



## **White Paper:**

**Biometrics as a Privacy Enhancing Technology**

By Walter Hamilton

Vice President, Business Development

**SAFLINK Corporation**

## **Biometrics as a Privacy Enhancing Technology**

SAFLINK has implemented biometric authentication for workstation and network access as a more secure, convenient and cost-effective technology for user authentication when compared with passwords, PINs and tokens. Biometric technologies provide “strong authