WG3 - Data Interchange Format standards for each biometric modality.
	Data Formats	Several standards apply (PKCS, etc.).	INCITS M1.3 and ISO/IEC SC 37 WG3 - Data Interchange Format standards for each biometric modality.

Category	Issue	Cryptographic Community	Biometrics Community
	Output Results	Binary – either the cryptographic operation works or it doesn't (meaning that the desired data is not returned).	Analog range of comparison scores. Scores are more akin to probabilities than definitive ratings.
Interfaces	APIs	Various common APIs	INCITS M1.2 and ISO/IEC SC 37 WG2 - Interface standards i.e. BioAPI.
Testing	Approach	Mathematical analyses of various kinds plus experimental attack implementations. Any and all attack challenges are welcome.	INCITS M1.5 and ISO/IEC SC 37 WG5 - Testing and Reporting standards.
	Input Test Data	Any data can be used.	Should be collected from live individuals under documented conditions. Many variables to control or at least acknowledge.
	Output Test Data	Decrypted messages which are either the same as the original messages or not the same. Also, the rate at which a particular cryptographic algorithm and/or implementation can be compromised or the computational complexity to do so.	Sets of performance graphs representing various cross-sections of the possible statistics of the comparison scores.
	Publication of Results	Open and encouraged. No restrictions for serious algorithms under consideration.	Restricted or governed strictly by the testing organization.
System Level	Integrity (Spoofing)	Integrity maintained at the system level using key management standards.	Liveness checking in various stages of development and deployment, depending on modality. Furthermore, a multimodal system will help ameliorate any spoofing attempts.
	Data Injection or Monitoring (Replay Attacks)	Have been dealing with this issue successfully for a long time.	Possible, but the biometric algorithm should reject an exact data match. Furthermore, conventional cryptographic techniques can be used to mitigate the risk.

For most of the comparison categories and issues in Table 5, the cryptographic and biometrics communities approach them in noticeably different ways. As such, the differences significantly outnumber the similarities. There are a variety of possible reasons for the differences, but the primary drivers for the reasons can be grouped into the following general areas:

1. **History** – The scientific disciplines from which the cryptographic and biometrics communities arose tended to approach their respective problems in different ways.
2. **Technological Maturity** – For everyday practical usage, cryptography has been studied, been available, and in use for a longer time than biometrics.
3. **Economics** – Because of differences in their respective marketplaces, different business strategies evolved between the two communities. The outcomes and side effects of these strategies either directly or indirectly led to several of the differences between the cryptographic and biometrics communities.

One of the challenges that this report attempts to address is to describe the different ways that biometrics can be used for e-authentication in such a way that it transcends some of the differences in Table 5. If successful, this approach would allow both the cryptographic and biometrics communities to utilize biometrics in e-authentication applications in a mutually beneficial manner.

5.6 Biometric Modality Comparison and Content-Bearing Capability

5.6.1 Biological and Behavioral Biometrics

As discussed in Section 4.3.1, *Biometrics* is the "Automated recognition of individuals based on their behavioral and biological characteristics". While the definition technically states that all biometric modalities are BOTH biological AND behavioral, it is common to attempt to classify each biometric modality as EITHER biological OR behavioral.

Biometrics researchers and developers have always been aware of differences among biometric modalities. Problems arise when attempts are made to partition biometric modalities into simple categories. The problem is that there seems to be differences but when one attempts to pin them down them they become elusive. For example, in Section 4.3.1, we presented the ISO definition of biometrics as "automated recognition of individuals based on their behavioral and biological characteristics".

Can we use this definition to divide biometrics into two or more groups according to degree to which they are biological vs. behavioral? Initially, it appears simple and straightforward: biometric characteristics that appear on the surface of the body, such as fingerprint and iris are "biological" and characteristics that have a strong temporal component, such as speech and signature/sign, are behavioral. According to *Webster's New Universal Unabridged Dictionary* "biology" is "the science of life or living matter in all its forms and phenomena, esp. with reference to origin, growth, reproduction, structure and behavior" and "biological" is defined as "pertaining to biology." The definition invalidates the opposition between "biology" and "behavior" – and even between "physiology" and "behavior." The issue is further muddied by the fact that biometrics that might normally fall into the "behavioral" category (e.g., sign/signature, keystroke, voice) rely heavily on the analysis of body structures, such as the size and shape of the vocal tract. Figure 12 illustrates the continuum into which various biometric modalities may fall with respect to this characterization.

Figure 12 - Spectrum of Modality Comparison

NOTE: Regardless of how a biometric modality is classified, a time based component or "dynamic" property exists for all modalities. Behavioral biometrics rely heavily on the capturing and using the temporal data in the biometric sample as well as monitoring gradual changes over time. Since they capture and use the temporal data, behavioral modalities are viewed as dynamic biometrics.

5.6.2 User Lifecycle and Revocation

Content-bearing biometrics add a new dimension to the biometric which introduces its own variability but it also adds a powerful set of discriminating data.

One way of dealing with sample variability is to measure and store it as part of the reference template. Most enrollment processes capture several samples that are all used to form a single template that incorporates variability data.

One of the ensuing benefits of measuring the sample variability and storing it in an adaptive template is that it is then much easier to determine individual sample distributions. Individual FRR thresholds can then be determined in an efficient manner, on an a priori basis, using sound statistical theory, as opposed to setting them based upon empirical data after the event. When the sample variations are measured during enrollment, it is possible to test the samples for consistency before forming the template. This prevents two or more people colluding to generate a combined template and thereby enabling any one of them to authenticate.

Should the content-bearing reference template actually become compromised, the revocation for whatever reason could be as simple as a re-enrollment. The re-enrollment of different content in the biometric data submitted can be undertaken at any time and in the same way that passwords and PINs can be changed.

5.6.3 Content-Bearing Biometrics and SP800-63

In SP800-63, one of the bases used to question the validity of biometrics as a form of security is that biometrics are not secrets. In fact, one of the unique properties of content-bearing biometrics is the ability of the enrollee to incorporate secret user-controlled data into the biometric process. In fact, content-bearing biometrics combine secrets with biometric samples to provide two-factor authentication and they do it in one step. For instance, the users of signature/sign biometrics can enroll with "signs" of their own choice which may or may not be their signatures. A person's signature can be considered to be a non-secret, special case of a sign in this modality. If the biometric enrollment process inhibits the display of the sign and deletes the raw sample data after extracting the biometric features, then there is a high degree of secrecy associated with the sample. The biometric process therefore combines both a secret (sign) and the associated biometric sample into one operation giving it effective two-factor authentication status. Similarly, voice and keystroke systems may contain passwords or phrases. During authentication both factors are checked: biometric and passphrase/secret. In all cases, these secrets are alterable in the same way standard passwords are changed. The strengths and vulnerabilities of these biometrically-linked secrets are identical to those for general use of passwords. When used in conjunction with the content-bearing biometric data, however, the biometric test would still discriminate even if the password were compromised. An example of

the use of the PIN with a biometric sample in a mobile device Password Replacement system is contained in the M1 document M1/06-0495:
http://www.incits.org/tc_home/m1htm/2006docs/m1060495.pdf.

Challenge-response to secret knowledge can be incorporated into authentication with content-bearing biometrics. In voice systems, for example, challenge-response is used when the biometric matching results are inconclusive or when the interaction is considered suspicious.

With all biometric systems, additional security factors can be added, such as a PIN. The PIN would have a multiplicative effect upon the inherent entropy of the biometric data, which contain both a secret and a biometric sample. Other content could be in the form of written text, spoken words or the user interaction sequence with the device such as certain finger placements or facial orientation and expression. Figure 13 is a simple illustration of the range of content possible by various biometric modalities and implementations.

Figure 13 - Spectrum of Embedded Content

6 Biometric Authentication Architectures

6.1 Architecture Comparison

The list of possible architectural configurations consists of the combinations of the following decisions relating to the location of the reference template storage and biometric matching operations shown in

Table 6. Processing (transforming the raw biometric data into a processed record suitable for matching) may occur at the point of capture or at the point of storage.

Table 6 - Biometric Matching and Storage Locations

Storage Location	Matching Location
Server (Central/Distributed)	Server
Local Workstation (Client)	Local Workstation (Client)
Device (Peripheral)	Device (Peripheral)
Physical Token	Physical Token

These locations are defined as follows:

Server. A centrally located (or distributed) computer that is remote from (networked to, but not physically collocated with) the requesting client. Sometimes referred to as a "biometric authentication server". (Note – this may or may not be part of, or co-resident with, a verifier.)

Client Workstation. The local computer platform (local host) from which a user initiates remote authentication. Generally a PC or equivalent (e.g., laptop) executing a general purpose operating system. For remote e-authentication, the client is the entity which hosts the web browser or other client application (e.g., VPN). PDA's and some other mobile platforms are considered clients in this context.

Device. In this context, two types of devices are defined:

- *Peripheral device*. A biometric sensor unit that can be connected to a client workstation via an interface (e.g., USB connection).
- *OEM device*. A biometric sensor module that is embedded within a client workstation or a peripheral. For example, a fingerprint sensor module that is hard mounted within a laptop PC or PDA.

Sensor devices may be "dumb" – i.e., it captures and returns raw biometric data only – or it may include some intelligence such that storage, processing, and/or matching may be performed within the device.

Physical Token. A physical object that may support biometric storage or matching. Examples include smartcards, PCMCIA cards, USB memory sticks, RF tokens, etc.

Note that devices and physical tokens exhibit a range of features, cryptographic capabilities, and tamper resistance.

6.1.1 Storage Locations

A biometric reference template must be stored at some location such that it can be retrieved during the identification or verification phase. This template is not the original (raw) biometric data itself, but a mathematical representation of the biometric data. Even though it is usually not computationally feasible to recreate the entire original biometric data from the biometric template, the storage architecture plays an important role in security and performance of the matching algorithm.

There are predominantly four different kinds of template storage architectures that exist in the field of biometrics: 1) Central Database 2) Local Database 3) Portable Storage 4) Storage on the sensor. The advantages and disadvantages of each of these storage architectures are discussed in the following paragraphs. It should be noted that systems exist that use a combination of these template storage methods. This allows for greater flexibility, when appropriate. For example, when network-based matching is used but a network connection is not available, then location matching may occur. This may occur in a notebook computer that uses central storage when the notebook has a network connection and local or on-sensor storage when the network is not present, such as when traveling on an airplane. The template storage method(s) chosen depend on the requirements of the system and the users, and other factors such as cost and management complexity.

Central Database

Storing all the reference templates on a central repository overcomes the problem of redundancy of data. In a biometric system where users can be authenticated from multiple locations, a centralized database that is networked with all the sensors provides an advantage of remote authentication. Data management is easier, since all the data is stored in a central repository. For example, if a user has to be removed from the system, an update to the central database will ensure that the user cannot be authenticated using the biometric system. Central databases offer the advantage of comparing a biometric sample to multiple templates, thus offering identification mode of authentication. The disadvantage of the central database approach is that an intruder can intercept the communication over the network, and in case of an unencrypted communication, the intruder could get hold of the template and use that in a replay attack. A centralized database that gets too large could potentially add to the computational complexity of the matching algorithm. Centralized databases also put the onus of securing the biometric templates with the owners of the biometric system. A compromise of the database could potentially compromise all the biometric templates stored on the database.

Local Database

Another storage architecture design is to store reference templates on a local database which would be accessible only to the workstation, access control device or other token where the sensor is attached. This storage architecture design is advantageous for users who log onto the same device regularly, such as with notebooks or for specific doors in an access control system. Because there is no central template repository, there is no focal point for an intruder to attack. Local databases can help by distributing the computational complexity of a centralized matching algorithm. The main disadvantage of a local database is that authentication from multiple locations is not possible, unless there is a copy of the user's template at every access point of the biometric system. This can be done in hybrid systems that synchronize the template information between the central and local databases. The added complexity is similar to systems that

synchronize on-line and off-line email, which is common today. Another disadvantage of these systems is the security of the local template database and/or local matching. If strong cryptographic methods are not used to protect the local database or the matching result, the template information could be substituted or the match result could be altered, leading to a security breach. If a user has to be removed from the system, the administrator has to ensure that every copy of user's template is removed from every local database, or the user account is canceled on all devices, which can be done by a central control system, such as in an access control system. Local databases do provide the added benefit of "off-line" or disconnected authentication. This allows systems to be used with the network connection is not available.

Portable Storage

Storage of the enrollment template on a portable (physical) token such as a smart card, biometric token, or other self-contained device is seen as the most privacy friendly option. The holder of the token has control over when their token is used, hence they control when and where their enrollment template is accessed and for what purpose. This control may provide the user with a sense of added security or privacy.

Since the template travels with the owner of the biometric data; it can be used for authentication at multiple locations. There is no communication over an open network assuming the authentication is done locally, thereby lowering the risk of an intruder trying to capture the enrollment template or alter the biometric match result.. The disadvantage of this method is the higher cost of implementation of such storage architecture. Every sensor must be accompanied by a device that can read the stored template and match the stored template, which can add to the total implementation cost. Also, the system administrator has no means of ensuring that duplicate enrollments do not exist. For example, a person could enroll the same fingerprint under two different identities. The only way of eliminating this duplication is to have a rigorous process when issuing a biometric storage token that prevents a duplicate enrollment. This can be done by maintaining a central list of all the enrolled users, but this would add to the complexity of the biometric system, so the system designer need to consider this tradeoff.

Storage on the sensor

Storing and matching of user's reference template(s) on the sensor itself provides a quick response to the identification or verification attempt. This type of storage architecture is growing in usage as the size and cost of biometric capture and matching devices continue to decrease. For example, the camera on cell phones could be used as a capture device for facial recognition controlled from the phone. Such storage architectures cannot be used for user authentication from multiple locations, but are helpful to authenticate specific users to specific devices such as notebooks, smart phones, portable storage devices and other mobile devices that hold information that should be kept secret. If the sensor and matcher use secure cryptographic processing methods, then the template and/or biometric match result can be protected from being stolen or altered, thereby enhancing the security of the system. If a user has to be removed from the system, the administrator would need to remove the template from the sensor, which can be done during a device provisioning process, such as a server-based "push" method, which is common in computer networks and cellular networks, where devices can be centrally managed. Storing templates on the sensor itself is an option only if the sensor is going to the physically secured such as by approved methods such as FIPS 140-2.

6.1.2 Matching Locations

The matching location for the biometric system is an important factor for the overall performance of the biometric system. The matching locations can be predominantly classified into four different categories: 1) Matching on central server 2) Matching on local machine 3) Matching on sensor 4) Matching on physical token. The advantages and disadvantages of each are discussed in the following paragraphs.

Matching on central server
In this type of a system, the matching of the reference template and the recognition sample takes place on a centralized server, which could potentially also store the biometric templates for all enrolled users. Matching on central server is a good option when all the templates are stored on a central database, and preferred means of authentication is identification. The biometric sensors can all be networked with the central server, allowing access from multiple locations with the matching algorithm executing on a central server. Matching on central server does introduce security concerns due to the network communication between the central matching location and the biometric sensors.

Matching on a local machine
Matching on a local machine can work with centralized database storage and local database storage architecture. For architecture storage that has a local database, matching on a local machine will give the optimal performance.

Matching on sensors
Several embedded biometric solutions that act as stand alone systems use a matching algorithm that is stored on the sensor itself. These kinds of solutions provide a quick result and also provide high level of security because of its isolated design. There is no communication with an outside system, thus eliminating any opportunities for an outside attack.

Matching on physical token
Technologies exist today that perform the matching of a biometric template and the presented biometric sample on a portable token such as a smartcard. This mechanism provides complete security for the template and verification process since it takes place on the smart card. This is also an isolated system in which the decision making unit and the storage of the template do not require any kind of external communication. From a security perspective, the weakest link is always the communication between the decision making unit, the sensor, and storage of templates. The closed system of a tamper proof smart card removes this link. Security vulnerability exists in the communication link between the smart card reader and the smart card itself.

6.2 Architecture Alternatives

Based on the available biometric solutions and prescribed assurance levels, six (6) out of sixteen (16) possible architectures identified have been selected for further analysis. The basis behind selecting the six (6) architectures chosen was determined by the most common architectures currently being deployed for biometric authentication. These industry trends are viewed as the starting point for not only securing remote biometric authentication, but also other authentication

credentials. Certainly, implementers could choose to use any of the sixteen (16) architectures in the matrix. The pre existing requirements for security at the pre-defined four levels of assurance were taken into account in finalizing the list of architectures included for this report. Should other architectures not currently being pursued prove to be of value, future work in those arenas could result based on demand.

The four options for both storage and matching described above create a total of 16 possible environments that can be utilized. These 16 permutations are listed in the matrix shown below in Table 7.

Table 7 - Biometric Storage and Matching Matrix

Match \ Store	Server	Client	Device	Token
Server	A			D
Client		B		
Device			C	E
Token				F

6.2.1 Architecture A – Store on Server, Match on Server

This architecture stores biometric templates on a server and requires that live samples be submitted back to the server in order for the matching process to occur. Once a match or no match result has been determined, the result is then sent to the verifier and the appropriate actions take place.

Related to this biometric architecture is the "Web Services Model." The Web Services Model is the basic architecture for interacting with remote Web services. It can be viewed as an extension of Architecture A (or possibly D) that includes a browser receiving data from the data collection device and transmitting that data over the network to the web application/service, biometric engine, or verifier responsible for authentication.

6.2.2 Architecture B – Store on Client, Match on Client

This architecture stores biometric templates on a client platform and requires that live samples be captured and matched at the client. Once a match or no match result has been determined, the client application communicates the result to the verifier. This architecture is beneficial in the case where authentication must happen very fast or in the case that the client is disconnected from the network and cannot communicate with a server.

6.2.3 Architecture C – Store on Device, Match on Device

This architecture stores biometric templates on an authentication device (e.g., a "self-contained" biometric sensor unit or a PDA, cell phone or other mobile device) and requires that live samples be matched on that device. Once a match or no match result has been determined, the device sends the appropriate signal to the mechanism it is securing. This architecture is typical in mobile device/remote network access control or a physical access scenario when the device obtains a live sample and matches it to its stored database in order to give access to a physical space.

> NOTE: A variation of this physical access example is the store on server, match on device scenario.

6.2.4 Architecture D – Store on Token, Match on Server

This architecture stores biometric templates on a physical token such as an integrated circuit chip card or smart card. In practice, the user inserts the smart card and presents their biometric. Both the stored template and live sample go to the server for matching.

6.2.5 Architecture E – Store on Token, Match on Device

This architecture stores biometric templates on a physical token such as an integrated circuit chip card or smart card. But unlike Architecture D, the live sample is compared and matched on the local device instead of on the server. This architecture would allow for an all inclusive device such as a PDA which would capture the sample, compare against the template, and hold another authentication credential.

6.2.6 Architecture F – Store on Token, Match on Token

This architecture stores biometric templates on a physical token such as an integrated circuit chip card or smart card. But unlike Architecture D or E, the live sample is compared and matched on the card instead of the server. This could result in access to an authentication token stored on the card, such as a certificate used in an authentication protocol.

7 Challenges to Biometric Authentication

In terms of use as an authentication mechanism, biometrics are considered a relatively new and different approach. Because of some of the differences in characteristics and use of biometrics in this role, the general security community, particularly cryptologists, have been sometimes skeptical that biometrics can be used effectively for this purpose. There is certainly a "paradigm shift" involved, since most biometrics do not fit the traditional mold. There is a basic understanding that biometrics are more tightly bound to a specific individual, and this is seen as a major advantage of the technology. However, over the last ten years, a number of critiques have been targeted at biometrics by security experts. Some of these critiques are valid and warrant analysis, while others are based on a basic misunderstanding of the technology itself or the ways in which its characteristics require modification to traditional processes. At times, biometrics are attempted to be "force fit" into a traditional paradigm to which they do not belong.

As part of this study, the following issues and questions were identified. Although some concerns raised are actually common to all authentication protocols, and for the most part have known solutions, this section concentrates on those which are either unique to the use of biometrics in an e-authentication environment, or which have unique aspects to them as a result of the use of biometrics. These challenges include:

1) Integrity -vs- Secrecy
2) Compromise
3) Revocation
4) Sensor Spoofing/Liveness Detection
5) Entropy/Strength-of-Function
6) Peer Review Methods
7) Privacy Considerations

Each of these critiques is addressed in the following subsections. It should be noted that although these topics are addressed separately, they are interdependent in many ways and therefore the discussions tend to overlap to some degree.

7.1 Integrity v. Secrecy

Traditional authentication protocols are generally based on the secrecy of the authentication "token". However, most biometrics (see Section 5) are not considered secrets and therefore fall outside of the traditional paradigm. This begs the question of the role and relative importance of secrecy and integrity of the biometric data in the overall authentication protocol and system. When the biometric is not a secret, then why and how should it be protected? If the authentication protocol cannot rely on the secrecy of the data, what does it rely upon?

7.1.1 The Role of Secrecy

The primary mechanism for protecting the secrecy (confidentiality) of any data is via encryption, although it is recognized that other protections, such as access control mechanisms, also apply. However, in the general case in which the biometric is not a secret, what purpose is served by this?

Biometric vendors often offer solutions that involve encryption of biometric references. The reasoning behind this is tri-fold:

1. To ensure the confidentiality (i.e., privacy) of the biometric data stored in the biometric system (see Section 7.7),
2. Although not a secret, access to digitally encoded copies of this data can make an attacker's job all that much easier, and/or
3. Encryption facilitates the segregation of biometric references used for different applications (to ensure that the biometric data from one application cannot be injected into another application).

With respect to the segregation of biometric references for different applications, standard encryption methods should be used, rather than proprietary transformation techniques.

Regarding the first two points, biometric characteristics are not necessarily secret and so it is not the secrecy of the information extracted that needs to be protected, but its integrity is critical. On the other hand, since the biometric reference is one of the critical data elements in the system, encrypting this data would be prudent for increased data protection.

Although confidentiality concerns are usually addressed for the enrolled reference template, of equal importance is the confidentiality of the live sample. In fact, this information (if it can be used) may be of more potential use to an attacker.

An interesting side note is that biometric data (particularly reference data) may be anonymous. It is actually the binding of the biometric information to an identity that can be most troublesome. (Within SP800-63, anonymous credentials are only allowed at levels 1 and 2.) It is this binding, however, that forms a credential and can provide a type of revocation ability.

It is noted that for biometrics that contain secret information (see Section 5.6), the role of secrecy coincides with that for traditional methods.

7.1.2 The Role of Integrity

Given that secrecy is not the basis of a biometric authentication protocol, then what becomes critical is that:

a) The biometric is captured from a living, present human being, and
b) The biometric data has not been modified in any way.

That is, the integrity of the biometric data and process is THE critical factor.

The first of these criteria is addressed by anti-spoofing and liveness detection as discussed in Section 7.2 and therefore not further discussed here.

Protection from modification is primarily provided through digital signatures. This could also include MAC'ing or embedding the biometric data within an X.509 attribute certificate which would normally be applied to the reference template. Where the signature is applied and when it is verified are also important considerations. The integrity of both the reference template as well as the live sample are of importance.

Knowing where the data originates is also part of the overall integrity (i.e., authenticity related to the source). The applied signature addresses this, but authentication of the various components, including the capture device, may also be warranted at higher assurance levels.

As stated above, the integrity of a biometric reference is critical to the assurance of the overall system security. The integrity of the authentication process is dependent on the integrity of the template (among other things) [7]. If either the reference template or the 'live' sample is untrustworthy, the resulting authentication will be untrustworthy. Untrustworthy templates or samples could occur for one or more of several different reasons:

- Accidental corruption due to a malfunction of the system hardware or software;
- Intentional modification of a bona-fide template by an attacker;
- The insertion of a biometric template corresponding to the attacker to substitute for the reference template of an authorized enrollee;
- The insertion of the biometric template corresponding to an authorized enrollee to substitute for the live template of the attacker.

The deliberate modification or insertion of a template would typically be the action of an attacker attempting to subvert the normal biometric authentication function and thereby gain access to the protected assets.

To use a fake template to defeat the biometric authentication mechanism, the template would need to be injected into an appropriate point in the biometric system. This could be the template database or a communications path in the system. For example the impostor could claim to be an authorized user but, when requested to supply the biometric feature, would instead inject the template belonging to the authorized user in the communications path.

A fake template would need to be able to overcome any integrity checking of the biometric system. Conversely, to protect the authentication integrity, the system must be able to detect and reject such attempts at meddling. Thus template integrity is a key issue in protecting authentication integrity. Note that template confidentiality is not an essential requirement for this purpose.

Biometric systems must employ effective template integrity protection. This could be through access control, to prevent unauthorized access to the templates, or by integrity checking, probably using cryptographic techniques. This could involve digital signatures, or template encryption. Integrity protection may need to be combined with other techniques (such as time stamping) to protect against the reuse of stolen templates. Reference templates can also be

marked (before signing) to distinguish them from live templates, in order to prevent the substitution of reference templates for live ones.

One emerging standard that addresses the integrity of the overall biometric authentication process is called ACBio (Authentication Context for Biometrics). This is briefly described in Annex D1.2.

Note that while digitally signing a template may be adequate to protect its integrity, it will not (on its own) provide any confidentiality of the data. If confidentiality is required for example to protect the privacy of the biometric data access control and/or encryption techniques may be necessary.

7.1.3 Biometric Identification Record Protection

Securing the BIR itself is a critical issue also. In order to tackle the issues of protection of biometric data during transmission and storage, the standards identified in Section 5.3.5 specify security requirements for effective management of biometric information.

The confidentiality of biometric data can be achieved using tested encryption methods like 3DES or AES. The integrity of the BIR can be achieved using a digital signature or Message Authentication Code (MAC). Integrity of the transmission, which would be necessary to detect replay attacks, can be achieved using a unique session key or time stamps.

The header of the BIR contains information about the vendor and type of technology used, in addition to other information. In order to maintain integrity, the BIR needs be digitally signed or a MAC has to be calculated for it. The information about the method used for calculating the MAC or digitally signing the biometric object then needs to be added to the BIR in addition to the MAC value, so the receiver of the BIR can perform the same MAC calculation and check it against the MAC value calculated by the sender. If those two values don't match, then the biometric object has been changed [1]. A high level reference model of BIR integrity is shown below in Figure 14.

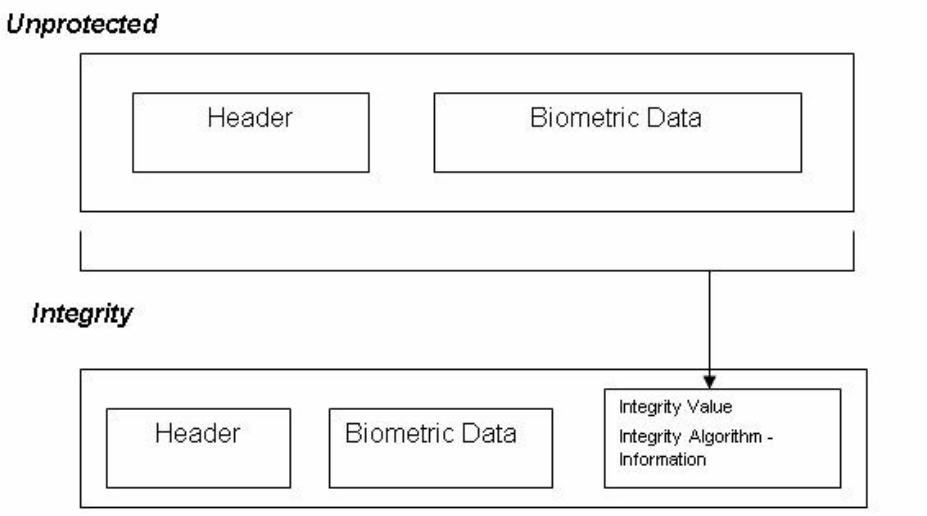

Figure 14 - Biometric Identification Record Integrity

As mentioned before, confidentiality of the BIR can be achieved by encrypting the biometric data block. The biometric data block would be encrypted using a cryptographic mechanism. The key management information and information about algorithm parameters would be included in the BIR. The receiver would use the information about the type of encryption algorithm used and key information and decrypt the biometric data block, provided that the encryption key is secret only between the sender and the receiver [1]. A high level reference model of BIR confidentiality is shown below in Figure 15.

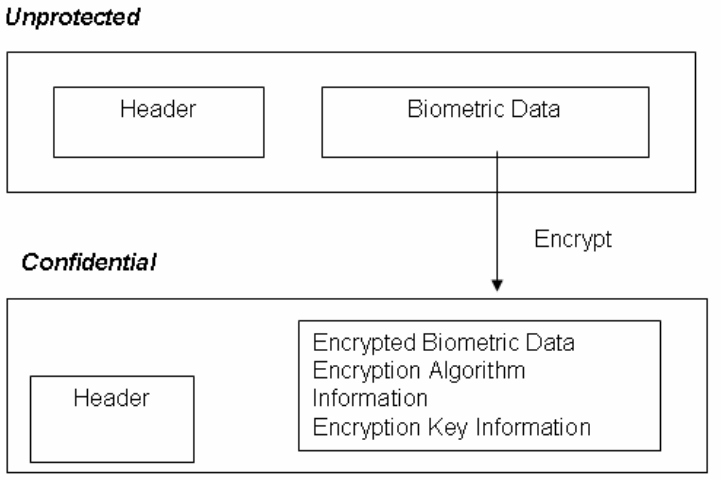

Figure 15 - Biometric Identification Record Confidentiality

In order to maintain integrity and confidentiality of the BIR, the biometric object can be digitally signed and information about the signature can be included in the security block of the BIR. Then the biometric data block can be encrypted, and information about the encryption algorithm and encryption key can be included in the security block of the BIR. This mechanism provides both integrity and confidentiality of the BIR.

7.1.4 Biometric CSP

One approach to consider is the use of a "Biometric CSP" for non-token based biometric implementations within remote e-authentication architectures. A biometric service provider (BSP) provides an API comprising biometric functionality. Cryptographic functionality is usually provided by a cryptographic service provider (CSP). It is possible to implement a combination of these capabilities in a single component that exposes both biometric and cryptographic interfaces.

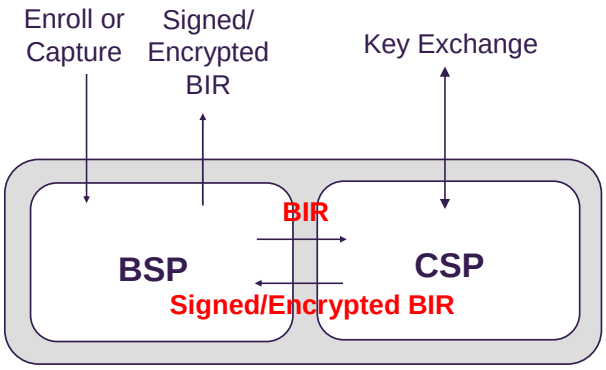

Figure 16 - Biometric CSP

In this way, the BSP can protect the confidentiality and/or integrity of the biometric data it generates through cryptographic means while allowing for the associated key management to be handled through a (logically) separate interface. For example, the biometric functions (i.e., enroll, verify) could be accessed via BioAPI while the cryptographic functions could be accessed via PKCS-11 or CAPI.

7.1.5 Key Management

The main objective for going through a cryptographic process is to retain the confidentiality and integrity of the data. Key management is an issue that plagues both symmetric encryption schemes and asymmetric encryption schemes. A major concern in the field of security is the possibility of the private key being stolen or misused. A solution that is often used is to store the private keys and protect those using passwords. Due to problems with remembering passwords, many users either choose simple words or phrases that are easily cracked or they simply write it down on an accessible document. The second problem is that a password is not tied to a user; the system running the cryptographic algorithm is unable to differentiate between the legitimate user and an attacker who fraudulently acquires the password of a legitimate user [11]. Biometrics offers the potential to considerably enhance the contemporary key management model. Complex passwords are easy to forget, and simple passwords are easy to crack by unauthorized individuals.

Several biometric characteristics of an individual are unique and remain constant over time. These properties of biometrics make it well suited for authentication for purposes of key management. Instead of entering a password to access the cryptographic key, the use of this key is guarded by biometric authentication. One company has created an innovative algorithm, called Biometric Encryption, for securing a key using a biometric. The key is linked to the biometric at a fundamental level during enrollment, and is later retrieved using the same

biometric during verification process. The key is kept independent of the biometric, so that if the key is compromised, the biometric template is not compromised. The key or the biometric template cannot be retrieved independently from the secure combination of the digital key and the biometric template.

The integration of biometrics with existing cryptographic techniques offers the potential for high confidence in applications where security is paramount. The additional benefits provided by the combination of biometric technologies with current cryptographic techniques can help improve security and convenience.

7.2 Compromise

"Compromise" is a problematic word, which is commonly used in cryptography to mean that a password or key (which was supposed to be kept secret) has been revealed, exposed, or guessed. A more general meaning of this word is that something has been put in jeopardy, or (as life, reputation, or dignity) endangered by some act that cannot be recalled, or exposed to suspicion, discredit, or mischief (Compromise). Revealing or exposing a password is considered a "compromise" of the password probably because it makes the password untrustworthy, discredited, and thus unusable as a credential. A disclosed password is untrustworthy and unusable as a credential because, once it has become known to other people; it is no longer uniquely associated with its original owner. The idea of biometric compromise is closely related to the argument that biometrics are not secrets i.e., copies of biometric features may be obtained with varying degrees of difficulty.

In the broadest terms, a biometric compromise would mean that another individual has the ability to provide your biometric data when a biometric application requests a sample. For example, that person has:

- An electronic copy (could be an image or a template) of your biometric data and has the ability to insert it into the application or authentication protocol at the appropriate time and place.
- A physical copy of your biometric characteristic (e.g., gummy bear with fingerprint, photo of iris) and the ability to fool a sensor's liveness detection (if any).

Note that a biometric compromise consists of two components. First, the adversary has to possess a reproduction of your biometric characteristic. Secondly, that reproduction has to be "usable". The adversary must have the knowledge, technology, and access to insert it into the biometric application. The adversary must be able to overcome any mechanisms (countermeasures) that are applied to prevent this "use" (e.g., encryption, liveness detection).

In biometric authentication, revealing or exposing a credential (a biometric characteristic) does not, in general, make it untrustworthy and unusable as a credential, and therefore does not constitute a "compromise". So the term "compromise" is either meaningless when applied to biometric authentication (in general), or should not be used unless its meaning has been adapted to the specific nature of this authentication technology. In short, in biometric authentication, a "disclosure" does not imply a "compromise" as it does in password-based authentication.

The word "compromise" is used in the following paragraphs to mean that a credential, in the context of a given authentication protocol, has become untrustworthy, discredited, and thus unusable within that authentication technology.

7.2.1 Can there be a compromise without an attack?

Similar to password-based authentication, a compromise can occur either with or without an attack. Just as when a password is discovered through a password guessing attack, a biometric can be compromised by forging a zero-effort attack against the system. Additionally, just as passwords can be written down, lost or stolen, the enrolled biometric template can be discovered if its storage location is compromised (e.g., if the physical token is lost or stolen or the database is broken into).

7.2.2 Are compromises permanent?

In biometric authentication, a state of compromise of a credential is limited in time and space. For example, a gummy finger may deceive some of today's fingerprint readers but will probably be detected and rejected by tomorrow's fingerprint readers as sensor technology improves.

In password-based authentication, states of compromise of credentials are (in principle) permanent, because a password can be remembered forever by whomever has gotten to know it. It is true that the basic biometric features cannot be changed, though in some cases, alternatives may be available such as the use of different fingers. However the simplicity of the argument conceals some more complex and subtle issues. Section 5.6 described some of the ways that content-bearing biometrics can be utilized in mitigating this potential problem.

7.3 Revocation of Biometric Identifier

Although the advantages of biometrics have been well publicized, there are a few key issues that could be detrimental to wide adoption of biometrics. Revocation of biometric identifiers is a key problem that needs a solution for biometrics to be widely adopted and integrated into the existing security infrastructure. This section addresses the following issues:

1) Potential issue of revoking a compromised biometric identifier and assessment of the problem,
2) Investigation, identification, and analysis of possible mitigation approaches,
3) Detailed description of possible solution,
4) Proof of concept implementation of the solution.

7.3.1 Potential issues of revoking compromised biometric data

According to ITU-T X.811, *Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Authentication Framework*, The definition of revocation is the “permanent invalidation of verification authentication information”

For some biometric modalities, it is not practical to revoke a biometric characteristic, per se. For example, revocation cannot mean that you can’t use your right index finger any more. This could be because some systems will require (by policy) that right index fingers be used, or because as soon as you have 10 compromises, you are out of fingers.

Revocation in a biometric system could refer to invalidating the binding of a biometric with a specific user ID, key or other identifier. A stored biometric could be associated (bound) with that identifier. Once a live biometric is compared to a stored biometric and a match is determined, the identifier can be declared valid. If this binding is removed (revoked), then the identifier will not validate.

The question is often asked, "If a password is acquired by an attacker, then it is easy to create a new one and revoke the old one; but if a biometric template is acquired by the attacker, the template cannot be changed, so how can the system be protected while still authorizing the legitimate user to have access?"

It is difficult for the biometrics advocate to respond to this statement because there is no equivalently easy answer. So what is an appropriate, strong answer that will emphasize that the two situations are not completely equivalent and that the biometric situation is not as hopeless as it might seem at first glance?

First, we make the point that the two situations are not really equivalent. The secret-based case is obviously simple to understand, because the problem it describes is simple, and the solution, create a new secret and revoke the old, is also simple. What is usually not discussed is that the threat posed because the attacker has the secret is a threat that is easy to exploit: all he has to do is enter the secret via the keyboard or other readily available device and he has all the privileges of the rightful owner. What is also not usually questioned is: What are the fatal flaws that permit the attacker to obtain the secret in the first place?

However, when the attacker has the compromised biometric data he still has the non-trivial problem of how to exploit it. His problem is in no way equivalent to the situation when he possesses the secret and wants to exploit it.

It must be noted that the biometric capture device is not at all equivalent to the keyboard or other secret-input device. The biometric device is built to capture a specific type of information directly from a human body.

It should be immediately apparent that the system is not equivalently vulnerable at the data entry points where, on the one hand, the attacker has obtained the secret, and on the other hand he has obtained biometric data (with the exception of coercing the user into presenting his biometric data to the sensor, but the secret is subject to the same coercion).

In order for the situation with the compromised biometric data to result in equivalent vulnerability for the protected system, the attacker has to have some way to inject the compromised data into the biometric processing path. This is without question not the equivalent problem to just typing the stolen secret into an available keyboard or inserting the card into the reader.

So the first reply is that the two situations are not at all equivalent, and the biometric system is not immediately vulnerable just because the attacker has obtained some data. Some audiences may be satisfied with this reply.

But a second concern must also be addressed, because the assumption implicit in the original question is that the attacker has acquired the biometric data because he has some capability to exploit it.

Now there are two key points to be made: first, the actual vulnerability of the system is inversely proportional to the security "hardness" of the system; and second, the popular view that biometric sensors are vulnerable to spoofing is actively being countered by sensor vendors, academic researchers and some integrators who are developing anti-spoofing techniques such as liveness detection. Both of these issues are discussed in greater detail later in this section.

The first point is that the total system, including the biometric authentication subsystem, should, as good practice, be hardened in proportion to the value of whatever the authentication subsystem is intended to protect, using good security techniques such as physical protections, encryption, data integrity, intruder detection, attended operation, and user training. None of these techniques are any different when applied to a biometric-based authentication system than to a secret-based system.

The second point is that the one vulnerability that is not fully addressed by good system practice, the capture of the raw biometric data (although attended operation helps), is not passively standing by in the face of spoofing threats, but is actively developing anti-spoofing technology not only in response to example threats but even in anticipation of threats that may be tried in the future.

Ultimately, however, the argument may degenerate into pitting the almost syllogistic statement that it's easy to replace something that has no physical reality (the secret), but it's hard to replace something that is based on a unique piece of physical reality (the biometric data).

The remainder of this section examines the current state of technology and alternative methods for revocation of a compromised biometric data and protection of the biometric data.

7.3.2 Possible revocation solutions

Centralized Approach

A centralized approach makes it easier to manage the data and puts the responsibility of keeping the database secure on owner of the security system and not the owner of the biometric data. While formulating possible solutions for the problem of biometric data revocation, an important element has to be considered: there has to be some form of human interaction with the security system in order for the revocation of the biometric identifier to take place the process cannot be fully automated.

A centralized approach offers a few different solutions for revocation of a biometric identifier which are discussed below:

The system administrator can delete the record which has been compromised. This is the easiest solution, but not the most efficient. The system administrator would be required to make a deletion every time a request for deletion was made.

A biometric identifier revocation list can be maintained by the owner of the security system. This kind of a list would be similar to a certificate revocation list. Whenever a user tries to identify or verify, after a match is found, the identity of the individual would be checked against the biometric identifier revocation list. If the particular user is on the biometric identifier revocation list, that individual would not be authorized by the system. Maintaining a biometric identifier revocation list provides an added benefit of audit control. Any identification or verification attempts made using the biometric identifier that has been revoked can be logged and the records can be kept for future purposes.

The database record which corresponds to the biometric identifier to be revoked can be flagged for revocation purposes. If a match is found for the record that is flagged, the user will not be authorized. This would provide advantages similar to that of a biometric identifier revocation list.

Smart card biometric template storage approach

Smart cards offer a localized approach for storing of templates, allowing the owner of the biometric data to be in control of who is allowed access to their biometric template. But smart cards pose challenges of a different kind. If a user loses his/her smart card with their biometric template on it, the security system needs to be alerted that the smart card has been lost. Even though the information on the card is cryptographically secured, the authorities have to be alerted about the missing smart card. In case there is an attempt to use a lost smart card, there has to be a method of alerting the system that there is such an attempt going on. Traditionally, smart cards have used the Public Key Infrastructure (PKI) approach combined with digital certificates to counter the problems of lost smart cards. (PKI is an infrastructure used to maintain public and private key pairs and reliably identify the owner of the public and private key pair.) Digital certificates help identify the integrity of the owner. A trusted third party issues a digital certificate to the owner of the public-private key pair whose identity has been established and verified. In an environment that uses smart card technology, the system administrator can establish and verify the identity of the person being enrolled. Digital certificates contain information about the owner of the card, the public key of the owner, the digital signature of the certification authority, and other data. Whenever a user attempts to verify using a smart card, the certification authority will be contacted and the digital certificate that has been issued to that smart card will be checked against the copy held by the certification authority. A certificate revocation list can be maintained which has information about all the certificates that should be rejected. If a smart card is lost, information about that smart card can be added to the certificate revocation list. Whenever a smart card that has been reported lost is used, the certification authority will reject that smart card from getting verified. In such a system, the owner of the smart card still regains control over the usage of the biometric template, without losing possession of the biometric template.

Security in any system is only as strong as its weakest link. Security technology can keep on advancing, but the human factor is a hurdle that technology cannot cross. Awareness and implementation of policies will help reap the benefits of advancement made by technology. If a

PKI system is used in conjunction with smart card technology, there should be policies laid down for issuance and reporting of lost smart cards. If an owner of the smart card does not report a lost smart card, the revocation system put in place breaks down. This human interaction with the system is a consideration that should be made whenever a security system is designed.

7.3.3 'Cancelable' Biometrics

One proposed solution to the problem of compromised templates is the introduction of predefined distortions of raw biometric data or extracted features [2]. When applied to image-based biometrics like fingerprints or facial recognition, this technique has the potential for enabling re-issuance of templates. Because the transformations are intended to be nonreversible, however, the possibility of converting a database from one specialized format to another may be limited. In addition, it is necessary at least in some cases to reverse the transformation prior to matching; this exposes the original biometric data to hacking during the matching process and may represent a significant vulnerability.

An alternative technique is based on the definition of unique, application- (or even transaction-) specific formats for biometric templates that prevent the unauthorized exchange of templates across multiple applications, yet provide a mechanism for authorized transfer across applications [3]. In addition they support the re-issuance of compromised templates without re-enrollment. Finally, the template matching operations are invariant across the transformations, so there is no need to return templates to a vulnerable "nontransformed" state in order to perform authentication.

A further simple approach to template revocation through cancelable biometrics is possible where the system employs a content-bearing biometric sample under the control of the user – see Section 5.6. Here, either the user (for privacy or security reasons) or the system administrator can decide that a change is necessary and in both cases any final necessary system inputs may be made through the systems administrator after the user re-enrolls based upon a different secret.

7.4 Sensor Spoofing

7.4.1 Spoofing Techniques

Biometrics leverage stable physiological and behavioral characteristics for the purpose of verification or identification [4]. If at any point these characteristics become easily mutable or transferable, one's degree of confidence in the system may be dramatically reduced. Spoof attacks on a biometric system are those in which an artifact is presented to a sensor for the purpose of being enrolled or recognized, or for the purpose of circumventing an enrollment or recognition process. Susceptibility of biometric systems to spoof attacks is a major concern for potential implementers.

Most tests of biometric system susceptibility to spoofing have been executed on fingerprint devices, not least because it is the only technology in which a variety of commercial products are readily available to end users. Known methods of spoofing certain fingerprint systems include the following:

- Using color-appropriate prosthetics created from molds taken of an enrolled finger;
- Using a high-resolution picture of the enrolled finger;

- Using the enrollee's latent fingerprints lifted via tape from a sympathetic surface;
- Using residual fingerprints left on the scanner and set in relief after the scanner surface has been sprayed with chemicals.

In 2002, Professor Tsutomu Matsumoto of Yokohama National University [5] in Japan conducted a test in which eleven optical and silicon fingerprint sensors accepted artificial fingers in at least sixty percent of attempts. Matsumoto's primary method of spoofing the systems was to create an impression of an actual fingerprint using gelatin derived from organic animal material.

7.4.2 Liveness Detection

Biometric systems attempt to counter spoof attacks through liveness detection – techniques by which systems determine that a submitted sample is from a living person. Methods of liveness detection are generally device-specific. For fingerprint systems, researchers are exploring spectroscopy and perspiration measurement, both of which have been shown to have some effectiveness in laboratory environments.

As for perspiration measurement, researchers at Clarkson University and West Virginia University devised a method of liveness detection that relies on certain optical, electro-optical, or solid-state fingerprint sensors [6]. These sensors have the capability to analyze the degree of moisture on a person's skin resulting from a live being's natural perspiration. By measuring expected changes in perspiration levels at intervals of zero, two, and five seconds, this system uses time-series detection to augment its liveness detection capability.

With respect to iris, each of the primary iris recognition vendors claims they have liveness detection capabilities, although their methods of liveness detection are proprietary and rarely, if ever, publicly disclosed. Professor John Daugman of Cambridge University, who pioneered the development of iris recognition algorithms, has delineated four overarching categories of countermeasures for iris recognition. They are:

1) Photonic and spectrographic countermeasures;
2) Behavioral countermeasures;
3) Analog physical attack countermeasures;
4) Digital replay attack countermeasures.

The first category, photonic and spectrographic countermeasures, is related to the spectroscopy techniques used with fingerprint recognition. Tissue, blood, fat, and melanin pigment in the eyes behave differently when they are interrogated by various wavelengths, and this fact can be leveraged in liveness detection. And 2D Fourier techniques can identify contact lenses with fake iris prints. A check for a red eye effect, the result of retinal reflection, can also be utilized.

The second category, behavioral countermeasures, is based on analysis of voluntary and involuntary behaviors, such as fluctuations in pupil size irrespective of lighting levels, detection of pupil movement and eye movement, and blinking. Future research may also explore the micro-movements that characterize live eyes.

The third category, analog physical attack countermeasures, can be used to detect high resolution photographs or contact lenses with imprinted iris patterns. These techniques may detect dot matrices and dyes used in some printing techniques, or they may detect the curvature of a contact lens relative to that of the iris. Analog physical attack countermeasures may also seek out Purkinje light reflections against the cornea, evaluating reflections present in live eyes – but not in photographs.

Liveness detection may be implemented by a combination of physical measures at the capture device where it interfaces with the human subject, and software implemented as part of the image acquisition process. It is unlikely that liveness detection will guarantee protection against sophisticated artifacts constructed to closely model human characteristics. The efficacy of the protection will need to be determined through a vulnerability assessment program. The barrier can be raised higher through the use of multi-mode biometrics (e.g. face and voice) or through multi-factor authentication such as biometric and PIN.

For other biometrics, liveness detection methods are typically behavioral. Facial recognition systems may require head movement, lip movement, or a change in facial expression. Voice recognition systems may ask users to recite a randomly generated phrase or alphanumeric sequence so as to avoid digital playback. A signature/sign system may ask for any one of a number of pre-enrolled secret signs – e.g. Mother's maiden name

The basic premise of technical counter-measures in biometric systems is to design and implement the system such that its security does not depend on the secrecy of the biometric features. To protect the authentication process, the biometric system must be able to detect and reject the use of a copy of a biometric sample instead of the live biometric sample.

7.5 Entropy / Strength of Function

Section 5 (in particular Table 4) of this document introduced a comparative analysis of authentication mechanisms based on characteristics ranging from technical to procedural; this section discusses entropy and strength of function which is a common characteristic used in comparing secrets based and cryptographic authentication mechanisms. Appendix A of the NIST Special Publication 800-63 provides a discussion on the entropy and strength of passwords. The discussion provides a clear analysis of the estimated "actual" strength of a password (depending on whether it is user-chosen or randomly generated). For example, a user-defined six character alphanumeric password with no dictionary checks (to determine if a known word has been used) has been assessed to have equivalent entropy of 14 bits. This means that to mount a brute force attack on such a system would require the generation and submittal of approximately 16,000 permutations of the six characters.

Based purely on required number of inputs, this might be assumed to be equivalent to a biometric system with a false match rate of approximately 1 in 16,000. However, to determine a more precise strength of function comparison, two additional complexities must be considered:

1. The difficulty of database acquisition. Although obtaining a database of 16,000 sample biometric characteristics is not impossible, templates are not necessarily readily available to an attacker. Generating 2^{14} 14-bit strings, however, is a simple coding operation.
2. The process of comparing a submitted biometric sample against a biometric reference in a biometric system is not a simple comparison operation, and typically requires significant processing power. This computational complexity must also be taken into account with respect to the computational complexity of password validation in a system in order to obtain true strength comparisons of these systems against brute force attacks.

Furthermore, the most fundamental benefit of a secure biometric system in comparison with a secure password-based system is that biometric characteristics are not transferable. Use of a secure biometric system provides an extension of the security perimeter from "something the user knows", to "something the user is". An individual can give away a password, regardless of its length. If all the liveness detection, biometric algorithm and other security components are in place, an individual cannot give another individual a biometric characteristic that will be accepted in the system.

It is well known that biometric template size is no real indicator of the ability of the system to discriminate between individuals. Biometric discrimination will depend on two different factors: Firstly, the degree of distinctiveness of the biometric feature among the population of likely users of the system; and secondly, the ability of the biometric system to uniquely and repeatedly separate these features. Additional, practical considerations also affect the results, including the acceptable rates of false rejection, and environmental conditions. It is sometimes possible to gain some theoretical view of the likely system discrimination potential, but this can currently only be validated through a program of practical performance testing with real users. Measurement of high discrimination capability inevitably entails the use of large test populations and this in turn places a practical limitation on the achievable accuracy of the test [7].

7.5.1 Component Approach

Statham suggests the concepts of raw and real entropy when determining relative strengths of function and its relationship to binding strength, which is the confidence that a person presenting an authentication credential is who they claim to be [8].

Real entropy consists of three components:

- Raw entropy
- Technical strength
- Human/procedural strength

Raw entropy: or discrimination is the ability of a mechanism to distinguish between individuals. This is the exploitation avenue most used for casual (low or zero-effort) attacks.

Technical strength: are exhaustion attacks against an authentication mechanism which exploit the vulnerabilities of that mechanism as well as indirect attacks against the supporting infrastructure (e.g., transmission paths, databases).

Human or procedural strength: include social engineering, "easy" secrets, failure to guard secrets, and corrupt users/administrators. This element reduces entropy sometimes to zero.

A detailed description of entropy and strength of function for passwords, hard tokens, and biometrics is shown below in Table 8.

Table 8 - Entropy and Strength of Function Description

	Discrimination	**Technical Strength**	**Procedural Strength**
Passwords	High - Large password space = high entropy	Strong - Long string = High entropy, very long time to exhaust - Cryptographically strong algorithms –can't be reverse engineered	Weak - Short passwords = low entropy - Easy-to-guess passwords – low/zero entropy - Written down = zero entropy - Divulged to colleagues = zero entropy - Vulnerable to social engineering = zero entropy
Tokens (physical)	Very High - Token store long "password"	Quite strong - Difficult to copy (physical barriers) - Very difficult to modify (physical & crypto barriers) - Attacks need considerable expertise and specialized equipment	Weak - Loss - Theft - (But at least you know that its missing!)
Biometrics	Medium-High (modality specific) - Entropy limited by FAR - (Not directly equivalent to PW entropy because you can't mount a simple exhaustion attack)	Medium - Spoofing - Reverse engineering of stored templates - Capture of stored images	Strong - Not reliant on human discipline - Human errors will not weaken the binding in the same way as for passwords and tokens

Based on the descriptions in Table 8, a side-by-side cross comparison is shown below in Figure 17. (It is noted that these represent relative figures of merit and that specific implementations may exhibit different characteristics. Your mileage may vary!)

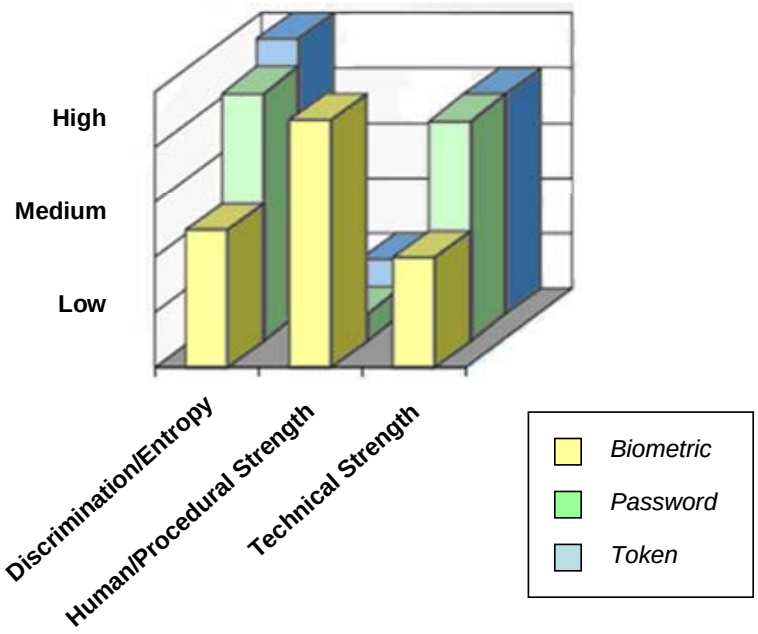

Figure 17 - Entropy and Strength of Function Comparison

Statham also provides an example of such a comparison for passwords and biometrics. Strength of function (SOF) relates to probabilistic mechanisms. For passwords, these maps to the probability of guessing the password, so the password SOF is defined by entropy (e.g., a 4-digit PIN has a raw entropy of 10,000 (10^4)). However, real entropy may be less due to restricted subsets, non-random choice, etc. Effective entropy is also reduced by multiple attempts.

How do we compare biometric entropy to password entropy? Is it a direct equality (e.g., FAR = PW raw entropy)? This makes no allowance for different potential retries in the two cases.

7.5.2 Raw Entropy

As Statham described above, the assumption of equating the raw entropy of guessing a password or PIN to that of the False Accept Rate (FAR) in a biometric system is not necessarily an equal one. The False Accept Rate (FAR) is an extension to the False Match Rate (FMR) described above in Section 4.3; with the added consideration that biometric matching algorithms contain thresholds which are adjustable and not solely based on the binary output of the FMR. Further explanation of this topic is shown below in Figure 18. The argument is that a "guessing" attack against a secret can be done simply by trying different combinations of characters until all of the possible combinations are tried, and somewhere along the way the secret will be found. This concept falls within the definition of raw entropy based on the fact that all possible combinations of information content (input characters) are considered. Applying the same logic of this assumption in conducting a "guessing" attack on a biometric system; an imposter would be improperly identified at the frequency of the FAR. For example, if a biometric system has a FAR of 0.01%, the assumption at hand would say that a random imposter has a 1 in 10,000 chance of being falsely accepted. Now equating the 1 in 10,000 probability back to PINs; this would be the same as a four digit PIN that has 10 possible characters (0-9) in each of the four placeholders (10 x 10 x 10 x 10 = 10,000).

The equal comparison assumption has three major discrepancies. The first and most obvious observation is that a brute force attack would normally only be focused on a single secret at one time. It is realized that increased computing power could allow attacks to take place at the same time on multiple secrets, or even in an iterative process, however this is beyond the scope of the comparison. Nonetheless, equating the entropy of a single secret to an entire biometric system is simply not the equal comparison. A more realistic example would be to evaluate all of the secrets in the system identifying the weakest one, or lowest entropy, to that of the FAR of the biometric system. A common concept used in security is that the system is only secure as the weakest link; this scenario would provide a better representation of system weaknesses side by side. Another alternative to equal comparisons would be to conduct a brute force attack on all of the fingerprints in the system individually. This would be similar to how an individual secret would be attacked using a brute force methodology. A detailed discussion of a brute force attack on a single fingerprint is included in the remaining paragraphs as it relates to the informational content contained in the fingerprint image. Sticking to the fundamentals of attacking fingerprints individually; fingerprints can be categorized in various ways. One such methodology that is widely used is to use the Henry System of Fingerprint Classification, which categorizes fingerprints into groups based upon ridge flow patterns, resulting in five classifications - Left Loop, Right Loop, Arch, Tented Arch, and Whorl [9]. Another method of categorizing fingerprint images is by which finger the image came from on the hand – Index, Middle, Ring, Little, Thumb. Overall, different fingerprint images will be tougher for an imposter to match than others based on the differences in characteristics, just as some secrets are harder to crack than others.

The second discrepancy with this assumption is the context surrounding the FAR for the biometric system. FARs are not a static value, which this argument may lead one to believe. The fact is FARs are a resulting value based on the threshold of the matching algorithm of the system. The matching threshold is a property that exists based on the fact that no two biometric samples should ever match exactly the same. Changes in the sample acquisition environment, user behavior, and also orientation with the sensor are all factors that will result in variations of biometrics samples just to name a few. On the opposite side of the matching threshold is the False Reject Rate (FRR). The False Reject Rate (FRR) is an extension to the False Non-Match Rate (FNMR) described above in Section 4.3.4.4; with the added consideration that biometric matching algorithms contain thresholds which are adjustable and not solely based on the binary output of the FNMR. Further explanation of this topic is shown below in Figure 18. The negotiation of the matching threshold and the resulting FARs and FRRs is a tool that biometric system designers and implementers can adjust to suit different needs and applications of the system. For instance, if the threshold is made to be more stringent, then the system will block more imposter users from being falsely accepted, but also will falsely reject a greater number of genuine users. Conversely, if the threshold is made to be less stringent, then a grater number of imposter users will be falsely accepted; but the system will also accept a greater number of genuine users that may not otherwise be accepted because they are in an extreme population that has problems using the system. The relationship between matching threshold, FAR and FRR is depicted in Figure 18.

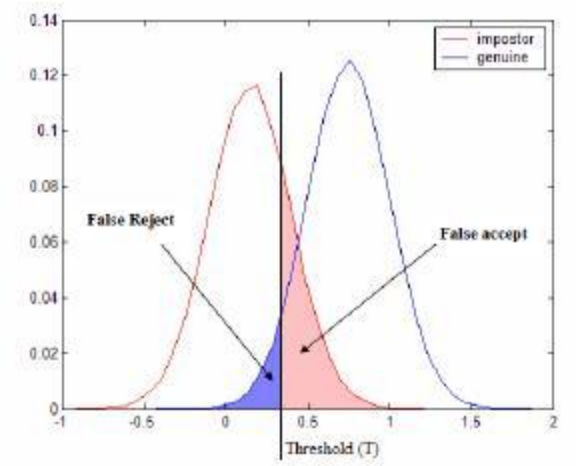

Figure 18 - Matching Threshold Relationships [18]

Because FARs can not be considered a blanket attribute for the system and should not be documented as a single value, it does not make sense to use them in the manner outlined in the original assumption for comparing biometrics to secrets.

The third discrepancy is the fact that the original argument does not account for the amount of actual information that is contained in the biometric. The entropy of secrets is directly tied to the informational content that comprises the secret. That being as the variation in number and represented values of input characters increases, so too does the key space and thus the entropy of the secret. In order to accurately compare these two types of authentication mechanisms, biometric entropy too must also be evaluated based on the key space and informational content of the sample.

One of the first and most well known works that addresses biometric entropy from the standpoint of key space was published in 2001 [10]. This approach focused on a hypothetical brute force attack against minutiae based fingerprints. The first step in this process was to define the total number of possible sites that minutiae could lie in a fingerprint image taking into consideration:

- The dimensions of the image in pixels
- How many pixels a standard minutiae point would consume
- The number of orientations allowed for ridge angle of the minutiae points
- The number of minutiae points in a reference template that is attempting to be matched against

Using the aspects noted above, a linear relationship was made between the amount of minutiae required to be matched and level of information contained in the fingerprint in the form of a bit value. Based on this method, a fingerprint system requiring 25 minutiae points to be matched would have 82 bits of information. This equates to a 16-character nonsense password (such as “m4yus78xpmks3bc9”) [10]. In the years since the initial publishing of their work, fingerprint systems, in particular fingerprint images, have expanded greatly. As technology has advanced, sensors have become more robust in the image acquisition process. At the time of publishing, Ratha et al. used the dimensions of 300 x 300 pixels for a fingerprint image. Currently, there are many fingerprint sensors that operate at 500 dpi or greater which would result in a fingerprint

image being greater than 300 x 300 pixels. All things considered, the method proposed by Ratha et al. takes a much more scientific and comprehensive approach to equating raw biometric entropy based on key space and information content than that of using the FAR of the biometric system.

7.5.3 Real Entropy

Again looking at the 4-digit PIN with a raw entropy of 10,000, the real entropy is actually about 5,000. Assuming 100 retries (over a period of time), chance success is 1 in 50, or SOF Basic level.

A biometric with an FAR of 1% has a raw entropy of 100. The real entropy is 100/<the number of attempts possible>, which yields a similar SOF as the 4-digit PIN.

7.6 Peer Review Methods for Biometrics

Fundamentally, the cryptographic community and the biometrics community approach peer review from very different perspectives. These differences, along with a comparison with other aspects from the two communities, were summarized in Section 5.5. From William Burr's presentation at the 2004 Biometric Consortium [12], there is a "culture clash" between the two communities. The cryptographic community is very adversarial and believes they have done a good job if they can publish an attack that can defeat a particular algorithm. They believe the algorithms should be completely open so everyone knows how the process works and the security comes as a result of the secretive key chosen for each individual case.

Public peer review of cryptographic systems is a popular practice for proving the strength of the algorithm or methodology being tested. If a cryptographic methodology is in fact able to be broken, tremendous publicity often ensues describing the details of how it was broken and the amount of resources needed to successfully break it. Generally speaking, there are three important aspects of a cryptographic system as it relates to the peer review process. These are the encryption and decryption functions, the cipher text, and the key. Cryptographic systems rely on the secrecy of a key; so in order to effectively "break" the system, the encrypted information must be revealed without any knowledge of the key. The other two aspects of the system are made completely open so that the encryption-decryption functions do not provide a single point of failure.

In comparison, a biometric system also has three important aspects that are analogous to a cryptographic system: the biometric sample, the biometric template or reference, and the matching algorithm. As it stands right now, the security of the biometric system is reliant on the strength and secrecy of the matching algorithm. The sample provided by many live-capture biometric systems is considered non-secretive information. The template or reference corresponding to that biometric sample should also be considered non-secretive as a template or reference could be created using the sample. In this sense, the biometric sample and its associated template should be considered non-secretive and thus are the two open parts of the system. It should be noted that the process of creating a template and the data it contains is still considered secretive information.

William Burr also claims that, "Cryptographers believe that a dental technician has the skills and materials to construct a copy of a fingerprint that will fool most fingerprint readers." However, it is important to keep in mind that with a biometric system, the success of any attack needs to be viewed in the context of the entire system, including an analysis of the tradeoffs between risk, security, convenience, and user alternatives. For example, the best cryptographic system in the world is useless if the user community writes down their passwords on yellow sticky notes and affixes them to their monitors. The cryptographic community is proud when they break a biometric system using fake fingerprints made from common materials [5]. While certainly these findings will help improve current and future biometric systems, it does raise the question of how easy it is to actually capture the biometrics for people who are already enrolled in the system, and what skill set is needed in order to create falsified biometric data that might work.

For example, in the case of trying to create false but valid fingerprints, the question becomes how much interaction is needed by the enrolled (i.e., known good) individual to effectively fool the fingerprint sensors. If the individual cooperatively submits their fingerprint into a mold or other means for the spoofing attempt; then biometrics are not being compared equally to the peer review process of cryptographic systems. It is significantly harder to extract a fingerprint which is capable of being used to spoof a sensor from the surface of a desk, for instance. This type of peer review would be non-cooperative. Beyond the difficulty of effectively retrieving a latent print, more variables also come into play, such as:

- To whom does the extracted fingerprint belong?
- From which finger does the print come?

This type of "user-cooperative" biometric peer review is not at the same level as peer reviews of cryptographic systems and thus is not an apples-to-apples comparison of the relative strengths of biometrics. In some ways, the effort needed to successfully fool sensors can be viewed as an added advantage because the biometric data can be known; but still not be used to break the system.

First of all, it is not always as easy to obtain a copy of the true biometric feature as it may seem. Let's use fingerprints as an example. In this case, once a target has been identified, the attacker must obtain a latent fingerprint. To do this, the print must be lifted from a suitable surface. This surface must be smooth, dry, and free from contaminants and background that can interfere. Then, the attacker must be able to distinguish the print of the chosen victim from among any other that are present on the surface. He must also select the print that corresponds to one of the digits that the victim has enrolled in the system (i.e., lifting the left thumb print will not be of use if the victim has enrolled his right middle finger). The print must also be a good, flat, complete (whole) print without any smudging, smearing, or distortion.

Second, the attacker must translate the perfectly lifted print into an artifact (e.g., latex mold). To do this, he must create a detailed etching of the ridge surface from which a mold can be manufactured, and the molded "fake finger" can be formed.

Lastly, the attacker must have access to the remote workstation/authentication point and opportunity to perform the attack. Presumably, the attacker has already obtained the User ID of the victim by another means (a requirement for a 1:1 verification system).

There remains some debate as to the secrecy of biometrics, at least for certain biometric modalities. While most biometrics (samples, etc.) are not secret, strictly speaking, they can be hard to capture by someone else. However, in the view of SP800-63, biometrics do not constitute secrets suitable for use in remote authentication:

When considering peer reviews for biometrics, these same principles of starting with no previous knowledge must apply in order to be compared on the same level. Whether or not it is believed that biometrics are secrets, the worst case scenario must be assumed that they are not secretive and can be obtained without voluntary assistance from the individual.

In contrast, the biometrics community is just the opposite – it is very test-oriented and market-driven with intellectual property rights at stake. While these two approaches may seem completely incongruent, they derive from fundamentally different factors. Cryptography is algorithm-based and completely repeatable and deterministic. That is, given a particular algorithm and its necessary data, the cryptographer will always get the same results. On the other hand, all biometrics are based on one or more statistical techniques with noisy input data from the biometric capture process. While any given biometric algorithm will process the same input in the same way, the probability of capturing an identical sample of an individual's biometrics is extremely low. For example, imagine the difficulty in capturing the exact same image of someone with a digital camera. With subtle changes in ambient lighting and the various auto-compensation mechanisms built into the camera, it is effectively impossible.

Biometric algorithms are more in the realm of statistical pattern matching, signal analysis, and classification and communication theory rather than the non-statistical algorithms that cryptographers use. This is not to say that cryptographers do not use statistical approaches. However, they do so in order to break a cryptographic algorithm, not as the basis of the algorithm itself.

Because all biometrics are statistical in some way, there will always be some probability of generating some type of error (for example, false match, false non-match, failure to enroll, etc.). This is true even of biometric algorithms and capture devices that are completely open and in the public domain. The cryptographic community is accustomed to dealing with systems that do not have error rates of any kind.

Because of the expense in developing and maintaining biometric algorithms and capture hardware, the financial marketplace demands that biometrics vendors give proper consideration to intellectual property rights. Consequently, the best algorithms for the different biometric modalities are kept private and proprietary and may be disclosed only when sufficiently protected by patents and the like.

To deal with the statistical nature of biometrics plus the market tendency for algorithmic secrecy, the biometrics community relies heavily on public testing of their systems, more or less in a black-box configuration with standardized input data, and prototype installations by evaluation customers.

Certainly, the adversarial approach by the cryptographic community can be beneficial to the biometrics community in several ways. For example, it can help ensure that claims made by biometric vendors are valid and can be substantiated. Furthermore, adversarial attacks can help to discovered new ways of breaking a biometric system so that these problems can be addressed and fixed.

Biometrics is just one piece of a system that can help secure it and maintain a level of trust in the users of the system. However, for systems and environments that have increasing security requirements, it is much more likely that multiple authentication methods will be used. Biometrics is the only one that has a chance of tying an individual to a credential or a token.

Because of its statistical nature, biometrics will always need to be analyzed, reviewed, and evaluated in at least a partially different way from cryptographic systems. The biometrics community has responded to this challenge by drafting and using standardized testing and reporting protocols. This approach will continue to be used until a better one is proposed, either within the biometrics community or by an external group such as the cryptographic community. Unless the cryptographic community can come up with a non-statistically-based way to guarantee the integrity of the relationship between an individual and a token or credential or a claim of identity, biometrics will continue to be used for this important purpose.

7.7 Privacy

Although privacy is not a security matter per se, it is an important consideration that certainly affects decisions regarding the deployment of biometric technology.

First of all, biometric data is considered personal information and is therefore sensitive in nature and covered by a variety of laws and regulations, particularly when used in public (government) sponsored systems.

Some users of biometric systems are concerned about misuse of their personal information, including their biometric data. For example, individuals have expressed concern that the company capturing their fingerprint may submit the print to a law enforcement agency for a criminal history investigation without their knowledge. However, all deployments of biometric technology should be implemented in accordance with local jurisdictional privacy laws and regulations. As such, the collector should fully disclose to the subjects the intended purpose of any information collected by or for the biometric system, and that its usage is limited accordingly. Note further, that to be authorized to request a criminal history investigation be performed on an individual; the submitter must obtain certification from the FBI to attest that they have a legitimate purpose for making such a request.

The following principles should be followed:

- Only the minimum amount of data should be collected
- Biometric data is captured for a specific purpose
- The user is notified of and consents to the data collection and its use (informed consent)
- The planned and actual use of the data is consistent with the purpose for which it was originally collected

- A retention period for the data is established and the data destroyed after that period (or when the user account is terminated)
- A sharing/selling policy that data shared with a second party cannot be shared with a third party unless explicitly agreed to beforehand
- Data is protected from unauthorized access (due diligence) and access is limited to those with a need to know

Additionally, in some cases (perhaps at Level 1, for example) the use of "anonymous" biometrics may be appropriate. That is, all that is known is that the biometric belongs to an authorized user (or a role), not the identity of that user (see SP800-63, section 7.2).

The International Biometric Industry Association (IBIA), in 1998, published a set of privacy principles [14] to which its membership are expected to adhere. These generally follow the above recommendations and are in alignment with the Code of Fair Information Practices (CFIP) outlined in the Federal Privacy Act of 1974. The International Biometrics Group has also done work in this area and has published some of this as the BioPrivacy initiative. Additionally, a study report regarding this and other cross jurisdictional and societal issues of biometric implementations is in progress within ISO/IEC JTC1 SC37 WG6.

Privacy is a hot topic in our culture and media today. This leads to "perceived" privacy concerns that the industry must be sensitive to in how it handles biometric data, since "perception <really> is reality". The success of deployed systems is highly dependent on user acceptance and privacy protection is a critical factor in that acceptance.

There is a truism that "You can have security without privacy, but you can't have privacy without security." This refers to the fact that the confidentiality of biometric data must be protected to ensure privacy, and that security mechanisms are required in order to provide this protection. Due diligence to ensure that biometric data is protected during transmission and storage and that access to this data is controlled is needed and are traditional security roles. Security is making sure the data is available for authorized users and protected from non-authorized users. Privacy is limiting the pool of authorized users to those who not only have a need to know, but who's purpose in getting the data fits the original reason for collecting the data in the first place.

8 Threats and Vulnerabilities for Biometric Authentication

Biometrics have a powerful potential to provide added security for a variety of applications. Already biometrics have been deployed to protect personal computers, ATMs, credit card transactions, electronic transactions, airports, nuclear facilities, and international borders.

Yet, while biometrics may improve security in a plethora of environments and serve many purposes, biometric systems, like any other security system, have vulnerabilities. The increasingly high profile use of biometrics for security purposes has provoked new interest in researching and exploring methods of attacking biometric systems.

8.1 Biometric Attacks

This section addresses biometric device and system vulnerabilities. Attacks on biometric devices and systems can be grouped into four categories:

1. Attacks during enrollment
2. Attacks at the input level;
3. Attacks at the processing and transmission level;
4. Attacks on the backend/storage level.

8.1.1 Enrollment Attacks

Inherent in the practical use of biometrics for E-Authentication is their binding to one's identity. Although the concept of an Identity Management System lies outside the scope of this document, from a biometric enrollment standpoint because of the essential binding requirement, the identity proofing process is a critical related function. Trust in this process of vetting a person's claimed identity, confidence in the validity of associated documents, and reliability in the authenticity of issued electronic credentials taken together provide the very underpinning of biometric based E-Authentication. Examples of threats to identity proofing include: (1) Use of forged documents to verify a claimed identity, (2) Collusion with corrupt personnel having system access and (3) Electronic attacks to impersonate legitimate system users and thereby gain electronic access to the ID application, proofing process and issuance system.

Countermeasures to these Identity Proofing threats include:

1. Enforced separation of roles and duties of those involved in the processing, approval and credential issuance process.
2. Close inspection of documents for forgery or tampering and use of third party substantiation; for example, use of written inquiries.
3. Electronic system security protection – strong access controls, data encryption, firewalls etc.
4. Strong issuance controls which confirm the user at time of credential issuance and which preclude manual modifications to personalization data.

Primary vulnerabilities during enrollment of a person's biometrics such as fingerprints, iris and facial features include:

1. Enrollment of a person's valid biometric(s) with a created or substituted identity. In this scenario, a person uses/enrolls their own biometrics under a false or assumed identity which subsequently allows that person to gain unauthorized access to and conduct eCommerce transactions and other logical and/or physical assets such as computers, networks, databases, applications and facilities.
2. Enrollment of substituted or swapped biometrics (not their own) along with a valid identity which subsequently can be used by a third party to masquerade and gain access to eCommerce systems and/or other logical or physical assets.
3. Enrollment of substituted or false biometrics (e.g. a "gummy bear fingerprint") with a false or assumed identity which can later be used to gain access to eCommerce systems and/or other logical or physical assets.
4. Enrollee collusion with the enrollment operator. In this scenario, any of the above can be facilitated, as well as, unauthorized entry of or modifications to system data records or input thereto.
5. External based attacks against the Enrollment Station and/or other system components it communicates with. Examples include spoofing, sniffed transmissions, Man-in-the-Middle, and Replay.

Countermeasures which mitigate against these threats during Enrollment of Biometrics include:

1 Observed enrollment of biometrics instead of un-observed self-enrollment
2 Identity check/confirmation of the applicant enrollee at time of enrollment
3 Remote system and enrollment station network protection and access controls, secure point-to-point encrypted communications channel(s)
4 Enrollment Station device level firewall, and detection systems of unauthorized modifications to all relevant data records and electronic file systems.

8.1.2 Input Level Attacks

The primary input-level attacks, vulnerabilities at the point of sample acquisition and initial processing, are spoofing and bypassing.

While spoofing is the most frequently-cited input-level vulnerability, other input-level vulnerabilities may be just as problematic, such as "overloading." "Overloading" is an attempt to defeat or circumvent a system by damaging the input device or overwhelming it in the attempt to generate errors. This is also sometimes called a buffer overflow attack for other security mechanisms. An example of this type of attack for a biometric system would be the rapid flashing of bright lights against optical fingerprint sensors or facial recognition capture devices can disrupt their proper functioning. Silicon sensors can be easily damaged by short circuiting them or dousing them with water.

Because many biometric systems rely on sensitive equipment that can be overloaded relatively easily, users may have opportunities to induce device or system failure. Systems must be designed such that, if overwhelmed, basic functions must not fail. And when biometric devices

can no longer serve their intended function, fallback processes must be defined and enforced. A person who causes a biometric system to fail may be doing so knowing that, as a consequence, an unguarded door may be used as a temporary alternative means of entry. Security systems must account for the potential functional failure of biometric systems and devices by means of adequate backup measures.

8.1.3 Processing and Transmission Level Attacks

Though input-level attacks are an obvious illustration of biometric system vulnerability, attacks at the processing and transmission level also deserve close attention.

As many biometric systems transmit sample data to local or remote workstations for processing, it is also imperative that this transmission be secure, lest the transmission be intercepted, read, or altered. Most biometric systems encrypt data in transit, but not all applications and devices lend themselves to encryption. Security techniques such as encryption are often seen as deployer-specific aspects of system design. While certain standards do treat encryption techniques, notably the X9.84 standard utilized by financial services institutions, standards such as BioAPI are encryption-agnostic.

Deployers need to assess the degree to which sample data might be exposed in transit or during storage, and they need to define applicable system security techniques and best practices. Taken as a whole; anti-spoofing measures, encryption of data in transmission, and applying appropriate fallback techniques are all critical aspects of biometric system security. These techniques can be further enhanced through the introduction of multi-factor authentication and randomization.

Multi-factor authentication can take two primary forms: the use of multiple biometrics or the use of biometrics in conjunction with smart cards and PINs. Both methods reduce the likelihood of an imposter being authenticated. Spoofing also becomes more time consuming and challenging when multiple body physiological or behavioral characteristics need to be copied and imitated. Impostors for whom a biometric matches an enrolled user are unlikely also to match with respect to a secondary biometric.

Adding randomization to the equation also adds security. Verification data, for example, could be randomized, such as asking for three fingerprints one day and a different combination of two fingerprints the next day. Additionally, where time provides, designers of biometric technologies and systems should explore random or cued challenges. That is, even if a person correctly authenticates once, the system might still challenge the user to re-authenticate to help increase its confidence that the biometric data submitted is genuine.

Cued challenges could also be paired with certain behaviors causing alarm – such as an uncommon stillness, lack of movement, or change during the acquisition of biometric data. Technologies can still bear further development and enhancement for monitoring and sensing micro-movement. Or perhaps aggressive challenges could be utilized in conjunction with measurements of intelligent response time. For example, voice verification biometric systems could measure the time it takes for a prospective entrant to read back a randomly generated pass phrase in order to try to fight playback attacks pieced together from various recordings. If the response time exceeds a minimum threshold or varies significantly from an average time

captured over a series of sample submissions at enrollment, the biometric system could issue a challenge and require recitation of a new pass phrase.

Finally, in conjunction with multi-factor authentication and randomization, vendors and researchers should explore taking advantage of internal or subcutaneous characteristics. By focusing on biometric aspects that are difficult to observe, capture, and duplicate covertly, security can thus be enhanced.

However, regardless of how well one tries to secure a biometric system, failures will inevitably occur. It is therefore critical that attention not only be paid to preventing breaches, but also to handling breaches that have occurred. A recently-publicized technique to mitigate the impact of certain system breaches is the concept of cancelable biometrics. IBM's cancelable biometrics solution uses algorithms to distort an image proffered and records the distortion into its generated templates [2]. The original image is never stored anywhere. The idea is that if a thief steals the template with the distortion on it, that particular distortion can be eliminated from the list of access-approved users, and the legitimate user can resubmit their original biometric data to generate a new distorted template. As long as the algorithms that generate the distortions are carefully protected and ideally varied from company to company or even system to system, this solution may be highly conducive to containment and resolution of a breach.

The solution, however, is not foolproof. If the original image is captured, it could theoretically be re-enrolled to generate a new, distorted template. Nevertheless, the creation of cancelable biometrics is a step in the right direction. If the biometrics community continues openly and aggressively to identify its weaknesses and to pursue methods of strengthening them, the entire international community will all benefit tremendously.

8.1.4 Back-end Attacks

The previous two sections have described input level and transmission level attacks. Ensuring integrity and protecting back-end subsystems is important in distributed biometric systems. Assuming that the back-end consists of a matching subsystem, or a decision subsystem, or a combination of both attacks on the back-end will mainly be targeted at modifying the matching or decision subsystem or compromising integrity of stored templates.

Attacking the template storage database is the most apparent type of back-end attack. The threat of unauthorized modification or replacement of stored templates can result in false accepts or false rejects depending on the motives of the attacker. If an attacker can find a way of injecting templates directly into the storage database then the attacker could introduce him/her into the system without following the appropriate enrollment procedures. The attacker could also hijack the identity of an authorized individual by replacing the original template with their own template, thereby still preserving privileges linked to the authorized individual. If a template is compromised, it could be reused in a replay attack. Although circumventing replay attacks addressed is addressed in the previous section, compromise of stored templates is one of the most important threats that should be considered when designing a distributed biometric system. These kinds of attacks can be prevented by using encryption and data integrity (hashing) methodologies. Applying common database security methodologies can also increase the level of difficulty for the attacker.

An attacker could modify or replace the matching subsystem or the decisions subsystem so that it gives an output as desired by the attacker. This is a serious threat in a networked environment. The integrity of the sample is not relevant in such an attack, and the authentication process can be compromised without attacking the input subsystem or transmission process. This kind of an attack can be circumvented by applying security methodologies like checking code integrity, and principles of building trusted systems.

A denial of service (DOS) attack targeted at the back-end subsystems is also a very realistic threat. Overloading the processing units of the back-end subsystem with excess traffic could lead to unavailability of services. DOS attacks have received a lot of attention in media over the last few years and it should be considered a very real threat to biometric authentication systems also. Traffic analysis and traffic monitoring are commonly used methods to thwart DOS attacks.

Along with technical threats, there are also policy related challenges that should be considered. Collusion between a malicious attacker and enrollment center could allow the attacker to enroll in the system using a stolen or a false identity. Although this threat is not focused only on the back-end subsystems, a properly formulated policy involving the front-end and back-end subsystems should make such attacks harder to perpetrate.

If template adaptation is deployed, this also presents a possible back-end attack. The greatest threat to template adaptation is an impostor with a similar biometric sample (e.g., a close, same-sex relative) will exploit the adaptation function to adapt the model in the direction of the impostor's biometric data. The most effective methods for preventing this kind of attack include establishment of a high threshold for adaptation or a high overall score derived from biometric verification plus other authentication factors (e.g., challenge-response, caller ID or other biometric input).

8.2 Threat Modeling

8.2.1 Vulnerable points of a biometric system

Using the general verification model previously introduced as Figure 8, points of possible attack can be identified. These are shown in Figure 19 and fall into 4 categories –

- Attacks during enrollment of one's biometrics and their binding to one's confirmed identity [Attack points 12 and 13].
- Attacks during processing/interaction [Attack points 1,3,5,9,11],
- Attacks between stages (when the biometric data is in transmission) [Attack points 2,4,6,8,10], and
- Attacks on the biometric data when it is at rest (in memory or in storage) [Attack points 1,3,5,7,9,11].

Note that depending on architecture and design, some of the steps may not be present, may be combined, or may occur within the same physical component (thus perhaps eliminating a transmission path). Therefore, certain attacks may be possible in one architecture, but not in another.

Threats and countermeasures for each of these possible attack points are identified in the next section.

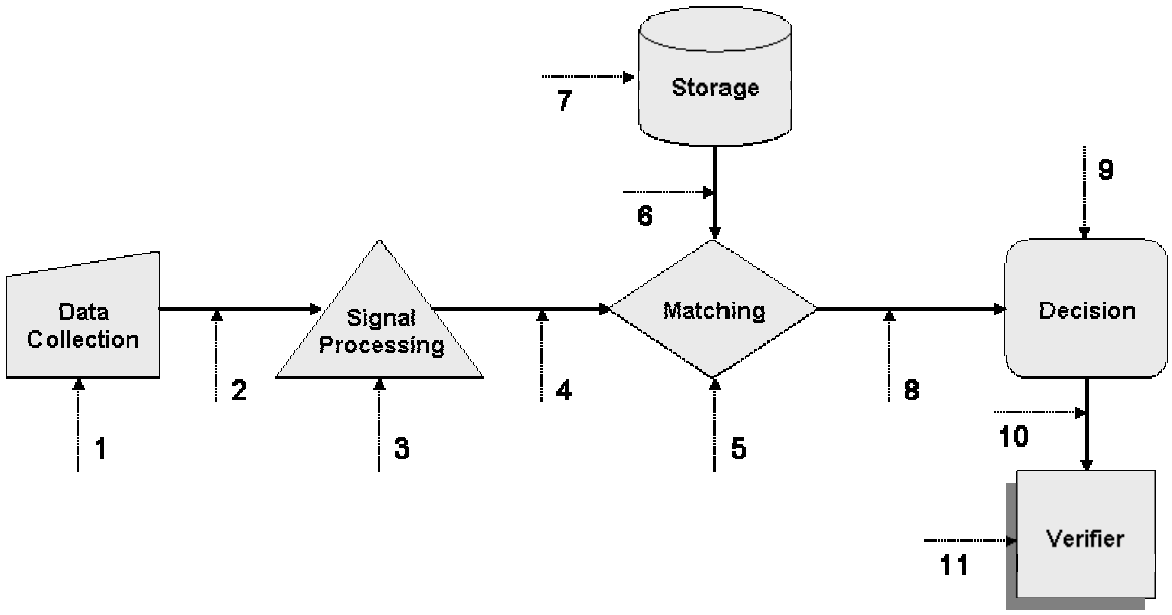

Figure 19 - Biometric System Threat Model

8.2.2 Threats and Countermeasures

Threats against the components and paths identified in Figure 20 are summarized in Table 9 below.

Table 9 - Biometric Threats and Countermeasures

Location	Threats	Countermeasures
1 Data Collection	Spoofing	• Liveness detection • Challenge/response
	Use of un-trusted device (Device substitution)	• Mutually authenticate/use symmetric key or asymmetric key
	Overloading/Flooding (Denial of Service)	• Rugged devices
2 Raw data transmission	Eavesdropping attack	• Transmit data over encrypted path/secure channel
	Replay attack	• Mutually authenticate/use symmetric key or asymmetric key • Digitally sign data • Utilize Timestamp/Time to Live (TTL) tag

		• Nonces (with MAC)
	Man in the middle attack	• Bind biometric to PKI certificate • Transmit data over encrypted path/secure channel
	Brute force attack	• Time out/lock out policies
3 Signal Processing	Insertion of imposter data	• Use strong tested algorithms
	Component replacement	• Signed components
4 Processed data transmission	Eavesdropping attack	• Transmit data over encrypted path/secure channel
	Replay attack	• Mutually authenticate/use symmetric key or asymmetric key • Digitally sign data • Utilize Timestamp/Time to Live (TTL) tag • Nonces (with MAC)
	Man in the middle attack	• Bind biometric to PKI certificate • Transmit data over encrypted path/secure channel
	Brute force attack	• Time out/lock out policies
5 Matching	Insertion of imposter data	• Use strong tested biometric algorithms
	Component replacement	• Signed components
	"Guessing" (FAR attack)	• Use strong tested biometric algorithms • 1:1 matching • Multi-biometric/multi-factor
	Manipulation of match scores	• Debugger hostile environment
	Hill-climbing	• Coarse scoring • Trusted sensor (Mutual authentication) • Secure channel

6 Template retrieval	Eavesdropping attack	• Transmit data over encrypted path/secure channel
	Replay attack	• Mutually authenticate/use symmetric key or asymmetric key • Digitally sign data • Utilize Timestamp/Time to Live (TTL) tag • Nonces (with MAC)
	Man in the middle attack	• Bind biometric to PKI certificate • Transmit data over encrypted path/secure channel
7 Storage	Database compromise (reading template, replacing template(s), changing bindings)	• Hardened server • DB access controls • Sign templates, Store encrypted templates • Store template on smart cards or other device.
8 Matching score transmission	Hill climbing attack	• Coarse scores • Trusted sensor (Mutual authentication) • Secure channel
	Manipulation of match score	• Secure channel • Mutual authentication between matcher and decision components
9 Decision	Hill climbing attack	• Coarse scores • Mutual Authentication • Secure channel
	Manipulation of threshold setting	• Protected function (access control) • Data protection
	Manipulation of match decision	• Debugger hostile environment
	Component replacement (“yes machine”)	• Sign components
10 Communication to application	Eavesdropping attack	• Transmit data over

		encrypted path/secure channel
	Manipulation of match decision	• Transmit data over encrypted path/secure channel
11 Application (verifier)	Malicious code	• Conform to standards (BioAPI, CBEFF) • Code signing

A brief description of each of the above named threats is provided below in order of occurrence.

Sensor Spoofing. The presentation of an artificial or non-live artifact to the biometric capture device in lieu of a legitimate biometric feature. (This is discussed in more detail in Section 7.2)

Untrusted Device. Substitution of a legitimate biometric capture device with a simulated, modified, or replacement unit.

Device Overloading. Presenting inputs to the device in such a way as to cause it to operate incorrectly or not at all (e.g., input flooding, interference, power surges, harsh environment).

Eavesdropping. The covert listening/recording of biometric data transmissions, possibly for use in a subsequent attack.

Replay Attack. Insertion of biometric authentication data (i.e., legitimate data obtained illicitly at an earlier time) into a transmission path as part of an authentication protocol.

Man-in-the-Middle. An attacker is able to read, insert and modify messages between two parties without either party knowing that the link between them has been compromised.

Brute Force Attack. Exhaustive presentation of a large set of biometric inputs to the authentication system in an attempt to find one that successfully works (matches) a legitimate enrollment record.

Component Replacement. Substitution of one of the (software) components in the authentication path in order to control its behavior (e.g., always providing a desired output, such as a given template, match score, or decision).

"Guessing". Capitalizing on a system using a biometric matching algorithm with a high false match rate (FMR), thus providing a higher than desirable likelihood that an arbitrary biometric feature presented to the system (a guess) will match.

Score Manipulation. Capturing and changing the value of a match score (in memory or during transmission) before it can be acted upon by the decision process.

Hill Climbing. Use of returned match score information to finely and incrementally alter the raw biometric input to achieve progressively increasing scores until the decision threshold is eventually exceeded. (This is a specific concern with unsupervised systems.)

Database Compromise. Access by an attacker to the stored biometric template (or set of templates) such that it can be read, modified/substituted, or its bindings (identity association) changed.

Threshold Manipulation. Accessing and changing (lowering) the value of the matching decision threshold, such that submission of an illegitimate biometric sample is likely to result in a successful match decision.

Decision Manipulation. Capturing and changing the value of a decision (in memory or during transmission) prior to granting of access.

Malicious Code. Insertion (presence) of illegitimate software within or interfacing to one of the components in the authentication path which alters the process/results.

8.2.3 Enrollment Threats

In addition to the threats identified for the relevant biometric functions (Data Collection, Signal Processing, and Storage) above, the enrollment process also involves an identity proofing component. The threats to the identity proofing portion of a biometric enrollment process are not unique to biometrics and are described in Section 7.1 of SP800-63. To this end, Figure 19 can be extended as shown below in Figure 20:

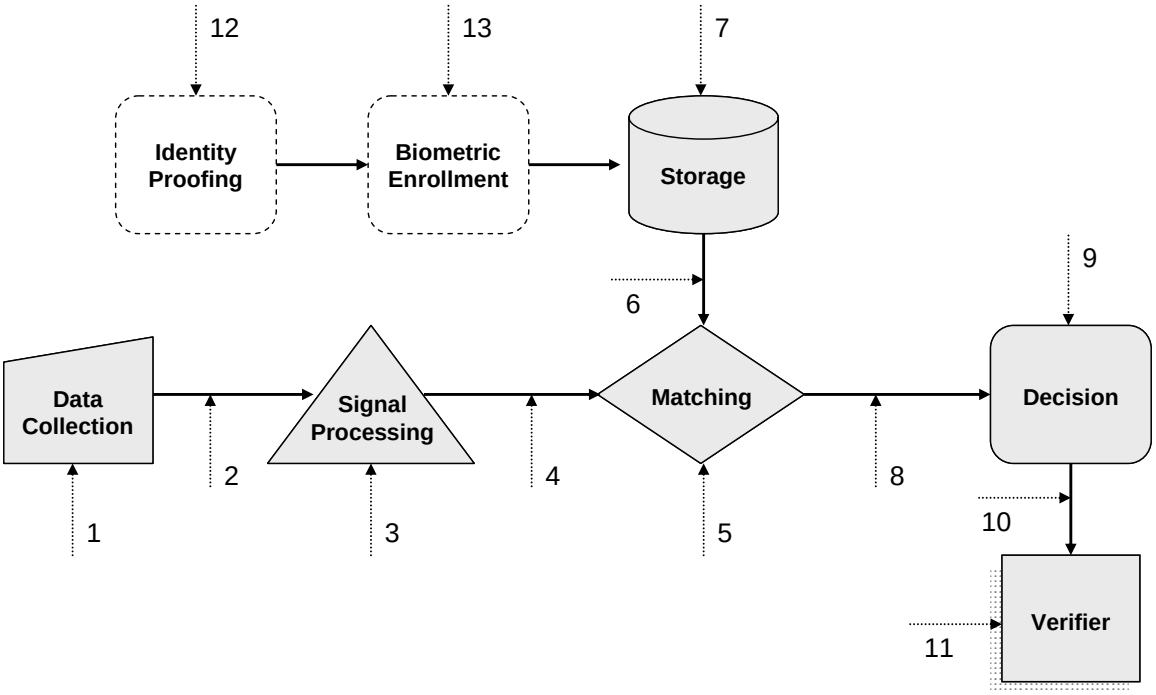

Figure 20 - Enrollment System Threat Model

Threats identified for the two additional steps (12 and 13) are delineated below in Table 10.

Table 10 - Enrollment Threats and Countermeasures

Location	Threats	Countermeasures
12 Identity Proofing	Forged documents	Close document inspection for authenticity, alterations etc. Independent inquiries and confirmation
	Collusion/Corrupt processing personnel	Separation of roles & duties, audit trails
	Unauthorized electronic or manual access to obtain, insert, modify or change data input and records	Strong system access controls, firewalls, encryption of data, chain of custody for records/modifications, protected storage repositories
13 Biometric Enrollment	Valid enrolled biometric but bound to false identity	Check of presented identity documents with those submitted during identity proofing process.
	Valid identity but bound to false biometric(s)	Observed enrollment of biometrics
	Unauthorized Access to Enrollment Station(s) and/or related data base	Network& Enrollment Station Access controls, protected transmission links including data transiting, and enrolled user data base protection l

8.2.4 Employing Countermeasures

There exist several security techniques to thwart attacks at these various points. For instance, finger conductivity or fingerprint pulse at the sensor can stop simple attacks at point 1. Encrypted communication channels can eliminate at least remote attacks at point 4. However, even if the hacker cannot penetrate the feature extraction module, the system is still vulnerable. The simplest way to stop attacks at points 5, 6, and 7 is to have the matcher and the database reside at a secure location. Of course, even this cannot prevent attacks in which there is collusion. Use of cryptography can prevent attacks at transmission and storage points.

The threats outlined in the figure above are similar to the threats to password-based authentication systems. For instance, all the channel attacks are similar. One difference is that there is no “fake password” equivalent to the fake biometric attack at point 1 (although, perhaps if the password was in some standard dictionary it could be deemed “fake”). Furthermore, in a password- or token-based authentication system, no attempt is made to thwart replay attacks (since there is no expected variation of the “signal” from one presentation to another). However, in an automated biometric-based authentication system, one can check the liveness of the entity originating the input signal.

Clearly there are benefits and threats to using biometric technologies for e-authentication. When compared to conventional authentication mechanisms such as PINS, Passwords, and physical Tokens; biometrics are stronger in some points and weaker in others. Based on this information, tables later in this document have been developed to show where biometric use is appropriate based on the assurance levels set forth in M04-04 and SP800-63.

Descriptions of some of the countermeasures listed in Table 11 are provided below. Those that are common/standard IT security practices are not herein defined.

Liveness Detection. Techniques by which systems determine that a submitted sample is from a living person. (See 7.3.2.)

Challenge/Response. A protocol in which the user is challenged to provide a live response as part of the authentication process. For behavioral biometrics, the response would be embedded in the biometric characteristic captured (i.e., a spoken, written, or typed word). For physiological biometrics, it could be a specific finger for facial expression. (See Section 5.6)

Nonces. Standing for "Number ONCE", an arbitrary number that is generated for security purposes such as an initialization vector. A nonce is used only one time in any security session. In this context, it would involve the matching server generating and sending a nonce to the capture client/device which would then embed the nonce into the (signed) biometric sample so that when the matcher receives it, it can validate that the sample came from who it was very recently sent to.

Signed Components. Software or firmware components are digitally code-signed and validated during installation and/or use to mitigate against their modification or substitution. (An example would be a signed biometric algorithm DLL.)

1:1 Matching. Since a single attempt against a 1:N system allows an attacker to simultaneously attack ALL biometric references, limiting each attempt to a single biometric reference, for which the account ID (claimed identity) must be known, severely increases the difficulty of an attack.

Multibiometric/Multifactor. The requirement to use more than one biometric characteristic or more than one authentication technology/method, increasing the sophistication and resources required of an attacker. (See also 8.4.2 and 8.4.3.)

Debugger Hostile. Methods to detect or prevent data from being manipulated while in RAM/memory (such as is done by code debuggers which could be used to change a match decision, for example).

Coarse Scoring. The return of match scores of sufficiently large incremental resolution such that small changes in input samples would result in a change in matching score smaller than that increment. In this way, an attacker does not receive the feedback required to successfully mount a hill-climbing attack.

8.2.5 Mapping of Threats to Security Levels

The concept of security levels in general, and in OMB M04-04, implies that there are varying levels of concern regarding the security of different transactions (and the data associated with those transactions) and that therefore, different levels of protection are needed at each level. This in turn implies that there are some attacks that should be addressed (i.e., countermeasures implemented) at one level that may not be warranted at another.

Mapping of threats to security levels involves several considerations, including:

- Value/sensitivity of the transaction
- How easy/difficult is the attack to mount (i.e., in terms of sophistication, resources required, time, etc.)
- Cost and complexity of the associated countermeasure(s)

Table 11 below maps the threat identified above to the level at which it applies. Note that for a given level, all threats identified at that level ***OR BELOW*** apply and therefore appropriate countermeasures are required:

Table 11 - Threats Addressed at Assurance Levels

Level	Threats to be Addressed
1	Eavesdropping, "guessing" (FMR attacks)
2	Replay, database compromise
3	Sensor spoofing, man-in-the-middle, hill-climbing
4	Un-trusted device, malware

8.3 Analysis of Architectures

In Section 6, the six most feasible architectures were selected for further analysis. These architectures are summarized below in

Table 12 - Selected Biometric Architectures

Architecture	Storage	Matching
A	Server	Server
B	Client	Client
C	Device	Device
D	Token	Server
E	Token	Device
F	Token	Token

These architectures are each outlined in further detail below as they relate to the assurance and security levels addressed in both M04-04 and SP800-63.

It should be noted that:

- although this report and the following analysis is focused on a remote e-authentication application, much of the content is equally applicable to more general biometric authentication implementations, and
- over some implementations can be designed to support more than one architecture, either as a configuration parameter or depending on environment (e.g., when connected to a network, server based storage and/or matching is performed but when disconnected, local/client based storage/matching is performed).

8.3.1 Architecture Components

Biometric data being transferred

The data being transferred will be of significant interest when addressing the threats of each individual architecture later in the report. Regardless of what architecture is pursued, there is normally going to be transfer of biometric data. For most systems, there will be two distinct pieces of data which are being transferred as listed below.

> *Sample Data.* The presented sample data which is used to create a biometric template of the user for use in future transactions. This can also be the sample which is presented in subsequent authentication attempts.
>
> *Biometric Template.* The processed data which is stored and then compared each time the user makes a biometric authentication attempt.

The principles of integrity and confidentiality should be applied to this data from its creation through its lifetime.

Authentication Architectures

Table 13, shown below, identifies the movement of biometric data in terms of type (live sample or enrollment template), source, receiver, and direction in order that exposure of this data associated with its transfer can be ascertained. This table depicts only the data that **must** be transferred between the two components under consideration for each architecture. It also does not address any middleware that might be in between the two entities listed. In this diagram, 'S' indicates Sample, 'T' indicates Template data, and the arrow indicates the direction of movement of the data between the two identified components.

Table 13 - Biometric Architecture Data Transfer

Match \ Store	Server	Client	Device	Token
Server	Device **A** S → Server			Server **D** T ← Token
Client		Device **B** S → Client		
Device			Device **C** T ← S → Device	Device **E** T ← Token
Token				Device **F** S → Token

Each of the six architectures selected and described in Section 6 are analyzed from a security perspective in the following sections.

8.3.2 Store on Server (A)

Description: This architecture stores biometric templates on a server and requires that live samples be submitted back to the server in order for the matching process to occur. Once a match or no match result has been determined, the result is then sent to the verifier and the appropriate actions take place.

> NOTE: Dashed lines in the following Figure 21 indicate that these components/functions may also be implemented on the server, but are not required to be as part of the architecture definition.

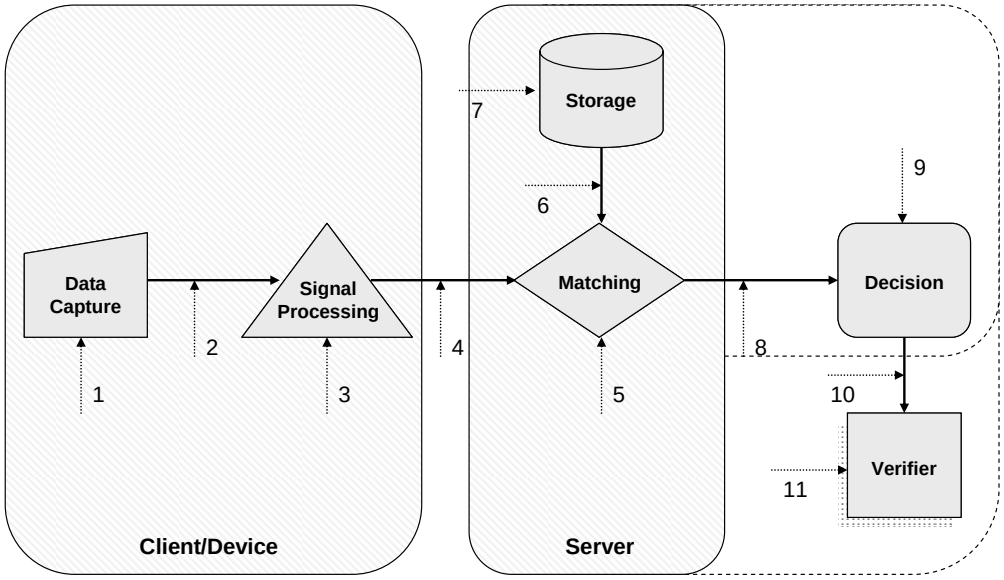

Figure 21 - Store on Server Match on Server Architecture

This is one of the most used architectures for biometric authentication in general and lends itself to a network environment, supporting for example a web services implementation (see Annex E.1). It facilitates access control by roving users to networked resources/data, in which both the biometric templates as well as the resources may be protected through physical security and behind a firewall. It does require reliable network connectivity and server configuration (e.g., redundancy/failover), secure communications, and database access controls.

From a security perspective in an open, e-authentication environment, the biggest considerations for this architecture are database vulnerability and transmission of the live sample across the network.

Use Cases:

User Type	**General Scenario**	**Application**
Citizen	Changes address on SSN web site or checks status of medical records with the veterans administration hospital. (level 2)	Person registers into the Social Security web site to manage their account. As part of the process, their biometric information is captured from a device on their local system. That biometric data is encrypted on the local system and sent to the SSN server for storage. When the user wants to change their address or make other inquiries into their account, they repeat the process and send their biometric data to the SSN server. If the server matches the previously stored data, the user if given access.
Agency Employee	An Agency employee asks to gain access to facilities,	Centralized storage of the biometric credentials is required, so updated records can be kept and

	such as offices, computer facilities and other employee locations, but not highly sensitive locations. (level 3)	managed in a timely basis.

Advantages:

- Storage and matching are collocated (minimizes exposure of template)
- Centralized storage allows for simplified administration

Disadvantages:

- Creates a single point of failure and attack
- Privacy considerations of central database storage

Data Transfer:
Sample **:** From the remote sensor to the server

Template**:** Internal on the server from database to matching algorithm

Authentication Determination**:** If the matching function is performed on a centralized server, there is a good chance the information about the authentication determination will not need to travel outside of the trusted environment.

Specific Threats:

1. Database compromise
2. Denial of Service attack

Specific Countermeasures:

1. Hardened server
2. Store encrypted templates
3. Database access controls

Assurance:
Level 1: YES
Level 2: YES
Level 3: YES: As long as there is multi-factor authentication
Level 4: YES: As long as a hard crypto token is used

8.3.3 Store on Client (B)

Description: This architecture stores biometric templates on a client platform and requires that live samples be captured and matched at the client. Once a match or no match result has been determined, the client application communicates the result to the verifier.

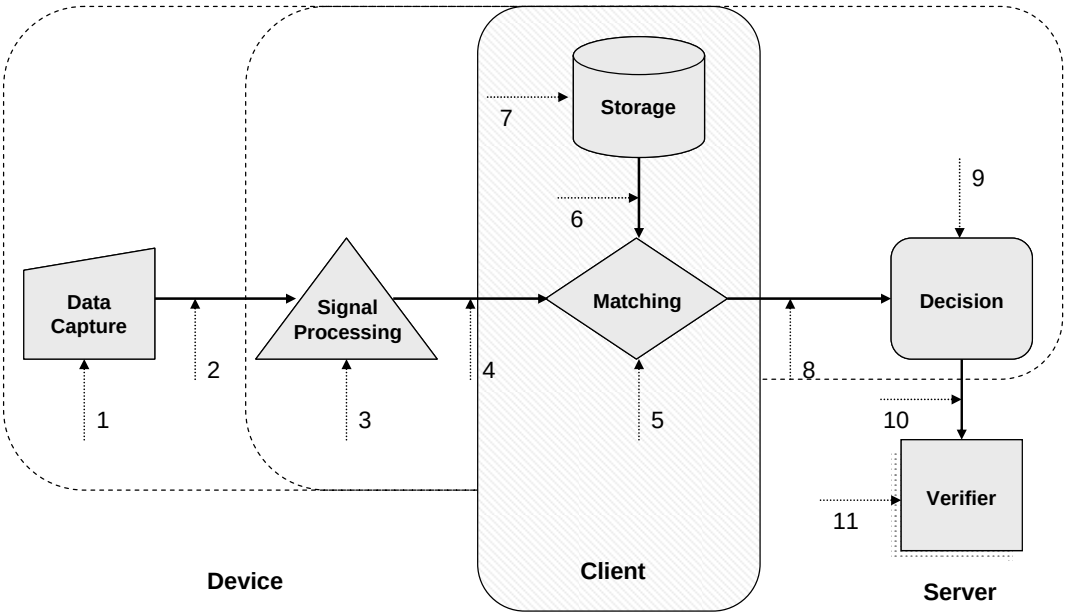

Figure 22 - Store on Client Match on Client Architecture

This architecture is beneficial in the case where authentication must happen very fast or in the case that the client is disconnected from the network and cannot communicate with a server. It is frequently used for standalone workstations or when the resources to be accessed are local to the client. Users must be enrolled on the workstation itself (i.e., at the access point) and enrollment templates stored on the workstation must be protected.

This architecture is common in the notebook space where, for example, a fingerprint sensor (possibly with an integral processor) is built into the notebook/laptop for logon to that machine. (Although use of that same sensor may also support other architectures, such as server based storage/matching.)

Storage on the hard disk of an untrusted client platform is a concern. Storage within a hardware security module (HSM) and use of a trusted platform module[1] (TPM) address some of these concerns.

From a security perspective in an open, e-authentication environment, the biggest considerations for this architecture are the untrusted nature of the client and the transmission of matching results/decisions across the network.

Use Cases:

User Type	**General Scenario**	**Application**
Citizen	Applies for annual park permit, or makes	To register to the Park site, the user enrolls locally on their computer using a biometric capture device.

[1] A hardware chip embedded on the motherboard that can be used to authenticate a hardware device.

	reservations at a national park for a summer family vacation. (Level 1)	To enter their account after registration, they match the template stored locally, and this releases a password to the Park site, validating the user to their account. No biometric information is stored centrally. Because the biometric processing is done on the client, there is exposure to spyware or other malicious code.
Citizen	Changes address on SSN web site or checks status of medical records with the veterans administration hospital. (level 2)	Person registers into the Social security web site to manage their account. As part of the process, their biometric information is captured from a device on their system and stored locally. When the user wants to change their address or make other inquiries into their account, they capture and match to the locally stored biometric data, releasing a password to the SSN server if there is a match. Because the biometric processing is done on the PC, where is exposure to spyware and other malicious code.

Advantages:
This architecture would be a simple way to use biometrics for website log-ins and transactions. Further more, if the client is truly trusted (i.e., is tamper resistant, can be cryptographically authenticated), it would promote a starting point for Single Sign On solutions.

Disadvantages:
- Biometric data stored on client machines which are generally considered untrusted

Data Transfer:
Sample**:** From the remote sensor to the client

Template**:** Internal on the client from database to matching algorithm

Authentication Determination**:** If the matching function is performed on a remote client, there is a good chance the information about the authentication determination will need to still travel over an un-trusted network to reach its final destination for eventual use in the security system.

Specific Threats:
1. Replay attack on the client
2. Hill climbing attempt
3. Un-trusted Client Machines
4. Component replacement
5. Data manipulation (thresholds, scores, results)
6. Database compromise

Specific Countermeasures:
1. Use TTL tag

2. Implement incremental feedback to the user
3. Certified clients & trusted path
4. TPM or HSM storage
5. Signed & encrypted reference templates

Assurance:
Level 1: YES
Level 2: YES
Level 3: NO
Level 4: NO

8.3.4 Store on Device (C)

Description: This architecture stores biometric templates on an authentication device (e.g., a "self-contained" biometric sensor unit or a PDA or smart phone) and requires that live samples be matched on that device. Once a match or no match result has been determined, the device sends the appropriate signal to the mechanism it is securing.

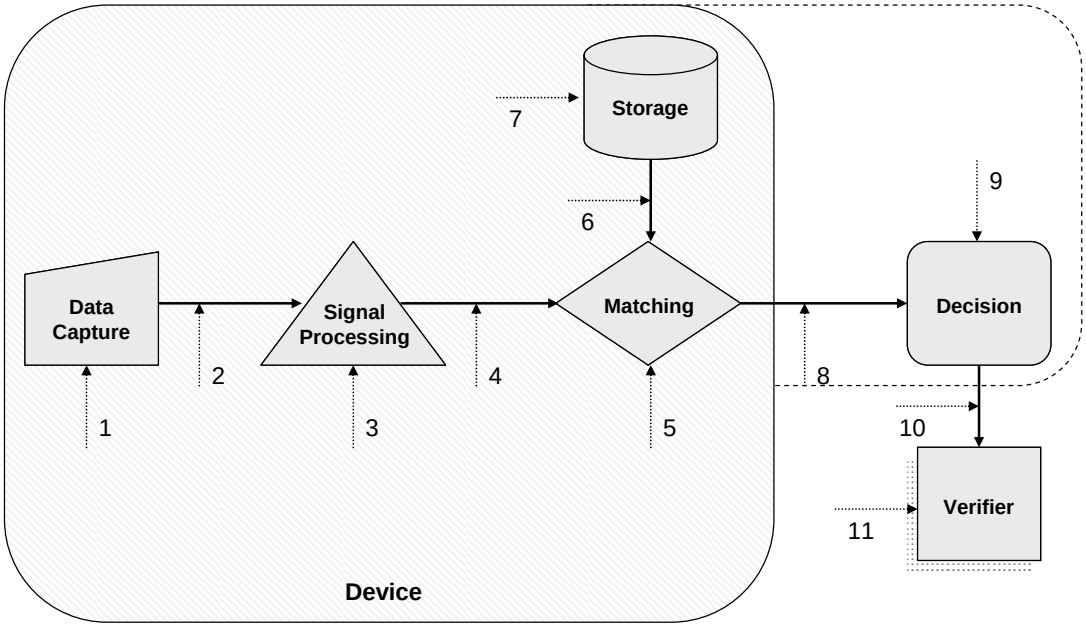

Figure 23 - Store on Device/Match on Device Architecture

This architecture is typical in a mobile virtual private network (VPN) or physical access scenario when the device obtains a live sample and matches it to its stored database (on the device) in order to grant access. [A variation of this example is the store on server, match on device scenario].

Self-contained devices can be implemented in a variety of form factors and "hardening".

From a security perspective in an open, e-authentication environment, the biggest considerations for this architecture are the integrity (e.g., tamper resistance, assurance level) of the device and transmission of the matching scores/decision outside the device. (Note that decision results may be in the form of an authentication token as opposed to a Boolean output.)

Use Cases:

User Type	General Scenario	Application
Citizen	Applies for annual park permit, or makes reservations at a national park for a summer family vacation. (Level 1)	To register to the Park site, the user enrolls locally on their computer using a biometric capture device. To enter their account after registration, they match the template stored locally, and this releases a password to the Park site, validating the user to their account. No biometric information is stored centrally, and all of the biometric processing is done within a dedicated processor so none of the biometric information is exposed to spyware or other malicious code.
Citizen	Changes address on SSN web site or checks status of medical records with the veterans administration hospital. (level 2)	Person registers into the Social security web site to manage their account. Their biometric information is captured from a reader on their local system and stored into a device with memory and a processor. When the user wants to change their address or make other inquiries into their account, they try to match the biometric data stored within their device, which processes the biometric data separately from the PC. If they match, a password is released and they are given access. This method protects the user from spyware and other malicious code on the PC.
Agency Employee	An Agency employee asks to gain access to facilities, such as offices, computer facilities and other employee locations, but not highly sensitive locations. (level 3)	Centralized storage of the biometric credentials is required, so updated records can be kept and managed in a timely basis.

Advantages:

- This architecture would be ideal for remote physical access devices that are being monitored and communicating over the internet.
- Using the device as the computing platform creates a greater degree of independence.

Disadvantages:

- Depending on security level, device certification may be required.

Data Transfer:

Sample**:** The sample is integral to the device.

Template**:** Internal on the device from database to matching algorithm.

Authentication Determination**:** If the matching function is performed on a remote device, there is a good chance the information about the authentication determination will need to still travel over an un-trusted network to reach its final destination for eventual use in the security system.

Specific Threats:

1. Spoofing
2. Hill climbing attack
3. Untrusted device

Specific Countermeasures:

1. Liveness detection
2. Implement incremental feedback to the user
3. Device certification, mutual authentication of device
4. A secret sample
5. Challenge/Response protocols

Assurance:
Level 1: YES
Level 2: YES
Level 3: YES: As long as there is multi-factor authentication
Level 4: YES: To release hard cert or as a second factor at verifier

8.3.5 Store on Physical Token (D-F)

Note that a physical token includes, but is not limited to, a smartcard (though this is arguably the most common implementation). Further, smart cards may be of the contact, contact less, or dual interface variety.

8.3.5.1 Match on Server (D)

Description: This architecture stores biometric templates on a physical token such as an integrated circuit chip card or smart card. In practice, the user inserts the smart card and presents their biometric. Both the stored template and live sample are transmitted to the server for matching.

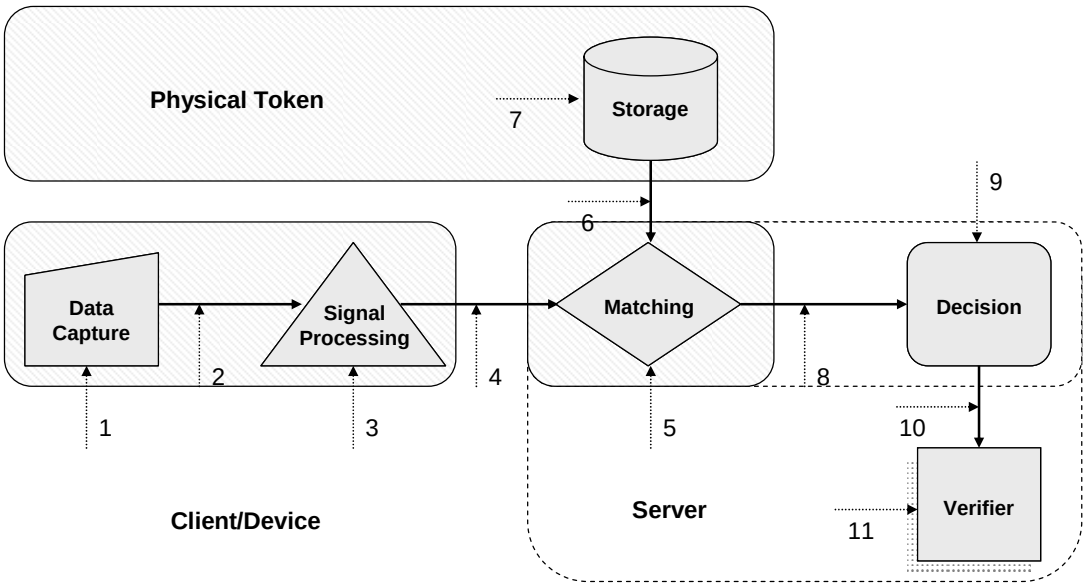

Figure 24 - Store on Token/Match on Server Architecture

This has been favored by some security agencies for two reasons: there is no centralized storage as a single point of attack and the matching is performed in a secure/controlled location. The server is in charge of signing the physical tokens (or data on that token) before they are deployed, providing for easier management and revocation. This architecture does contain the requirement to transfer both the stored template and presented sample each time an authentication attempt is made.

Note that this architecture (or a variation in which the data is stored on a smartcard, but matching is performed locally) is used in the US Government's Personal Identity Verification (PIV) program, implementing HSPD-12.

From a security perspective in an open, e-authentication environment, the biggest considerations for this architecture are the integrity (e.g., tamper resistance, assurance level) of the physical token and transmission of the template/sample across the network. (Note that the stored template may be signed, encrypted, and/or packaged within an X.509 certificate.)

Use Cases:

User Type	**General Scenario**	**Application**
Agency Employee	The agency employee is registered into their human resources database. During the process, a biometric sample is captured and stored. When the agency employee is reviewing and/or modifying personal	Employee are issued an ID badge with their biometric information stored on that ID badge. When they want to gain access to their personal information on the HR database, the system reads the biometric data from their ID badge, and the live capture biometric information. Both biometric samples are sent to the agencie's server for matching. If there is a match, the employee is

	information on that HR system, their biometric data is captured and sent to the HR database. If there is a match, they are granted access.	granted access.
Agency Employee	An Agency employee asks to gain access to facilities, such as offices, computer facilities and other employee locations, but not highly sensitive locations. (level 3)	Users are enrolled into a ID badge. During verification, the ID badge is presented and the template is sent from the card to the server, along with the live capture biometric sample. If there is a match, the user is given access.
Agency Employee	A Veteran Affairs pharmacist dispenses a controlled drug from a qualified and authorized doctor. (level 3 or 4)	The pharmacist is enrolled into a ID badge. During verification, the ID badge is presented and the template is sent from the card to the server, along with the live capture biometric sample. If there is a match, the pharmacist is given the controlled substance for dispensing to the patient.
Agency Employee	Agency investigator uses a remote system to gain access to potentially sensitive personal client information, from over the internet and from a personal residence or other unsecured facility. (level 4)	The investigator presents their biometric ID badge to the system. The biometric information from the ID badge, along with a live capture of the same biometric is sent to the server for matching. Typically, a 2nd factor is required, which is the ID badge, and maybe a 3rd factor, such as a PIN or password.
Government Supplier	Maintains an account with the GSA contracting office for large government procurements. (to level 3)	The Gov supplier representative is issued an agency ID badge with their biometric credentials. When they access their account with the GSA, the biometric from their ID badge and a live sample are sent to the GSA server for comparison. If there is a match, and the ID badge is valid, access is granted.
Government Supplier	Government supplier is managing large database of criminal information (level 4)	The Gov supplier representative is issued an agency ID badge with their biometric credentials. When they access their account with the GSA, the biometric from their ID badge and a live sample are sent to the GSA server for comparison. If there is a match, and a 2nd factor such as PIN is provided and the ID badge is valid, access is granted.

Advantages:

- No central storage to protect
- Matching occurs in a secure environment

Disadvantages:

- Hardware and/or cryptographic protection of template data required

Data Transfer:
Sample: From the remote sensor to the server

Template**:** From the physical token (device) to the server

Authentication Determination**:** If both the matching and decision functions are performed on a centralized server, then the information about the authentication determination will not need to travel outside of the trusted environment.

Specific Threats:

1. Eavesdropping attack on either of the two communication channels
2. Insertion of imposter data on either of the two communication channels

Specific Countermeasures:

1. Enforce strong data protection during communication
2. Implement means in which the template can be verified as valid when returned to the server.

Assurance:
Level 1: YES
Level 2: YES
Level 3: YES: As long as there is multi-factor authentication
Level 4: YES: As a second factor at verifier.

NOTE: Although use of a biometric token may not yet be considered cost-effective for Level 1 and 2 transactions, it is possible that as the technology becomes more ubiquitous and the cost decreases, this may in fact become worthy of consideration.

8.3.5.2 Match on Device (E)

Description: This architecture stores biometric templates on a physical token such as an integrated circuit chip card or smart card. But unlike Architecture D, the live sample is compared and matched on the local device instead of on the server.

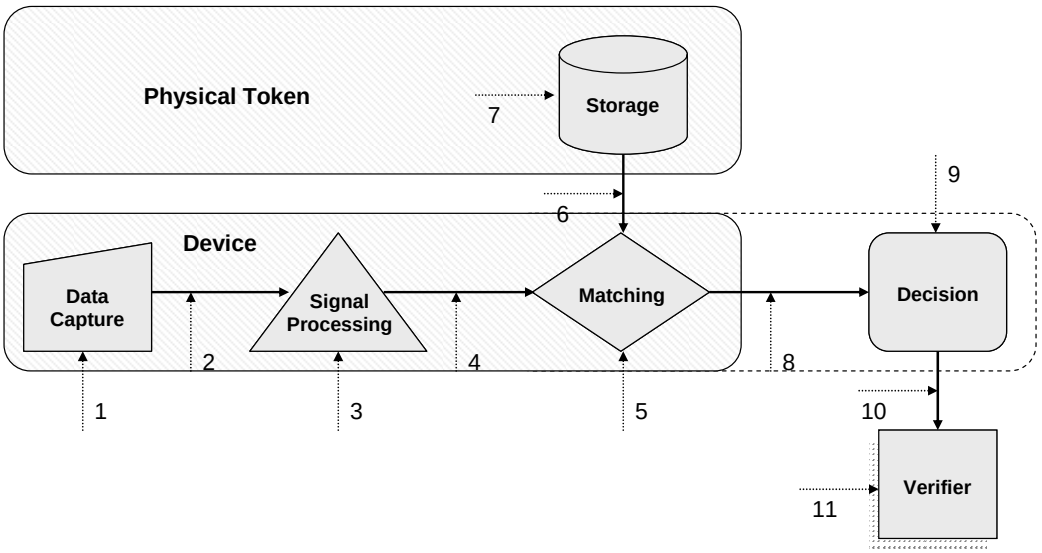

Figure 25 - Store on Token/Match on Device Architecture

This architecture would allow for a single trusted device that is both a physical token and biometric reader, which would capture the sample, compare it against the template, and hold/release another authentication credential. The most obvious uses of this architecture would be a PDA or an all encompassing cell phone device or a physical access (door reader) device.

From a security perspective in an open, e-authentication environment, the biggest considerations for this architecture are the integrity (e.g., tamper resistance, assurance level) of the physical token and device and transmission of the matching scores/decision across the network.

Use Cases:

User Type	**General Scenario**	**Application**
Agency Employee	The agency employee is registered into their human resources database. During the process, a biometric sample is captured and stored. When the agency employee is reviewing and/or modifying personal information on that HR system, their biometric data is captured and sent to the HR database. If there is a match, they are granted access.	Employees are issued an ID badge with their biometric information stored on that ID badge. When they want to gain access to their personal information on the HR database, the system reads the biometric data from their ID badge, and their live capture biometric information. Both biometric samples are sent to a secure processor such as a USB token device or secure processor within their computer. The processor is a FIPS 140-2 level 2 certified device. If there is a match, the employee is granted access.
Agency Employee	An Agency employee asks to gain access to facilities, such as offices, computer	Users are enrolled into a ID badge. During verification, the ID badge is presented and the template is sent from the card to the device, along

	facilities and other employee locations, but not highly sensitive locations. (level 3)	with the live capture biometric sample. If there is a match, the user is given access.
Agency Employee	A Veteran Affairs pharmacist dispenses a controlled drug from a qualified and authorized doctor. (level 3 or 4)	The pharmacist is enrolled into a ID badge. During verification, the ID badge is presented and the template is sent from the card to the device along with the live capture biometric sample. If there is a match, the pharmacist is given the controlled substance for dispensing to the patient.
Agency Employee	Agency investigator uses a remote system to gain access to potentially sensitive personal client information, from over the internet and from a personal residence or other unsecured facility. (level 4)	The investigator presents their biometric ID badge to the system. The biometric information from the ID badge, along with a live capture of the same biometric is sent to the device for matching. This device is a FIPS 140-certified device for secure processing. Typically, a 2nd factor is required, which is the ID badge, and maybe a 3rd factor, such as a PIN or password.
Government Supplier	Maintains an account with the GSA contracting office for large government procurements. (to level 3)	The Gov supplier representative is issued an agency ID badge with their biometric credentials. When they access their account with the GSA, the biometric from their ID badge and a live sample are sent to the device for comparison. the device is a FIPS 140-2 level 2 device. If there is a match, and the ID badge is valid, access is granted.
Government Supplier	Government supplier is managing large database of criminal information (level 4)	The Gov supplier representative is issued an agency ID badge with their biometric credentials. When they access their account with the GSA, the biometric from their ID badge and a live sample are sent to the device for comparison. The device is a FIPS 140-2 level 2 device. If there is a match, and a 2nd factor such as PIN is provided and the ID badge is valid, access is granted.

Advantages:

- Proximity of storage/matching
- Privacy friendly as user controls their enrollment template

Disadvantages:

- Device certification may be required for higher assurance levels
- Hardware and/or cryptographic protection of template data required

Data Transfer:

Sample**:** Internal from the sensor on the device to the matching algorithm on the same device.

Template: From the token database to the matching algorithm on the device (may or may not be exposed).

Authentication Determination: If the matching function is performed on a local device; there is a good chance the information about the authentication determination will need to still travel over an un-trusted network to reach its final destination for eventual use in the security system. (Note that authentication results may be transmitted in the form of an authentication token.)

Specific Threats:

1. Spoofing
2. Physical attacks to the device

Specific Countermeasures:

1. Live ness detection
2. Require tamper resistant devices to prevent disclosure of sensitive information

Assurance:
Level 1: YES
Level 2: YES
Level 3: YES: As long as there is multi-factor authentication
Level 4: YES: To release hard cert or as a second factor at verifier.

8.3.5.3 Match on Physical Token (F)

Description: This architecture stores biometric templates on a physical token such as an integrated circuit chip card or smart card. But unlike Architecture D or E, the live sample is compared and matched on the card instead of an external server or device. Successful verification could result in access to and release of an authentication token stored on the card, such as a certificate used in an authentication protocol.

Note that data capture/signal processing may occur internal or external to the physical token.

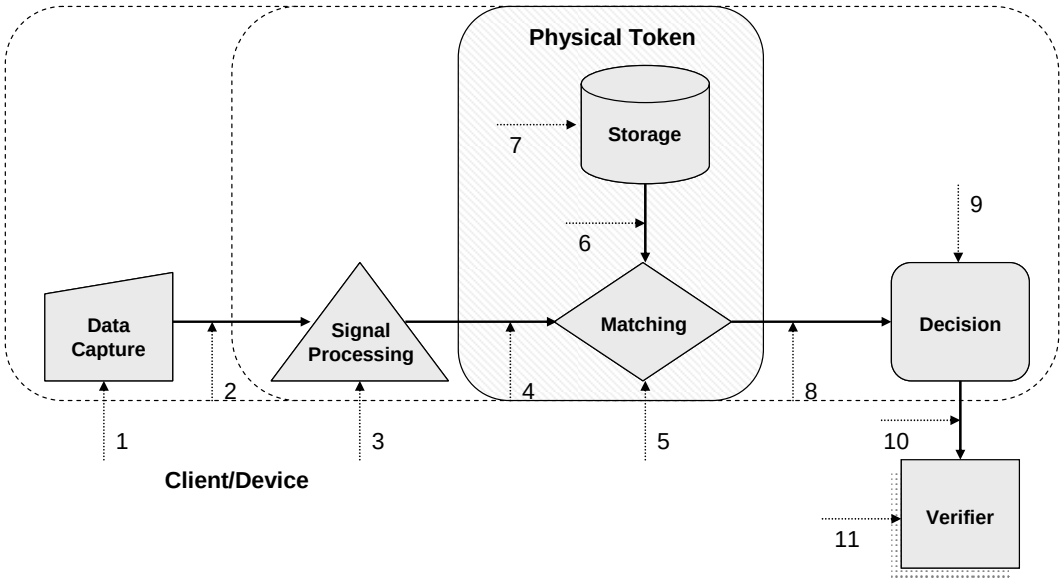

Figure 26 - Store on Token/Match on Token Architecture

This would be a biometric PIN replacement. This architecture is most similar to the way biometrics is viewed as being acceptable for use by NIST SP800-63. Certified authentication match of the biometric characteristic can "unlock" another form of authentication which is released to the system.

From a security perspective in an open, e-authentication environment, the biggest considerations for this architecture are the integrity (e.g., tamper resistance, assurance level) of the physical token and device and, when performed, transmission of the matching scores/decision across the network.

Use Cases:

User Type	**General Scenario**	**Application**
Agency Employee	The agency employee is registered into their human resources database. During the process, a biometric sample is captured and stored. When the agency employee is reviewing and/or modifying personal information on that HR system, their biometric data is captured and sent to the HR database. If there is a match, they are granted access.	Employees are issued an ID badge with their biometric information stored on that ID badge. When they want to gain access to their personal information on the HR database, the system reads their live capture biometric information and sends the extracted template into the ID badge for comparison. If there is a match, the ID badge validates the transaction and the employee is granted access.
Agency	An Agency employee asks	Users are enrolled into a ID badge. During

Employee	to gain access to facilities, such as offices, computer facilities and other employee locations, but not highly sensitive locations. (level 3)	verification, the ID badge is presented and the live capture biometric sample is processed to generate a template and then send to the physical token for matching. If there is a match, the user is given access.
Agency Employee	A Veteran Affairs pharmacist dispenses a controlled drug from a qualified and authorized doctor. (level 3 or 4)	The pharmacist is enrolled into a ID badge. During verification, the live capture biometric sample is processed and sent to the physical token for matching. If there is a match, the pharmacist is given the controlled substance for dispensing to the patient.
Agency Employee	Agency investigator uses a remote system to gain access to potentially sensitive personal client information, from over the internet and from a personal residence or other unsecured facility. (level 4)	The investigator presents their biometric ID badge to the system. A live capture of their biometric is processed and sent to the physical token for matching. Typically, a 2nd factor is required, which is the ID badge, and maybe a 3rd factor, such as a PIN or password. The token is a FIPS 140-2 certified device for secure processing.
Government Supplier	Maintains an account with the GSA contracting office for large government procurements. (to level 3)	The Gov supplier representative is issued an agency ID badge with their biometric credentials. When they access their account with the GSA, a live biometric sample is collected and processed and sent to the physical token for comparison. The token must be a FIPS 140-2 level 2 device. If there is a match, and the ID badge is valid, access is granted.
Government Supplier	Government supplier is managing large database of criminal information (level 4)	The Gov supplier representative is issued an agency ID badge with their biometric credentials. When they access their account with the GSA, a live biometric sample is collected and processed and sent to the physical token for comparison. The token must be a FIPS 140-2 level 2 device. If there is a match, and a 2nd factor such as PIN is provided and the ID badge is valid, access is granted.

Advantages:

- Co-location of storage/matching
- Privacy friendly as user controls their enrollment template

Disadvantages:

- Token certification may be required for higher assurance levels
- Hardware and/or cryptographic protection of template data required

Data Transfer:

Sample: From the sensor to the matching algorithm on the physical token.

Template: Internal from the database to the matching algorithm on the physical token.

Authentication Determination: If the matching function is performed on a remote physical token; there is a good chance the information about the authentication determination will need to still travel over an un-trusted network to reach its final destination for eventual use in the security system.

Specific Threats:

1. Spoofing
2. Physical attacks to the device

Specific Countermeasures:

1. Liveness detection
2. Require tamper resistant devices to prevent disclosure of sensitive information

Assurance:
Level 1: YES
Level 2: YES
Level 3: YES: As long as there is multi-factor authentication
Level 4: YES: The verifier is a hard crypto token in and of it self.

8.3.6 Architecture Applicability to Security Levels

Table 14 - Biometric Architectures and Assurance Level Comparison

	Assurance Level 1	Assurance Level 2	Assurance Level 3	Assurance Level 4
Architecture A	Yes	Yes	Yes, if used with multi-factor authentication	Yes, if used with hard crypto token
Architecture B	Yes	Yes	No	No
Architecture C	Yes	Yes	Yes, if used with multi-factor authentication	Yes, if device is trusted and used with hard crypto token
Architecture D	Yes	Yes	Yes, if used with multi-factor authentication	Yes, if used with hard crypto token
Architecture E	Yes	Yes	Yes, if used with multi-factor authentication	Yes, if device is trusted and used with hard crypto token
Architecture F	Yes	Yes	Yes, if used with multi-factor authentication	Yes, if the token is FIPS 140 certified

8.4 Considerations

8.4.1 Trust

One of the key aspects of consideration is the amount of trust and confidence between the two entities which are interacting to achieve remote e-authentication. The amount of trust in the end to end system will be a determining factor in which assurance levels can be achieved.

"Semi-Open"
Both remote and centralized entities are apart of the same organization, but the data must be traversed over the internet or some sort of un-trusted network.

"Completely Open"
Remote entity has no relationship with the centralized entity from an information technology perspective.

These two architectures can most closely be related to the modern example of VPN technologies. The "semi-open" architecture would be similar to an office to office VPN where both entities are at a high level of mutual trust.

The "completely open" architecture would be similar to an employee connecting remotely via VPN to the main corporate headquarters from an airport internet kiosk. In this case, the organization must initially accept all initial VPN requests because all the possible origins of VPN connection can not be pre-determined. The level of trust in this architecture is lower because it is reliant solely on the claimant provided credentials.

8.4.2 Multi-factor authentication

The verification location for each individual credential being authenticated is important to note when discussing multi-factor authentication.

It should be noted in discussing multi-factor authentication, that there are two methods of implementing this – serial (chained) or parallel (concurrent).

In the chained approach, one factor activates/enables a second factor which is what is presented to the verifier. This is depicted below in Figure 27.

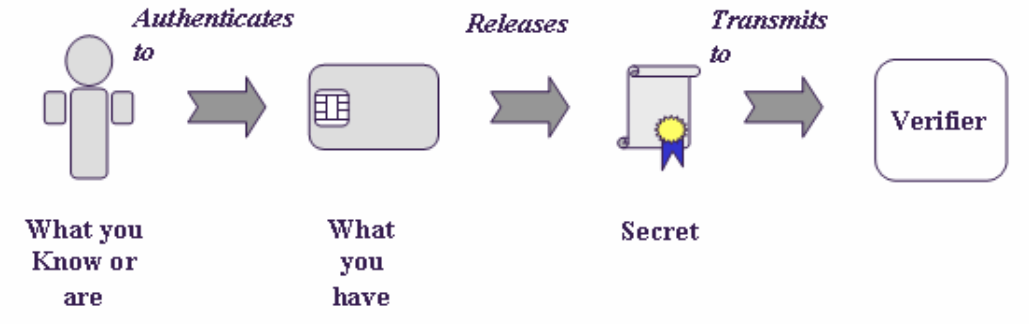

Figure 27 - Serial Multi-factor Authentication

In the concurrent approach, both factors are provided by the user and are independently verified at the verifier, as shown below in Figure 28.

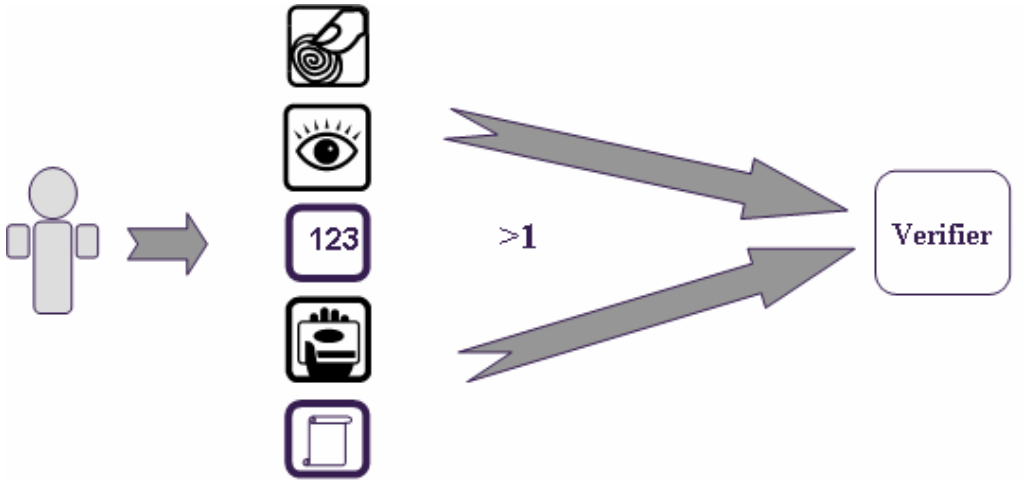

Figure 28 - Parallel Multi-factor Authentication

In SP800-63, the use of biometrics at Levels 3 & 4 are via the chained method, where the biometric is used to release the cryptographic authentication token (soft or hard cert). A case could be made that this is not as strong as a concurrent approach, as stated in the following (excerpted from the public comments on SP800-63):

> An authentication protocol must be analyzed from the perspective of the relying party (the Verifier) in an information infrastructure. For an authentication transaction to be "multi-factor", the relying party must be able to consider and validate each form of identity assurance independently. In fact, the introduction to Section 5 of SP800-63 correctly describes the E-Authentication Model as “When a claimant successfully demonstrates possession and control of a token in an on-line authentication to a verifier through an authentication protocol”. While using a PIN or password protected hard token might produce a higher level of trust for the token from a global perspective, it does not represent multi-factor authentication to the Verifier, since it is impossible to independently validate the PIN or password with respect to the token itself, or with respect to the identity being claimed. Nothing in this context construes an irrevocable connection between a user and a claim of identity, nor can it demonstrate the will or intent of the user - an important aspect of non-repudiation in the common law sense. Since the Verifier cannot validate the token and the PIN or password independently, the PIN/password protected hard token represents only a single authentication factor in the authentication protocol. However, if the PIN/password is validated by the relying party, along with the validation of another token (like a PKI certificate), the authentication process is then truly multi-factor, satisfying section 8.2.4 of SP800-63 “Authentication requires that the claimant shall prove through a secure authentication protocol that he controls the token.”

Based on this discussion, there are some biometric architectures that could be affected:

- Store on Server, Match on Client. Assuming the client is not authenticating the hard crypto token but simply passing it to the system along with biometric match determination.
- Store on Client, Match on Client. Assuming the client is not authenticating the hard crypto token but simply passing it to the system along with biometric match determination.
- Store on Device, Match on Device. Assuming the device is not authenticating the hard crypto token but simply passing it to the system along with biometric match determination.

Matching of the sample provided against the stored template on the hard crypto token itself is currently viewed as acceptable multi-factor environment.

Environments affected:

- Store on Token, Match on Token. The verifier is a hard crypto token in and of itself.

8.4.3 Multi-biometric authentication

Multimodal biometric systems represent an emerging trend that attempt to increase the level of security by using more than one biometric for identification or verification. Increasing the number of credentials required to be shown by an individual increases the level of security and makes its harder for an impersonator to break into the system. The same holds true for multimodal biometric systems. Reinforcement of evidence from multiple biometric systems can offer increasingly irrefutable proof of an individual's identity [15]. Several research studies have been conducted to test the increase in security and performance of multi-biometric systems.

Multimodal biometric systems can be categorized into three general groups:

1. Feature extraction level fusion: In this system two or more samples are captured from one or more sensors, and the features extracted from each individual sample are fused into a single feature vector. During the identification/verification stage, the acquired samples are fused into a single feature vector and used to match with the template. This system has only one matcher, and only one matching score.
2. Matching score level fusion: In this system two or more samples are captured from one or more sensors, and the features extracted from each individual sample are stored as separate feature vectors. During the identification/verification stage, separate matchers are used to compare the enrollment templates with the acquired samples and the multiple matching scores are fused to create single matching score which is used to make a decision. This system has multiple matchers, and the multiple scores are fused.
3. Decision level fusion: In this system two or more samples are captured from one or more sensors, and the features extracted from each individual sample are stored as separate feature vectors. During the identification/verification stage, separate matchers are used to compare the enrollment templates with the acquired samples, and multiple matching scores are used to make individual decisions about each matching process. Decisions from the multiple matchers are combined to make a single decision about the matching process.

In an authentication system designed for use over open networks and remote locations, multimodal biometric systems have to take into consideration what type of system architecture will be used. For instance, a multimodal biometric system that uses feature extraction level fusion, sample acquisition at the client end, and matching operation at the server end can perform the fusion operation at the client end or the server end. Multimodal biometric systems can be used effectively to reduce FTE rates, FRR and FAR, and decrease the matching times for large databases. But multimodal biometric systems also increase the cost and complexity of a system, and if not properly designed they do not provide any additional benefits. The sensitivity of these problems increases in a distributed environment where operations are performed over open networks. An analysis which examines the different levels of multimodal biometrics fusion, and the different distributed architectures will be necessary to fully realize the advantages of multimodal biometrics.

9 Recommendations

This section summarizes recommended changes to SP800-63 to accommodate the use of biometrics at the various security levels.

A most basic recommendation is made to include biometrics as acceptable and feasible mechanisms for use in the remote e-authentication environment at all four of the security levels defined by OMB and NIST. This recommendation comes based on the work of the INCITS M1 technical committee on Biometrics, in the form of this technical report. The most compelling location of discussion on biometrics is in Section 8 (Authentication Protocols) of SP800-63. This location in the document would allow for the use of biometrics to be most accurately linked to the four security levels. Also worth including into the document is an Annex explaining the functions of biometrics, similar to the annex already contained on passwords. This proposed annex would include portions of this report such as the biometric concept diagram and functional models.

A full set of proposed edits to SP800-63, less the informative annex, is provided as Annex A.

A summary of these recommendations are as follows:

- As integrity is a major premise and requirement for biometric authentication, biometric reference data should always be digitally signed, MACd, or contained within an X.509 attribute certificate. Biometric sample data should be similarly protected at Levels 2 and above.
- Biometric data should always be encrypted during network transmission and when stored on a hard disk (i.e., on a server or client) for both privacy reasons (as biometrics are considered personal data) and to increase the difficulty of an attacker obtaining digital copies of this information. When stored in a hardware device or physical token where physical security protection is provided, encryption is not necessary; however, to read the biometric reference from the device/token requires mutual authentication (i.e., it is not a free read) and the channel should be encrypted.
- IT/computer security requirements and mechanisms apply to biometric authentication systems/protocols and address many of the vulnerabilities. Additional threats that are unique to biometrics are identified, prioritized, and countermeasures specified by assurance level (see Table 18 in Annex A below).
- Biometrics may be used alone only at Levels 1 and 2; however, when server-based matching is not used then another authentication token (e.g., a password, etc.) must be provided to the remote verifier in order to complete the authentication protocol.
- A dynamic, content-based biometric comprises two-factors and is thus suitable for use alone at Level 3 and below (since both the biometric part and the embedded secret part are independently verified).
- As a hard cert is always required at Level 4, matching on the server is only applicable as a 2nd factor and matching on a device or physical token is only applicable to initiate release of that hard cert.
- Storage and matching on the client workstation is not suitable for Levels 3 or 4.

- Maximum False Match Rates (FMR) is specified for each assurance level (see Table 19 in Annex A below). It is noted that biometric entropy and strength of function are not directly correlated. FRR is application dependent.

It is further noted that biometric authentication differs from the standard model in that:

- Biometric enrollment must occur during registration and results in the applicant providing the biometric to the RA/CSP.
- During authentication, it is a newly captured biometric sample that is compared to the registered biometric reference to verify identity. The claimant does not present the credential per se, but a biometric sample from the same source as that registered.
- For server-based matching, this requires that the verifier have knowledge of the registered biometric (credential).
- For non-server-based matching, this requires that a different token be sent to the verifier (or used to participate in an authentication protocol). This token may be bound to the same credential as the biometric or the biometric verification may be used to unlock the token from another binding.

The following tables provide a direct relationship between the proposed requirements of biometrics and the four security levels.

Table 15 - Minimum Protection Requirements

Protect against	Level 1	Level 2	Level 3	Level 4
FMR attacks (guessing/brute force)	√	√	√	√
Database compromise		√	√	√
Sensor spoofing			√	√
Hill climbing			√	√
Untrusted sensor				√

Note that these are in addition to the more general requirements of SP800-63 which includes requirements for resistance to eavesdropping, replay attacks, main-in-the-middle, etc.

Table 16 - Maximum FMR Requirements

Requirement	Level 1	Level 2	Level 3	Level 4
FMR rate (not to exceed)	1 in 100	1 in 100	1 in 1000	1 in 1000

Neither FNMR nor FRR are specified (though the FMR must be measured at a selected, operationally suitable FNMR) as these are application dependent. It is noted, however, that failures to enroll (FTE) and false rejections must be accounted for in the overall authentication scheme (e.g., a backup mechanism may need to be provided in these instances).

In terms of the entire SP800-63 document as a whole, it is recommended to clarify the wording of a "token". Currently, this term is used to describe any credential the user has some degree of control over during the process of authentication. It is believed that confusion over this term has occurred because, according to SP800-63, a token can be any credential, both tangible and intangible. While this blanket definition may be relevant in some remote authentication scenarios, it does not coincide with other authentication systems that consider a token to be

something that is physically tangible by the user. Common examples of a physical token in such systems would be an ID card, smart card, magnetic stripe card or any combination of these.

10 Future Work

This section is meant to outline the future actions to be pursued in the field of biometric and E-Authentication. While section 9 summaries the recommendations of this ad hoc group, and Annex A propose specific changes to the current draft of NIST SP800-63, there remains the need to further review and investigate many of the topics covered in this report. Below are some of the initial (at the time of publishing) areas identified which future work is anticipated and encouraged.

- INCITS M1.4 – Task Group on Biometric Profiles should develop a profile for biometrics in e-authentication.
- PhD level study to further characterize and quantify key space, entropy and strength of function for biometrics. This would most likely require a mathematician, statistician, biologist, security expert.
- Work with NIST to review the recommendations of this report as part of a future revision cycle for SP800-63.
- Further analysis as to the downstream implementation impact of inserting a biometric authentication capability into the Federal e-Authentication initiative, which is based on SP800-63.

Annex A: Recommended Edits to SP800-63

The following represents the edits to SP800-63 needed to implement the recommendations of Section 9. Note, however, that it is probable that these edits will necessitate additional changes within the document which are not documented herein.

A.1 Edits to Section 4 (Definitions)

Replace definition of "biometric" with the following definition for "biometrics", which is the accepted definition of ISO/IEC JTC1 SC37:

"Automated recognition of individuals based on their behavioral and biological characteristics."

A.2 Edits to Section 5 (E-Authentication Model)

Change second paragraph to read:

E-authentication begins with *registration*. An *applicant* applies to a *Registration Authority (RA)* to become a *subscriber* of a *Credential Service Provider (CSP)* and, as a subscriber, is issued or registers a secret, called a *token*, or enrolls a biometric characteristic, which may or may not be used directly as a token, and a *credential* that binds the token/biometric to a name and possibly other attributes that the RA has verified. The token/biometric and credential may be used in subsequent authentication events.

In the remainder of Section 5 (and beyond), replace "token" with "token/biometric" where appropriate. [Alternatively, a "biometric token" could be defined.]

In (or just after) the fourth paragraph, add:

"Physiological (biological) biometrics are generally not considered secrets, though behavioral biometrics may incorporate a secret (i.e., a passphrase intrinsically embedded within a voice or sign sample – hereafter referred to as "content-bearing biometrics"). For a non-secret ("static") biometric characteristic used in lieu of a traditional token, rather than possession and control of the token, the factors that must be demonstrated are related to the *integrity* of the biometric sample – that it was captured from a live, present human being and that it has not been modified.

A.2.1 Edits to Section 5.1

After the second (or third) paragraph, add:

"In the case of biometrics, the RA captures and processes the biometric sample from the claimant and provides it as a *biometric reference* to the CSP, rather than the CSP creating it. The CSP binds the biometric reference to the identity to create the biometric credential."

In biometric authentication, it is a live biometric sample that is captured and used in an authentication protocol. This live sample is compared against the biometric reference to determine if it matches (belongs to the same human being that was enrolled/registered). As a result, the integrity (rather than the secrecy) of both the live sample and reference that is critical. (For content-bearing biometrics, the secrecy of the embedded content must also be protected.)

A.2.2 Edits to Section 5.2

In the next to last paragraph, change to read:

"Biometrics are unique personal attributes that can be used to verify the identity of a person. They include facial features, fingerprints, DNA, iris and retina scans, voiceprints and many other characteristics. In this document, biometrics are used in the registration process to be able to later prevent a subscriber who in fact registered from repudiating the registration, to help identify those who commit registration fraud, and to unlock tokens. ~~Biometrics are not used directly as tokens in this document.~~ In addition, biometrics may be used in lieu of a traditional token under circumstances described in this document."

Also, add to the end of the last paragraph:

"Biometrics may also be used in lieu of a token as specified in Section 6."

A.2.3 Edits to Section 5.3

Change end of 2nd bullet to read "some attribute (such as a biometric)".

A.2.4 Edits to Section 5.4

Add second paragraph as follows:

"Biometric authentication may be accomplished in a number of ways, based on authentication architectures which differ in where the biometric reference is stored and where the biometric matching operation is performed. The choice of architecture affects the role and operation of the verifier. In the case where neither storage nor matching is performed on a server (i.e., is performed on a physical token, device, or client platform) and results in a traditional token being "released", there is no impact on the verifier. However, for server based matching, the verifier is involved. If the reference is not stored on the server, then the verifier merely performs the matching and constructs the assertion accordingly. If the reference is stored on a server (either under the direct control of the verifier or accessed from a trusted source, such as the CSP or

trusted directory/database server), then the verifier takes on an additional role related to the reference biometric. In either case, when server based matching is performed, the verifier is no longer isolated from the biometric data. However, since for static biometrics it is the integrity rather than the secrecy that is of concern, the assumptions above do not hold. (Note, however, that it is incumbent upon the verifier to validate the integrity of the biometric data as part of the authentication process.)

A.3 Edits to Section 6 (Tokens)

Add to end (prior to 6.1):

- *Biometrics* – a live biometric sample that is compared to a previously registered biometric reference to verify identity. Processed biometric samples are typically binary records that represent the extracted unique features of the source characteristic (which may or may not be reconstructable from this biometric "template/model"). Biometric authentication does not rely on the knowledge or possession of a token per se, but the physical presence of the claimant. Thus for biometrics in general, and static biometrics in particular, the authentication protocol must address the "liveness" and integrity of the live sample that is presented for verification.

A.3.1 Edits to Section 6.1

Add to third bullet: "The replica may be used to construct an artifact for use in "spoofing" the biometric sensor or inserted at various points in the biometric processing or authentication protocol."

In the 2nd set of bullets, add:

- *Anti-spoofing mechanisms* can be incorporated into the biometric capture device and/or software. In the case of a behavioral biometric, this may include a challenge-response mechanism. Additionally, nonces, timestamps, and counters address related time-lag issues.

A.3.2 Edits to Section 6.2

Add after 3rd paragraph:

"Biometrics have different vulnerabilities/threats depending on the authentication architecture in use. All architectures involve the use of a biometric sensor and are thus vulnerable to sensor spoofing attacks, though these are not easily accomplished without collusion and/or sophisticated artifact manufacture (i.e., it is much more difficult than typing in a guessed or stolen password). Other threats which are unique to biometric authentication involve specific types of manipulation of data during storage, transmission, or processing – either the biometric data itself, the matching

threshold, or the match scores/decisions, though standard IT countermeasures (normal computer security controls) are available for these."

Add 5th bullet to end of 4th paragraph as follows:

- Biometrics can be used as follows:
  - Biometrics alone can be used at assurance levels 1 and 2.
  - Content-bearing biometrics can be used at assurance levels 1 through 3.
  - Biometrics can be used as a 2nd factor at all assurance levels (1 through 4).

A.4 Edits to Section 7 (Registration)

In this section, role of biometrics in the registration process needs to be addressed. To that end, the following recommendations are made:

At the end of Section 7 (before 7.1) add:

"To support biometric authentication, the applicant's biometrics must be enrolled by the RA during the registration process. As with other factors remote enrollment is possible, but engenders a higher risk that a set of biometric characteristics will be bound to the wrong identity. Therefore, the remote enrollment process should utilize a one-time password to access the capability and be limited to assurance levels 1 and 2. [Note that because biometric enrollment generally requires specialized equipment (sensor devices), remote enrollment may not be feasible at all in many circumstances.] All biometric enrollment records must be protected from unauthorized disclosure or modification."

A.4.1 Edits to Section 7.1

Add a second paragraph to 7.1.2 as follows:

"In some cases, it may be important that the same person is not permitted to register more than once, particularly with differing identities. To combat against this, biometric enrollment for the purpose of uniqueness (or duplicate) checking can be performed. By performing a one-to-many biometric search as a part of each registration, the RA can determine if the applicant is already registered under the same or different identity and make decisions accordingly. If biometric authentication is to be supported and if the same biometric modality is to be used, then the enrollment may also be used for that purpose. Note that some biometric modalities that are suitable for authentication are not suitable for uniqueness checking."

A.4.2 Edits to Section 7.2

Add a new paragraph at the end of 7.2.1 as follows:

"If biometric enrollment is performed as part of the registration or identity proofing process, an informed consent statement must be obtained from the applicant. This statement, in addition to containing the privacy policy for the biometric data, must address under what conditions the data will be shared with law enforcement."

A.5 Edits to Section 8 (Authentication Protocols)

Section 8 contains the details of how biometric authentication can be utilized at each of the four assurance levels.

A.5.1 Edits to Section 8.1

Change last sentence of first paragraph of 8.1.1. to read:

"Therefore, protocols that expose long-term authentication secrets more than is absolutely required, even to trusted entities, should be avoided, as should exposure to compromise of the integrity of biometric data."

Under the paragraph beginning "Specific attack mechanisms …", add to the end of the first bullet: "or obtain digital copies of biometric data."

Add to the end of "In-band attacks":

Biometric attacks, to include:

- Sensor spoofing, where an artifact is presented to the sensor in place of a legitimate biometric characteristic.
- Sensor substitution, where an untrusted sensor outputs a pre-programmed rather than live biometric characteristic.
- Hill-climbing attack, where the imposter uses returned match score information (when provided) to finely and incrementally alter the raw biometric input to achieve progressively increasing scores until the decision threshold is eventually exceeded.
- Biometric guessing or brute force attack, which capitalizes on a system using a biometric matching algorithm with a high false match rate (FMR) or an exhaustive set of biometric inputs, thus providing a higher than desirable likelihood that an arbitrary biometric feature presented to the system (a guess) will match.
- Output manipulation, where the value of a score or decision (in memory or during transmission) is changed prior to granting of access or where the value of the matching decision threshold is changed (lowered) such that submission of an illegitimate biometric sample is likely to result in a successful match. (For server based matching, this would require compromise of the verifier or its associated matching server.)

In section 8.1.2 (Resistance to Protocol Threats), add the following bullets:

- *Biometric attack resistance*: An authentication protocol is resistant to biometric attacks if it is impractical to utilize a biometric sample (either raw or processed) to achieve

successful authentication by introducing it at the sensor or by replay. For non-server-based matching, resistance includes making it impractical for decision-related parameters or data to be modified.

A.5.2 Edits to Section 8.2

Change end of first sentence to read "token/biometric."

A.5.2.1 Edits to 8.2.1 (Level 1)

Change end of last sentence of first paragraph of 8.2.1 to read "controls the token or provides the biometric."

At the end of 8.2.1 (before 8.2.1.1), add:

"Biometric data shall be encrypted during transmission (channel encryption is sufficient) and disk storage. Biometric references shall be signed upon creation. All biometric authentication architectures (implementing storage/matching on server, client, device, or physical token) meet Level 1 requirements. Biometrics may be used alone (in lieu of a token), to release a password/PIN or other token, or in conjunction with a token. Limits shall be placed on the number of biometric authentication attempts allowed in a given time period for each account (value to be selected considering FRR)."

Add to 8.2.1.1: "Note that although no lifetime requirements exist for biometrics at Level 1, some biometrics change over time and may require incremental or ongoing adaptive updating following successful authentication or re-enrollment after some period of time. Use of adaptation could extend the lifetime of the biometric."

At the end of 8.2.1.3, add:

"Protection of biometric data, either content-bearing or not, shall be via discretionary access controls. Additionally, biometric reference data shall be both signed/MACd (or stored within an X.509 attribute certificate) and encrypted when stored on a disk (i.e., server or client). Note that although static biometric data is not considered secret, encryption is required during transmission or when hardware protection is not used for both privacy protection (as biometrics are considered personal data) and to increase the difficulty of obtaining digital versions of this data that could possibly be used in system attacks."

At the end of 8.2.1.4, add:

"Biometric algorithms shall provide a maximum False Match Rate (FMR) of 1 in 100 (1%) at an operationally acceptable False Rejection Rate (FRR). (Note that biometric entropy and strength of function are not directly correlated.)"

At the end of 8.2.1.5, add:

"Many combinations of biometric technologies and storage/matching locations should be able to meet the requirements of Level 1. For example, a simple fingerprint scanner (with associated capture/processing software) could be installed on a client workstation and integrated with a browser. During authentication, the claimant's fingerprint is captured, signed, and transmitted over an encrypted channel (e.g., TLS) to the verifier where it is decrypted, its signature is validated, and it is matched against the registered (enrolled) fingerprint reference template (store on server/match on server architecture). Alternatively, iris recognition (client based) could be used to release a password or Kerberos ticket for use in a more traditional authentication protocol."

A.5.2.2 Edits to 8.2.2 (Level 2)

Change end of second sentence of first paragraph of 8.2.2 to read "controls the token or provides the biometric."

At the end of 8.2.2 (before 8.2.2.1), add:

"Biometric data shall be encrypted during transmission (channel encryption is sufficient) and disk storage. Biometric references and samples shall be signed upon creation. Only match-on-server biometric authentication architectures (with storage either on server, client, device, or physical token) meet Level 2 requirements unless combined with another token (i.e., biometrics can be used alone only when server based matching is performed). When used alone, limits shall be placed on the number of biometric authentication attempts allowed in a given time period for each account (value to be selected considering FRR)."

Change last sentence of first paragraph of 8.2.2.1 to read: "Shared secret or biometric based authentication systems may simply remove revoked subscribers from the verification database."

At the end of (or after) the second paragraph of 8.2.2.1, add "Note that revocation of a content-bearing biometric credential containing some shared secret will require re-enrollment when that secret content is changed."

Add to the end of 8.2.2.3:

"Files of biometrics used by CSPs and verifiers at Level 2 shall be protected by discretionary access controls that limit access to administrators and only those applications that require access. Such biometric files shall not contain unencrypted biometric references. Biometric references stored on hard disks (i.e., server or client) shall be stored in encrypted form using Approved encryption algorithms and modes and decrypt the biometric reference only when immediately required for matching (authentication). Biometric references stored in hardware devices or physical tokens (i.e., protected by hardware or mutual authentication read protection) are not required to be encrypted. In addition any method allowed to protect shared secrets at Levels 2-4 may be used for biometric data at Level 2. Additionally, stored biometric data shall be signed/MACd (or stored within an X.509 attribute certificate). Note that although static biometric data is not considered secret, encryption is required during transmission or when

hardware protection is not used for both privacy protection (as biometrics are considered personal information) and to increase the difficulty of obtaining digital versions of this data that could possibly be used in system attacks."

At the end of 8.2.2.4, add:

"Biometric algorithms shall provide a maximum False Match Rate (FMR) of 1 in 100 (1%) at an operationally acceptable False Rejection Rate (FRR). (Note that biometric entropy and strength of function are not directly correlated.)"

At the end of 8.2.2.5, add:

"Many combinations of biometric technologies and storage/matching locations should be able to meet the requirements of Level 2. For example, either of the examples of 8.2.1.5 would suffice, assuming other requirements of 8.2.2 are met."

A.5.2.3 Edits to 8.2.3 (Level 3)

Add to end of first sentence: "(except as noted below)."

After the 3 major bullets, add the following:

"In addition to the three token types above, biometric authentication may be used at Level 3 as follows:

- A content-bearing biometric with intrinsic, embedded secret (or challenge/response) content (2-factors) may be used with encryption of the live sample being performed using a shared secret key (or other, stronger cryptography which demonstrates key possession – 3rd factor). Channel encryption alone does not satisfy the encryption requirement. Any embedded password/passphrase must meet the requirements of Level 1 for authentication assurance. Encryption shall be performed using a cryptographic module validated at FIPS 140-2 Level 1 or higher overall.
- A biometric can be used to release a soft (or hard) certificate for use in an authentication protocol as described above.
- A biometric may be used as a 2nd factor to be verified at the verifier along with a one-time password or certificate-based protocol.

Additional requirements for biometrics used at Level 3 include the incorporation of an anti-spoofing mechanism within the sensor/software and the use of coarse scoring (to prevent hill-climbing attacks)."

Add to the end of the first sentence in the paragraph immediately following the bullets: "controls the token or provides the biometric."

Between the last 2 paragraphs, add:

"Biometric authentication has the advantage of being tightly bound to the human claimant. Because it is used in a multi-factor environment, biometric unique attacks are mitigated."

In the last paragraph, change the beginning to read: "All three token types and biometric alternatives present …" and delete "three" from the beginning of the second sentence.

Change the end of the first paragraph of 8.2.3.1 to read: "Shared secret and biometric based authentication systems may simply remove revoked subscribers from the verification database. Verifiers shall check to ensure that the credentials they use are valid. Additionally, all biometric data shall be signed/MACd or contained within an X.509 certificate – any of which may be revoked or otherwise invalidated."

In the first paragraph and numbered subparagraphs of 8.2.3.3 change each instance of "long-term shared secrets" to read "long-term shared secrets and biometric data".

At the end of 8.2.3.3, add:

"Additionally, stored biometric data shall be signed/MACd (or stored within an X.509 attribute certificate). Note that although static biometric data is not considered secret, encryption is required during transmission or when hardware protection is not used for both privacy protection (as biometrics are considered personal data) and to increase the difficulty of obtaining digital versions of this data that could possibly be used in system attacks."

At the end of 8.2.3.4, add:

"Biometric algorithms shall provide a maximum False Match Rate (FMR) of 1 in 1000 (0.1%) at an operationally acceptable False Rejection Rate (FRR). (Note that biometric entropy and strength of function are not directly correlated.)"

At the end of 8.2.3.5, add:

"When biometric authentication is used to release a certificate, then the client authenticated TLS (as stated above) is sufficient. If a content-bearing biometric is used or a biometric is provided as a second factor, then the tunneling method is required."

A.5.2.4 Edits to 8.2.4 (Level 4)

Add after 2nd paragraph:

"At Level 4, biometrics may only be used as a second factor, either to release the hard certificate or as a second factor that is seen at the verifier. In addition to the anti-spoofing and coarse scoring requirements of Level 3, a trusted biometric sensor device is required (i.e., meeting the common criteria requirements for the basic biometric protection profile). The biometric sensor may be embedded within the physical token carrying the hard cert, embedded in the reader

device for that physical token (e.g., smartcard reader), or a separate device. If the sensor is separate from the physical token, then mutual authentication of the biometric sensor is required.

Change the end of the first paragraph of 8.2.4.1 to read: "Shared secret and biometric based authentication systems may simply remove revoked subscribers from the verification database. Verifiers shall check to ensure that the credentials they use are valid. Additionally, all biometric data shall be signed/MACd or contained within an X.509 certificate – any of which may be revoked or otherwise invalidated."

In 8.2.4.2, add "or biometric data" after "long-term shared secrets".

A.6 Edits to Section 9 (Summary of Technical Requirements by Level)

Add Table 17:

Table 17 - Biometric Usage at Each Assurance Level

Biometric Authentication Type	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Biometric as a second factor	√	√	√	√
Biometric with content	√	√	√	
Biometric alone	√	√		

Add Table 18 (Same as Table 15 above):

Table 18 - Minimum Protection Requirements

Protect against	**Level 1**	**Level 2**	**Level 3**	**Level 4**
FMR attacks (guessing/brute force)	√	√	√	√
Database compromise		√	√	√
Sensor spoofing			√	√
Hill climbing			√	√
Untrusted sensor				√

Add Table 19 (Same as Table 16 above)

Table 19 - Maximum FMR Requirements

Requirement	**Level 1**	**Level 2**	**Level 3**	**Level 4**
FMR rate (not to exceed)	1 in 100	1 in 100	1 in 1000	1 in 1000

Notes:

1. FMR values are measured at a given, operationally acceptable FNMR.
2. Specification of FRR is left to the specific application requirements.
3. FMR is not increased between levels 3 and 4 because:
   - Multi-factor authentication is required at these levels, and
   - The strength of the other factors are increased (i.e., from soft certificates to hard certificates)

Extend Table 6 (In SP800-63) to add the following rows (or create table 6A):

Required Property	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Digital signature, MAC, or X.509 attribute certificate for biometric references	√	√	√	√
Encryption of biometric references stored on a hard drive (server or client)	√	√	√	√
Encryption of biometric references stored on a hardware device or physical token OR mutual authentication read protection			√	√
Digital signature, MAC, or X.509 attribute certificate for transmitted biometric samples		√	√	√
Encryption of transmitted biometric samples	√	√	√	√

Add Table 7 (In SP800-63) as follows:

Biometric Architecture	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Store on Server / Match on Server	√	√	w/content or cert	As 2nd factor
Store on Client / Match on Client	√	w/token		
Store on Device / Match on Device	√	w/token	w/content or cert	With or to release hard cert
Store on Token / Match on Server	√	√	w/content or cert	As 2nd factor
Store on Token / Match on Device	√	w/token	w/content or cert	With or to release
Store on Token / Match on Token	√	w/token	w/content or cert	With or to release hard cert

Annex B: Bibliography

B.1 Subject References

Below is a listing of documents referenced in of this report.

1. Stapleton, J., *American National Standard X9.84-2001 Biometric Information Management and Security*. 2001.
2. Ratha, N.K., *Cancelable Biometrics*. 2005.
3. Hao, F., R. Anderson, and J. Daugman, *Combining cryptography with biometrics effectively*.
4. IBG, *Vulnerabilities of Biometric Technologies - Transcript of September Teleconference*. 2005.
5. Matsumoto, T., et al. *Impact of Artificial Gummy Fingers on Fingerprint Systems*. in *SPIE*. 2002.
6. *Clarkson University Engineer Outwits High-Tech Fingerprint Fraud*. 2005 [cited; Available from: http://www.yubanet.com/cgi-bin/artman/exec/view.cgi/8/28878.
7. Mansfield, D.T. and P. Stratham, *BIOVISION Roadmap to Successful Deployments from the User and System Integrator Perspective*. 2003, BIOVISION.
8. Stratham, P. *Threat Analysis, How Can We Compare Different Authentication Methods?* in *Biometric Consortium Conference*. 2005. Arlington, VA.
9. Henry, E.R., *Classification and Uses of Finger Prints*. 1900, London: Routledge and Sons.
10. Ratha, N.K., J.H. Connell, and R.M. Bolle, *Enhancing security and privacy in biometrics-based authentication systems.* IBM SYSTEMS JOURNAL,, 2001. **40**(3).
11. Soutar, C., et al., *Biometric Encryption.* ICSA Guide to Cryptography, 1999.
12. Burr, W.E., D.F. Dodson, and W.T. Polk, *Electric Authentication Guidelines*. 2004, National Institute of Standards and Technology.
13. *Electronic Fingerprint Transmission Specification*. 2005, Federal Bureau of Investigation.
14. *Biometric Privacy Principles*. 1998, International Biometric Industry Association.
15. Hong, L., A. Jain, and S. Pankanti. *Can Multi-biometrics Improve Performance?* in *IEEE Workshop on Automatic Identification Advanced Technologies* 1999. Morristown NJ.
16. INCITS project 1790-D, Fusion Information Format for Data Interchange – 4th Draft, October 29-0950 (M1/06-0950)
17. ISO/IEC DTR 24722, Technical Report on Multi-Modal and Other Multi-Biometric Fusion
18. Chikkerur S. S. (2005). *Online Fingerprint Verification System.* Masters Thesis, State University of New York at Buffalo, Buffalo, New York.

B.2 M1 Documents

Following is a listing of all documents posted to the INCITS M1 document register related to the work of the AHGBEA and this report. All can be found at the following URL: http://m1.incits.org/m1htm/2006docs/m1docreg_2006.htm.

M1/05-0274	Terms of Reference
M1/05-0275	Call for participation/contrib. and 1st mtg announcement
M1/05-0294	Background – NIST Workshop presentations (Breakout session #2: Elements of Secure Biometric-Based Authentication Systems)
M1/05-0319	Transaction Security contribution (access ctrl for mobile)
M1/05-0341	OSS Nokalva contribution (BIP)
M1/05-0342	2-week agenda for Mtg#1
M1/05-0343	TBF contribution (getting started)
M1/05-0345	Background – NIST Workshop presentations (Architecture panel presentations)
M1/05-0351	ITU-T liaison statement on telebiometrics
M1/05-0352	SC27 liaison statement on BAC
M1/05-0408	Issues list
M1/05-0409	BioVision doc on security issues (PW protected)
M1/05-0410	Notes from Meeting #1
M1/05-0411	Call for contributions to Mtg #2/report
M1/05-0465rev	Meeting #2 announcement & draft agenda
M1/05-0514	Strawman report outline
M1/05-0515	Contribution on threat model framework
M1/05-0516	Contribution on a bibliography
M1/05-0568	2-week agenda for Mtg#2
M1/05-0590	Iridian contribution on application specific biometrics
M1/05-0689	Revised Terms of Reference
M1/05-0714	Call for contributions to the 1st working draft technical report
M1/05-0752	IBG contribution (Vulnerability of Biometric Technology – transcript of Sep05 teleconference)
M1/05-0754rev	Meeting #3 announcement & draft AHGBEA
M1/05-0755	DynaSig contribution (BioPen White Paper – Implementing OMB M-04-04 authentication levels)
M1/05-0756	Purdue contribution (Biometric identifier revocation & system security issues)
M1/05-0757	Purdue contribution on bibliography
M1/05-0758	Purdue contribution (response to M1/05-0714)
M1/05-0759	Bioscrypt contribution (Biometric Systems – Security Issues)
M1/05-0760	TBF contribution (Responses to questions about replacement of biometric data)
M1/05-0770	Transaction Security contribution (comments on M1/05-0514)
M1/05-0771	SAFLINK contribution (response to M1/05-0714)
M1/05-0772	Base Document for AHGBEA study report
M1/05-0801	2 week agenda or 3rd meeting of AHGBEA
M1/05-0853	AHGBEA report to M1.4 December meeting
M1/06-0022	Contribution from the Physiological/Behavioral Subgroup

M1/06-0023	Meeting announcement and draft agenda for 4th AHGBEA meeting
M1/06-0072	ITU-T (Telebiometrics) project summary
M1/06-0084	Contribution from the Peer Review Subgroup
M1/06-0085	Contribution from the Architecture Subgroup
M1/06-0086	Contribution from the Threat Model Subgroup
M1/06-0087	Contribution from the Revocation Subgroup
M1/06-0088	Contribution from the Authentication Concepts Subgroup
M1/06-0089	ACBio Project Summary (formerly BAC), Purdue Univ.
M1/06-0090	Template Protection Project Summary (Transaction Security contribution)
M1/06-0091	2-Week Agenda for the 4th Meeting of ADHGBEA
M1/06-0112	First Working Draft – Study Report on Biometrics in E-Authentication
M1/06-0117	"Biometric System Security" presentation by Anil Jain
M1/06-0135rev1	2nd Revision - Terms of Reference
M1/06-0179	Call for Contributions on Threat Model
M1/06-0207	Report to INCITS M1.4 – 21/22 February 2006 - 4th meeting report
M1/06-0209	Meeting Notes for the 4th Meeting
M1/06-0216	Report to INCITS M1.4 – 5 April 2006 (on Meeting #5)
M1/06-0306	2-Week Agenda for the 5th Meeting of AHGBEA
M1/06-0349	AHGBEA Issues List and Action Items
M1/06-0350	Iridian Contributions to AHGBEA
M1/06-0351	Purdue Contributions on Multimodal biometric systems
M1/06-0351	Presentation on FIPS 140-3
M1/06-0385	Call for Contributions and Extension of Previous Call on Threat Model
M1/06-0400	Meeting Notes for the 5th Meeting
M1/06-0415	VXML Forum Comments on & Contributions to AHGBEA
M1/06-0420	Transaction Security Contribution to AHGBEA
M1/06-0424	2nd Working Draft – Study Report on Biometrics in E-Authentication
M1/06-0430	Meeting Announcement and Draft Agenda for the 6th Meeting
M1/06-0436	Call for Comments/Contributions to Working Draft 2
M1/06-0437	2nd Revision – AHGBEA Issues List
M1/06-0439	DoD Contribution on Enrollment Function
M1/06-0440	Daon Contribution to the AHGBEA Report (on gaps)
M1/06-0495	Transaction Security Comments and Contribution on WD2
M1/06-0496	2-Week Agenda for the 6th Meeting of AHGBEA
M1/06-0512	Proposed Disposition of Comments on WD2
M1/06-0553	AHGBEA Report to M1.4 on Meeting #6 (12 June 2006)
M1/06-0554	3rd Revision – Terms of Reference
M1/06-0583	3rd Revision – AHGBEA Issues List
M1/06-0584	Meeting Notes for the 6th Meeting
M1/06-0585	Revised WD2 – Study Report on Biometrics in E-Authentication
M1/06-0611	Meeting Announcement and Draft Agenda for the 7th Meeting
M1/06-0642	3rd Working Draft – Study Report on Biometrics in E-Authentication
M1/06-0643	2-Week Agenda for the 7th Meeting of the AHGBEA
M1/06-0664	Call for Comments on WD3 of the AHGBEA Report
M1/06-0668	Transaction Security comments on WD3
M1/06-0669	Purdue comments on WD3

M1/06-0670	Biometric Bits comments on WD3
M1/06-0739	Meeting Notes for the 7th Meeting
M1/06-0806	2-Week Agenda for the 8th Meeting of the AHGBEA
M1/06-0916	5th Working Draft – Study Report on Biometrics in E-Authentication
M1/06-0940	Meeting Notes for the 8th Meeting
M1/06-0947	1st Letter Ballot on AHGBEA Final Report
M1/06-0989	2-Week Agenda for the 9th Meeting of the AHGBEA
M1/06-1026	Proposed Disposition of Comments on Letter Ballot (M1/06-1041)
M1/06-1027	6th Working Draft – Study Report on Biometrics in E-Authentication
M1/06-1027rev	Revised WD6 – Study Report on Biometrics in E-Authentication
M1/06-1041	Results of 1st Letter Ballot on AHGBEA Final Report
M1/06-1049	AHGBEA Report to M1.4 on Meeting #8/9 (14 Dec 2006)
M1/06-1091	4th Revision – Terms of Reference
M1/06-1093	Meeting Announcement and Draft Agenda for the 9th Meeting
M1/06-1094	Meeting Notes for the 9th Meeting
M1/07-0015	2-Week Agenda for the 10th Meeting of the AHGBEA
M1/07-0023rev	Revised Meeting Notes for the 10th Meeting
M1/07-0025	Comments on WD6 regarding Static/Dynamic, Biological/Behavioral
M1/07-0035rev	2nd Letter Ballot on AHGBEA Final Report
M1/07-0104	Results of the 2nd Letter Ballot on AHGBEA Final Report
M1/07-0157	Meeting Announcement and Draft Agenda for the 11th Meeting
M1/07-0183	Proposed Disposition of Comments on 2nd Letter Ballot
M1/07-0184	Approved Disposition of Comments on 2nd Letter Ballot
M1/07-0210	2-Week Agenda for the 11th Meeting of the AHGBEA
M1/07-0211	Transaction Security Comments on WD6rev
M1/07-0213	Meeting Notes for the 11th Meeting
M1/07-0214	AHGBEA Report to M1.4 on Meeting #10/11 (19 March 2007)

Annex C: Contributors

C.1 Technical Editing Team

Catherine J. Tilton	Daon	Chair, AHGBEA
Matthew Young	Purdue University	Report Editor

C.2 Contributors

The following companies and organizations provided written technical contributions towards this report:
Alphabetical by Company Name:

Organization	Name
Authentify	Andy Rolfe
Biometric Associates	John Hochstein
Bio Password	Dave Friant
Bioscrypt	Colin Soutar, Rene McIver
BioVision	Philip Statham, Tony Mansfield
CrossMatch	Greg Cannon
Daon	Cathy Tilton
DoD BTF	Dale Hapeman
DHS	John Mayer-Splain
DynaSig Corp.	Richard Kim
IBG	Victor Lee
Innove	Jeff Stapleton
Iridian Technologies	Jim Cambier
OSS Nokalva	Alessandro Triglia
NIST	Fernando Podio
Purdue University	Matthew Young, Shimon Modi
SAFLINK	Dustin Best
TBF	Fred Herr
Transaction Security Inc.	Rod Beatson
UPEK	Michael Chaudoin
Viisage	Jim Kottas
VoiceXML Forum	Judith Markowitz

C.3 Committee Members/Participants

The following individuals participated in the discussions and decisions of the AHGBEA in the development of this report.

Alphabetical by First Name of Participant:

Name	Organization	Name	Organization
Alessandro Triglia	OSS Nokalva	John Mayer-Splain	DHS
Andy Rolfe	Authentify Inc	Jon Agre	Fujitsu Labs of America
Anne Wang	Cogent Systems	Judith Markowitz	Voice XML Forum
Artour Karaguiozian	Motorola	Ken Gregory	Precise Biometrics
Arun Vemury	DoD	Kevin Farrell	Nuance
Axel Munde	BSI	Lisa Rajchel	ANSI, SC37 secretariat
Bart Elberg	BearingPoint	Matthew Doty	Dynasig Corp
Baruch Levanon	Idesia	Matthew Ennis	Lumidigm
Benham Bavarian	Motorola	Matthew Swayze	Daon
Bob Pinheiro	Consultant	Matthew Young	Purdue University
Cathy Tilton	Daon	Michael Crusoe	Authenti-Corp
Colin Soutar	Bioscrypt Inc.	Michael Hogan	NIST
Conor White	Daon	Micheal Davis	Assa Abloy ITG
Cynthia Lee Musselman	Adept Associates	Mike Beattie	Carnegie Mellon University
Dale Hapeman	DoD BMO	Mike Chaudoin	UPEK
Dale Setlack	Authentec	Mira LaCous	Bio-Key International
Dan Page	Integrated Biometrics	Nick Accomando	Retica Systems
Dave Benini	Aware	Patrice Yuh	FBI
Eric Winters	DOD	Peter Tapling	Authentify
Fernando Podio	M1 Chair	Philip Statham	CESG
Frank Acker	DoD	Richard Kim	Dynasig Corp
Fred Herr	TBF	Robert J. Bollig	Thomas Herbert Consulting
Geoff Olinde	EDS	Rod Beatson	Transaction Security Inc.
Gena Alexa	Unisys	Samir Tamer	Recognition Systems
Greg Cannon	Cross Match Technology	Sara Matzner	Southwest Research Institute
Gregory Zektser	DoD BMO	Scott Swann	FBI
Guy Cardwell	Motorola	Shimon Modi	Purdue University
Henry J Boitel	Biometric Bits	Shinil Cho	Technoimagia Inc
Jeff Maynard	Biosig-ID	Stark Draper	Mitsubishi Electric
Jeffrey Stevens	EDS	Steve Elliott	Purdue University
Jim Cambier	Iridian Technology	Tim Brown	Identix
Jim Kottas	Viisage	Tovah LaDier	IBIA
Jim Wayman	SJSU	Valorie Valencia	Authenti-Corp
Joe Ryder	CSLA	Walter Hamilton	IBIA/SAFLINK
John Campbell	NBSP	William Burr	NIST
John Hochstein	Biometric Associates	Zaida Candelario	IRS-Office of Privacy

C.4 M1.4 Members

The following were members of INCITS M1 task group 4 (M1.4) at the time of publication of this report.

Alphabetical by Member Organization:

Member	Representative(s)
BearingPoint	Rish Pathak, Bart Elberg
BioCom	Wayne Kyle
Biometric Associates	John Hochstein
Biometric Foundation	Fred Herr
Bioscrypt	Colin Soutar
Booz Allen Hamilton	Donald Waymire, Christopher Crooks
CrossMatch Technologies	Greg Cannon
CSC Identity Labs	Daniel Munyan, Rick Tomredle, Rick Lazarick
EDS	Jeff Stephens
ID Technology Partners	Mark Jerde
International Biometrics Group	Michael Thieme
L1 Identity Solutions	Kirsten Nobel, Tim Brown, Jim Kottas
NIST	Fernando Podio, Michael Hogan
Noblis	Larry Nadal, Donald D'Amato
OSS Nokalva	Alessandro Triglia, Paul Thorpe
Purdue University	Matthew Young
Retica Systems	Nick Accomando, Yasonari Tosa
The Biometric Foundation	Fred Herr
UPEK	Michael Chaudoin
US Army Biometrics Task Force	Dale Hapeman, Arun Vemury
US Dept. of Homeland Security	John Neumann, John Mayer-Splain

C.5 M1 Members

The following were members of INCITS technical committee M1 at the time of publication of this report.

Alphabetical by Member Organization:

Member	Representative(s)
ATMEL	Jean-François Mainguet
Authenti-Corp	Valerie Valencia
Authorizer Technologies	Omid Jahromi
Aware	David Benini
BearingPoint	Rish Pathak, Bart Elberg
BioCom	Wayne Kyle
Biometric Associates	John Hochstein
Biometric Foundation	Paul Collier, Fred Herr

Bioscrypt	Colin Soutar
Booz Allen Hamilton	Donald Waymire, Christopher Crooks
Cogent Systems	Anne Wang, Xian Tang
Computer Sciences Corporation	Rick Lazarick, Daniel Munyan
CrossMatch Technologies	Greg Cannon
Daon	Cathy Tilton, Matthew Swayze
EDS	Jeff Stephens, Jeffrey Poulson
Fujitsu Laboratories	Jonathan Agre, Gerry Byrnes
Geometrix	Thomas Maurer, David West
ID Technology Partners	Mark Jerde, Richard Chang
International Biometrics Group	Michael Thieme, Phil Youn
L1 Identity Solutions	Tim Brown, Keith Edwards
Motorola Inc.	Artour Karaguiozian, Guy Cardwell
National Biometric Security Project	Dominique Harrington, Gerald Williams
NIST	Fernando Podio, Michael Hogan, Michael McCabe
Noblis	Donald D'Amato, Larry Nadel
OSS Nokalva	Alessandro Triglia, Paul Thorpe
Precise Biometrics	Ken Gregory, Krister Walfridsson
Purdue University	Stephen Elliott, Matthew Young, Eric Kukula
Retica Systems	Nick Accomando, Yasonari Tosa
Underwriters Laboratory	Louis Chavez, Dave Mills
UPEK	Michael Chaudoin
US DoD Biometrics Task Force	Gregory Zektser, Dale Hapeman
US Dept. of Homeland Security	Brad Wing, John Neumann, John Mayer-Splain
US Dept. of State	Barry Kefauver, John Atkins
University of West Virginia	LaRue Williams, Arun Ross

Annex D: Role of Standards

D.1 Standards Organizations and Activities

D.1.1 Standards Organizations of Interest

ISO - International Standards Organization

- JTC 1 - Joint Technical Committee in the field of information Technology
  - SC 17 - Cards and personal identification
  - SC 27 - IT security techniques
  - SC 37 - Biometrics

NIST - National Institute of Standards and Technology

IETF - Internet Engineering Task Force of the Internet Architecture Board

- Security Area Directorate
  - The XML Digital Signature Working Group
  - Secure Mime Working Group
  - IETF Open PGP
  - IETF X.509 Public Key Infrastructure WG
  - IETF Transport Layer Security (TLS) WG
  - Incident Handling Working Group
  - Security Issues in Network Event Logging (SYSLOG) Working Group
- Media Resources Control Protocol (MRCP) – security for media service (notably, speaker verification and identification)

ITU - International Telecommunications Union

ANSI - American National Standards Institute

- X9 - Financial Services
  - X9F - Information & Data Security
  - X9F4 - Cryptographic Applications
    - X9.84 - Biometric Info. Mgmt. & Security
- INCITS - InterNational Committee for Information Technology Standards
  - M1 - Technical Committee on Biometrics
  - CS1 - Technical Committee on Cyber Security

VoiceXML Forum

Speaker Biometrics Committee – speaker verification and identification

W3C - World Wide Web Consortium

- SIV Committee of the Voice Browser Working Group – VoiceXML specification for speaker verification and identification
- Technology and Society Domain – Internet Security standards and protocols
  - XML Signature Working Group

- HTTP/1.1 – hypertext transfer protocol
- Electronic Commerce Interest Group – XML Signature, XML Encryption, Semantic Web, Micropayment Initiative, etc.

D.1.2 Relevant initiatives within other organizations

FIPS 140-2: Security Requirements for Cryptographic Modules
In May 2001, NIST produced Federal Information Processing Standards (FIPS) 140-2 to create baseline requirements for using cryptographic modules. Through NIST, there have also been some other FIPS standards which may be deemed relevant to the AHGBEA. This project is now moving towards version FIPS 140-3.

ITU-T: X.1081, *Telebiometric Multimodal Model Framework* (TMMF), Q.8/17
Telebiometrics System Mechanism (Ref: 37N1076)

The scope of the Telebiometrics System Mechanism (TSM) is the establishment of secure biometric authentication over open networks between client systems having unspecified (by TSM) biometric authentication technologies available and server systems (aka verifiers) having unspecified (by TSM) authentication policies. Its presumption is that the transaction between the client and server is of high enough value and exposed to sufficient risk that biometric authentication of the end user is a requirement.

TSM's scope includes the specification of:

1) Message protocols to establish secure sessions between clients and servers,
2) Preconditions required to support TSM,
3) Data formats for messages.

TSM does not define a particular authentication policy for servers, but identifies several attributes that such a policy should include, based on Common Criteria best practices. It also does not prescribe biometric technologies for clients, but identifies attributes that clients must have to qualify for use within TSM sessions.

It defines an authentication model with three possible storage/matching locations: client, server, or third party server. It includes a discussion of threats and countermeasures against each. It further identifies attributes that should be included in both the client and verifier's authentication policy.

ISO SC 27: Authentication Context for Biometrics (ACBio), ISO/IEC JTC 1/SC 27 N4126rev1
US Tag: ANSI/ INCITS CS1, Cyber Security

ACBio is an end to end authentication context for information systems that utilize biometrics. From the perspective of a remote entity wishing to make an application decision given a biometric system, ACBio aims to allow the remote entity to challenge the authenticity of each step that led to that biometric decision. This remote entity (verifier) will be able to mitigate the risks that a falsified template was utilized, or that a non-live sample was utilized, or that an

unreliable biometric device or algorithm was involved in the transaction. Given this information and the current application level policy, a verifier may then make a more informed decision about what action to take.

ACBio treats the processing steps defined in the general biometric models as separable events, each of which can act as a responsible agent for handling biometric information involved in a transaction. Each of these agents is responsible for responding to cryptographic challenges from the remote verifier that will allow the verifier to authenticate the biometric data. The cryptographic techniques are a combination of challenge-response, symmetric key and asymmetric key cryptography, and strong hash functions.

In addition, ACBio provides for the ability for a vendor who has taken the effort to have his implementation evaluated at a testing laboratory to deliver that signed certification report to the verifier, again to improve the decisions that the verifier must make while under varying threat levels.

ISO SC27: ISO/IEC 24745 - Information technology – Security techniques – Biometric template protection (Ref: 27 N4832 – 2nd WD – Jan 06)

US Tag: ANSI/ INCITS CS1, Cyber Security

ISO SC 27 Project 24745, Biometric Template Protection, recommends that templates are protected using distortion of the features/template to deal with revocation requirements and automatic key generation from the biometric sample for template encryption. Currently there appears to be some confusion as to the part that each technology will play in the process. There are a number of references quoted, some of which relate to one or the other of these techniques. With regard to template encryption and automatic key generation from the sample, it is not clear how this will affect the overall accuracy in terms of the biometric FRR/FAR and there are no references purporting to measure the resulting accuracy. It is recommended that this project be monitored but that there should be no recommendations from AHGBEA to include the techniques specified in SC 27 24745 at this stage.

ISO SC27: ISO/IEC 19792, Information technology – Security techniques - A framework for security evaluation and testing of biometric technology (4th WD)

US Tag: ANSI/ INCITS CS1, Cyber Security

ISO/IEC JTC1 SC 27 Committee Draft (CD) 2 19792, ***Security Evaluation of Biometrics***, provides high-level requirements that shall be addressed during a security evaluation of a biometric component, system or application. The requirements address security relevant error rates, vulnerability assessment, and privacy aspects of biometric technology. While the requirements are generic and independent from any specific evaluation methodology, they could form the basis for incorporating biometric evaluation into existing evaluation and certification schemes.

The CD provides guidance on the requirements for biometric security evaluations for both biometric system evaluators and biometric product developers. It covers only biometric-specific

aspects of a security evaluation. Non-biometric aspects, which would typically be addressed in an overall system security evaluation, are not addressed. The CD refers to and utilizes other biometric standards, notably ISO/IEC 19795, Biometric performance testing and reporting, developed by ISO/IEC JTC1 SC 37. These standards have been adapted as necessary for the specific requirements of biometric security evaluations.

ISO TC68: ISO DIS 19092, *Financial Services – Biometrics*
US Tag: ANSI X9F

ISO 19092 is the international counterpart to ANSI X9.84. ISO 19092 is currently being drafted, and there are slight differences from ANSI X9.84 (see D1.3. below). The requirements in ISO 19092 relating to biometric capture and data storage are currently identical to ANSI X9.84. ISO 19092 does not reference FIPS 140-2, however. Rather, the security level requirements are specified in an annex. ISO 19092 defines additional specific requirements relating to the transmission of biometric data. Biometric templates must be protected against substitution. In addition to authenticating the source and destination, biometric systems must also ensure the integrity of the data itself at the receiving end of the transmission.

W3C SIV Committee of the Voice Browser Working Group: SIV specification for VoiceXML v3.0

In 2005 both the VoiceXML Forum and the W3C established working groups in speaker verification and identification (SIV).

The Forum's group is called the Speaker Biometrics Committee (SBC). The mission of SBC is to:

- Identify use cases for voice-only and multimodal applications
- Develop requirements for developing an SIV module as part of the next version of the VoiceXML standard language (version 3.0)
- Review existing deployments and implementations of SIV that have been implemented as extensions to the existing VoiceXML standard (version 2.x)
- Develop a CBEFF-compliant, data exchange file format for SIV
- Develop best practices for user interface design, application architecture and other aspects of SIV development and management
- Engage in community/industry education and evangelism related to SIV

The group has published the following documents

- SIV Introduction and Best Practices Draft – document outline and draft of one chapter
- SIV applications – categorization and description of deployed applications and application types
- Speaker Identification and Verification (SIV) Requirements for VoiceXML Applications
- Data exchange file format Draft

These documents are available on the VoiceXML Forum Website
www.voicexml.org/resources/biometrics.html

The group is finishing an update of the requirements and data exchange file format documents and has also completed an SIV glossary which will be published soon.

The W3C's SIV Committee is a committee within the W3C's Voice Browser Working Group, the group that focuses specifically on standards for speech and voice. Its goals are:

- Translate the general requirements generated by the Forum's SBC into specific
- Construct an SIV module for VoiceXML version 3.0

The committee has completed work on its requirements. Those requirements were approved by the Voice Browser Working Group in September, 2006. The SIV committee has now turned its attention to creating the SIV module for VoiceXML 3.0

D.1.3 Existing Biometric Standards

D.1.3.1 ANSI/INCITS 358-2002 BioAPI

The BioAPI specification is a standard open system application programming interface (API) that provides a common method for a software application to communicate (generically) with underlying biometric technology services. Further, it does not dictate the method or location beneath the API where the biometric operations are performed.

BioAPI version 1.1 includes security features such as:

- Biometric Data Block which may be encrypted
- Entire BIR may be signed
- Header Field indicates security options
- No linkage of personal identifier or data

ISO/IEC 19784-1, BioAPI (International Version)

BioAPI version 2.0 retains all of the security functionality from version 1.1, as well as:

- Timestamp in header
- Expiration date in header
- Expanded security block

D.1.3.2 ANSI X9.84 Biometric Information Management and Security

ANSI X9.84 describes controls and procedures for using biometrics for secure remote electronic access or local physical access controls for the financial industry. The techniques specified in ANSI X9.84 are designed to maintain the integrity and confidentiality of biometric information and provide strong authentication. It defines a method for disparate systems to communicate biometric information in a common format.

X9.84 defines the following requirements related to capture, transmission, and storage of biometric data:

Capture. ANSI X9.84 establishes security requirements related to biometric capture for enrollment, but not other purposes. The requirements include:

- Establish mechanisms and procedures to ensure the operator is authorized to capture biometric information
- Establish mechanisms and procedures to ensure a person's claimed identity is properly verified (i.e. utilizing other documentation, such as a passport)
- Establish mechanisms and procedures to ensure biometric information is bound, or belongs to, the person during transmission, using cryptographic mechanisms or reference numbers.
- Biometric components must meet or exceed Federal Information Processing Standard (FIPS) 140-2 Level 2 requirements in a controlled environment, FIPS 140-2 Level 3 requirements in an uncontrolled environment
- Maintain the integrity and accuracy of biometric data throughout the biometric lifecycle

Transmission. ANSI X9.84 has established security requirements applying to the transmission of biometric data, including:

- Maintain integrity of biometric data using cryptographic mechanisms
- Mutually authenticate the source and destination, i.e. sender and receiver, using cryptographic mechanisms

The standard describes various cryptographic mechanisms, including:

- Digital signatures
- Message authentication codes (MAC)
- Encryption algorithms

Storage. ANSI X9.84 requires that biometric systems establish access control mechanisms to prevent unauthorized access to stored biometric data. The standard also allows for the encryption of data for privacy reasons, although this is not strictly required.

X9.84 utilizes the Abstract Syntax Notation version 1 (ASN.1) to facilitate transmission of biometric data in common language between systems.

ASN.1:
Encoding rules are sets of rules used to transform data specified in the ASN.1 language into a standard format that can be decoded on any system that has a decoder based on the same set of rules. ASN.1 and its encoding rules were once part of the same standard. They have since been separated, but it is still common for the terms ASN.1 and BER (Basic Encoding Rules) to be used to mean the same thing, though this is not the case. Different encoding rules can be applied to a given ASN.1 definition. The choice of encoding rules used is an option of the protocol designer.

The specific encoding schemes of ASN.1 is described in D.2

ANSI X9.84-2003

The current release of X9.84 implements XML and the XER encoding rules to create a data format similar to CBEFF. X9.84-2003 brought about the creation of XML common biometric format (XCBF) created by the Organization for the Advancement of Structured Information Standards (OASIS). XCBF focuses on converting between the BiometricObject data container with in X9.84 and BIR within CBEFF as well as the cryptographic methodologies in providing integrity and security of the biometric data being transmitted. Many of the data field names and types are similar, if not the same between the two conventions.

The XCBF data structure is described in D.3

D.1.3.3 INCITS 398:2005 (NISTIR 6529-A) and ISO/IEC 19785-1:2006, Common Biometric Exchange Formats Framework (CBEFF) Standards

CBEFF is a biometric standard that defines a set of data elements that are used to describe biometric data records using agreed record headers. CBEFF facilitates biometric data interchange between different system components or between systems, promotes interoperability of application programs and systems that use biometrics, supports forward compatibility for technology improvements, and facilitates the software and hardware integration process.

CBEFF conforming record headers can: (1) describe attributes of the biometric data that assist applications to determine whether the data is of interest to the application, especially the format of that data; (2) carry information associated with the biometric data, such as private keys or database indexes; and (3) describe the record's security attributes (digital signatures and data encryption). The CBEFF header specifies data elements relevant to e-authentication applications such as data elements that allow to time stamp the biometric data, allows to store a validity period for that data and allows to include payload data in the header.

There are currently two versions of CBEFF:

- ANSI INCITS 398-2005 (CBEFF 1.1). CBEFF was originally developed in a series of workshops jointly sponsored by the (US) National Institute of Standards and Technology (NIST) and the Biometric Consortium. CBEFF 1.0 was published as NISTIR 6529 in 2001. CBEFF 1.1 was published as NISTIR 6529-A, it was fast tracked as an American National Standard through INCITS in 2004 and was published by ANSI/INCITS in 2005.
- ISO/IEC 19785-1:2006 (CBEFF 2.0) is a standard developed by ISO/IEC JTC 1 Subcommittee 37 – Biometrics. This Subcommittee developed CBEFF 2.0 based upon CBEFF 1.0, with participation of experts of more than a dozen different national standards bodies.

D1.3.4 ISO/IEC 24708 Biometric Interworking Protocol (BIP)

The biometric interworking protocol specifies BioAPI framework-to-framework communication. BIP allows a BioAPI application to use a BSP on another framework to perform:

- Capture
- Enrollment

- Verification
- Identification

Level 2 of BIP is a fully functional BIP enabled framework. This architecture can support all BioAPI applications and BSPs from end to end.

Level 1 of BIP is simply a BIP endpoint. This architecture consists of self contained biometric devices with no BioAPI framework that can be controlled remotely by an application on a PC over the network.

Remote Authentication Using BIP

One possible way of using BIP in remote authentication is described below.

The main BioAPI application runs on a server that plays the role of the "verifier" in remote authentication. The server contains a BIP-enabled BioAPI framework which acts as the master framework. The subject's computer (client) contains a BIP-enabled BioAPI framework which acts as the slave framework. A biometric sensor is attached to the client, and is managed by a BSP installed on the client.

The BSP installed on the client is not used for doing biometric verification, but only for doing capture. Biometric verification is done by using a BSP installed on the server. The BSP installed on the client and the BSP installed on the server may either be the same BSP product or two different BSP products (if they are different products, the latter must understand the BDB format used in the BIRs created by the former).

The main BioAPI application running on the server uses both the (local) BSP on the client and the (remote) BSP on the server (at different times). The application calls BioAPI_BSPLoad and BioAPI_BSPAttach on the remote BSP in order to create a session for capturing biometric samples from the subject. It calls BioAPI_BSPLoad and BioAPI_BSPAttach on the local BSP in order to create a session for doing verification. The main BioAPI application drives the whole process as if it were operating with two local BSPs, passing BIRs from one to the other.
(It would also be possible for the main BioAPI application to use, for biometric verification, a BSP present on another computer altogether, also connected to the server by using BIP, and possibly hosting a biometric template database.)

Another BioAPI application runs on the client. The purpose of this BioAPI application is to support the capture process and to perform other services (not related to remote authentication) useful to the subject. The (secondary) BioAPI application manages a GUI and is able to display images and text received via incoming GUI event notifications.

Neither the secondary BioAPI application nor the BSP running on the client are required to be trusted by the server. One of the problems in remote authentication is that the verifier cannot be sure that the software running on the remote client is really getting input data from a biometric sensor. Traditional antispoofing techniques (as used in local authentication) may not be sufficient

in remote authentication because there may be no guarantee that the software on the client will really use the biometric sensor, or even that there is a biometric sensor at all.

In order to address this problem, certain features of BIP such as GUI event notifications and GUI event notification requests (e.g., BioAPI_NotifyGUIImageEvent) can be used to support a form of interactive capture, driven by the application on the server, where the application conveys instructions or challenges to the subject at the same time as it is collecting samples from the subject. Some forms of "remote liveness detection" can be achieved by analyzing the captured samples – which are supposed to be affected in some way by the reactions of the subject to the instructions or challenges received – to determine whether they reflect those instructions or challenges or not. Such techniques would be technology-dependent, but BIP would support them by providing the basic messaging infrastructure and API.

In detail, the functions BioAPI_NotifyGUIImageEvent and BioAPI_NotifyGUIStateEvent cause a GUI event to be generated within the endpoint that hosts a given BSP, as though the GUI event had been generated by the BSP. These functions are not useful in a local BioAPI system configuration (because the GUI event notification would be sent to the same application that calls BioAPI_NotifyGUIImageEvent or BioAPI_NotifyGUIStateEvent), but, in a distributed system configuration, these functions enable the main BioAPI application to forward GUI event notifications (received from a BSP) to a secondary BioAPI application that interacts with a user (either the subject or an operator). In remote authentication, this mechanism supports conveying arbitrary images and text to the subject, while the BSP is performing a capture under the control of the application on the server.

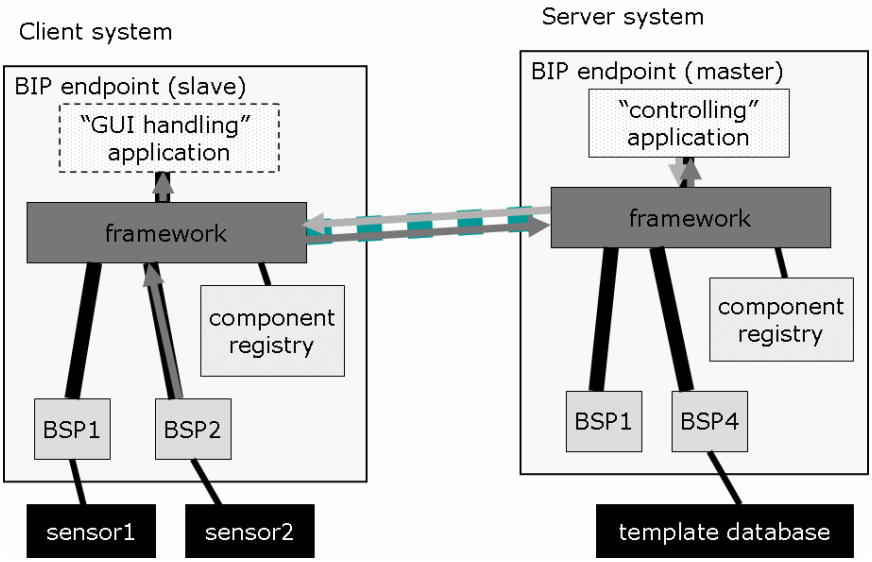

Figure 29 - BIP Architecture

D.1.3.5 IETF MRCPv2

Internet protocol for Chapter 11 Speaker Verification and Identification and Chapter 12 Security Considerations. The MRCPv2 protocol allows client hosts to control media service resources including speaker biometrics systems residing in servers on the network. Security considerations for MRCPv2 are specified in *Media Resource Control Protocol Version 2* and in Oran 2003.

MRCPv2 also specifically supports secure Internet transport layer protocols such as TLS, HTTPS, FTPS, and SIPS.

D.2 Encoding schemes of ASN.1

The ASN.1 encoding rules currently standardized are: Basic Encoding Rules (BER), Distinguished Encoding Rules (DER), Canonical Encoding Rules (CER), Packed Encoding Rules (PER), XML Encoding Rules (XER) and Extended XML Encoding Rules (E-XER).

BER: was created in the early 1980s and is used in a wide range of applications, such as Simple Network Management Protocol (SNMP) for management of the Internet; Message Handling Services (MHS) for exchange of electronic mail and TSAPI for control of telephone/computer interactions.

DER: is a specialized form of BER that is used in security-conscious applications. These applications, such as electronic commerce, typically involve cryptography, and require that there be one and only one way to encode and decode a message.

CER: is another specialized form of BER that is similar to DER, but is meant for use with messages so huge that it is easiest to start encoding them before their entire value is fully available. CER is rarely used, as the industry has locked onto DER as the preferred means of encoding values for use in secure exchanges.

PER: is more recent than the above sets of encoding rules and is noted for its efficient algorithms that result in faster and more compact encodings than BER. PER is used in applications that are bandwidth or CPU starved, such as air traffic control and audiovisual telecommunications.

XER: (XML Encoding Rules) allow you to encode a message that has been defined via ASN.1 using XML. You can now add visibility to your ASN.1-described messages via XML.

E-XER: (Extended XML Encoding Rules) is an amendment to the ITU-T Rec. X.693 (23002) ASN.1 Encoding Rules: Specification of XML Encoding Rules (XER). Extended-XER encoding makes ASN.1 an XML schema notation as powerful as XSD, with the simplicity of ASN.1.

D.3 XCBF data structure

D.3.1 Biometric Header

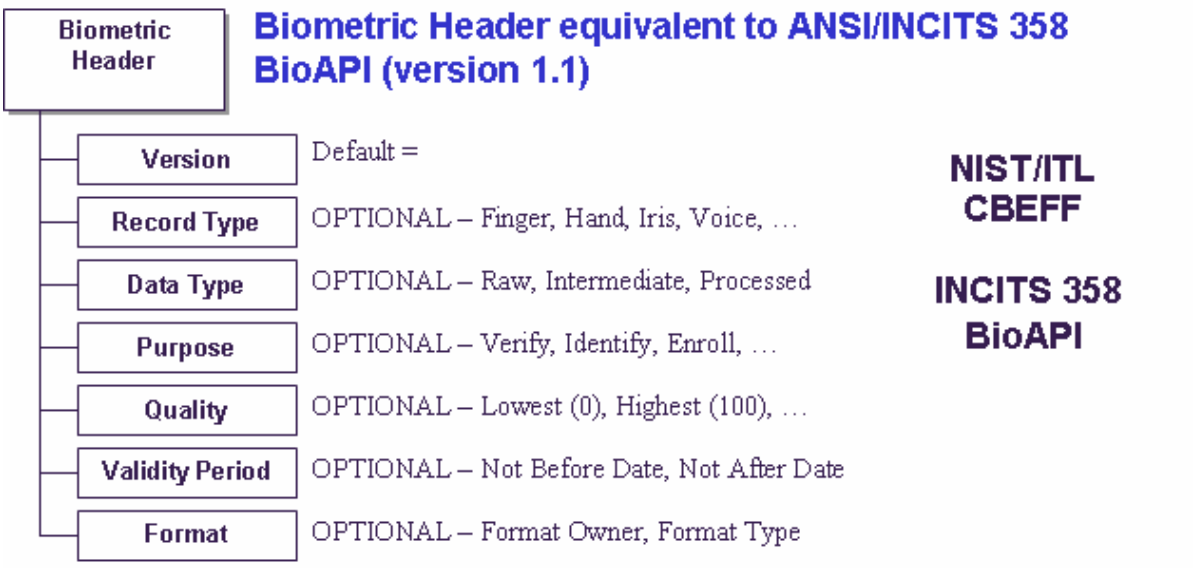

Figure 30 - XCBF Biometric Header

D.3.2 Biometric Object

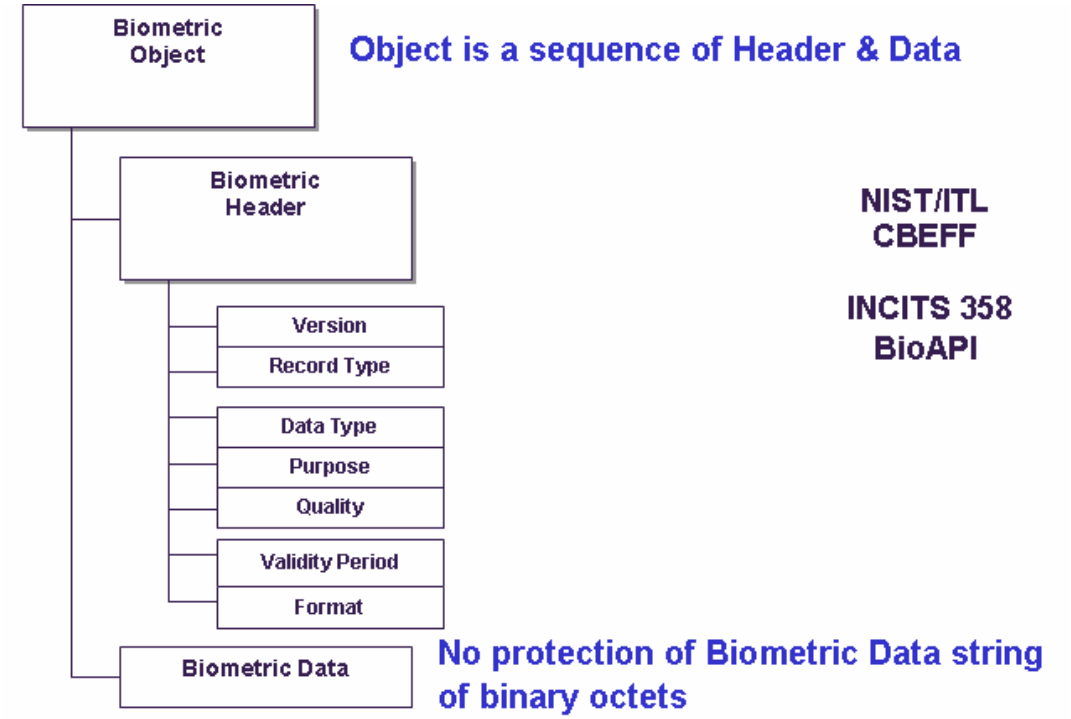

Figure 31 - XCBF Biometric Object

D.3.3 Integrity Object

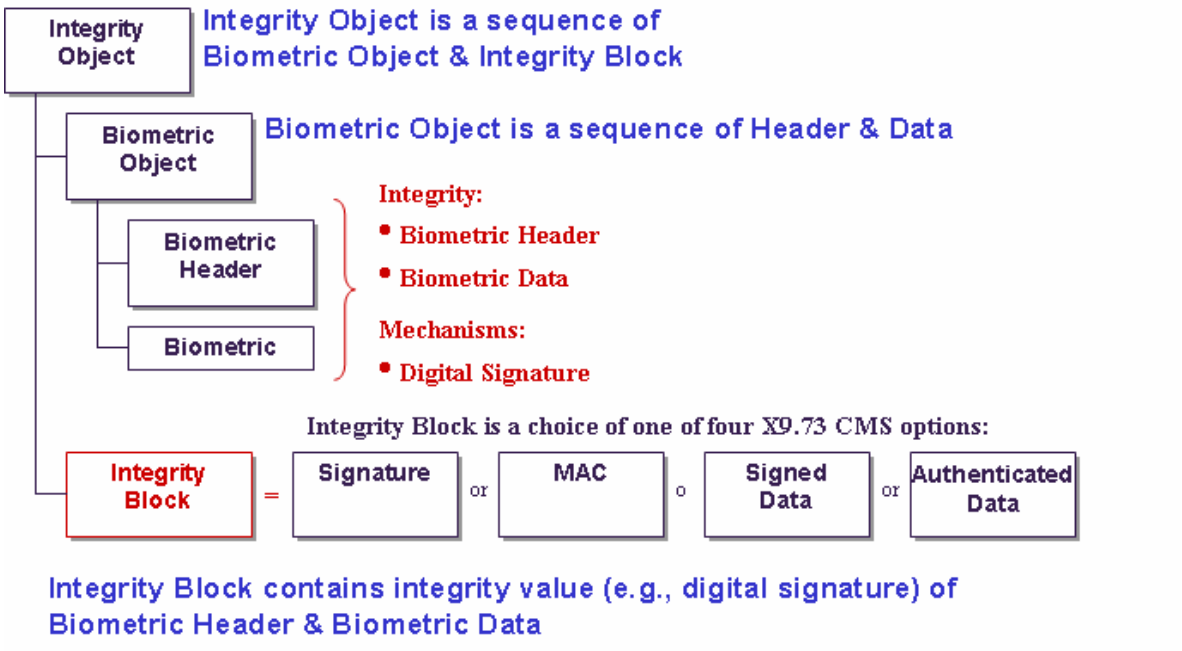

Figure 32 - XCBF Biometric Integrity Object

D.3.4 Privacy Object

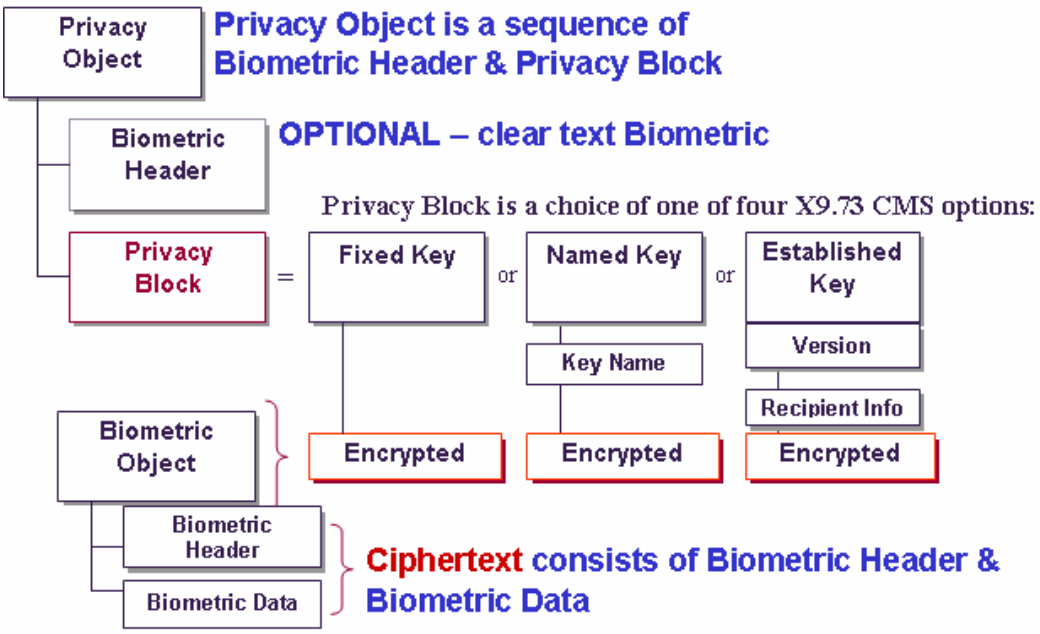

Figure 33 - XCBF Privacy Object

D.3.5 Integrity and Privacy Object

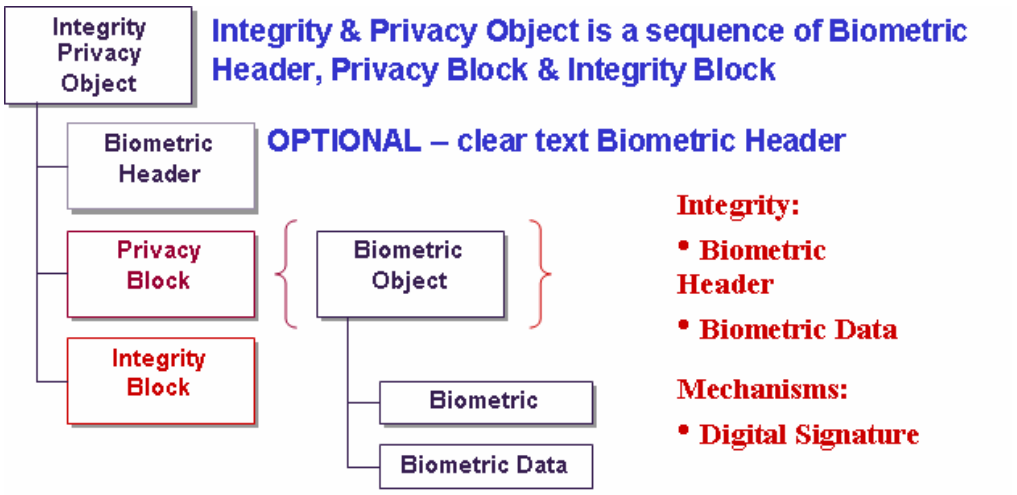

Figure 34 - XCBF Integrity and Privacy Object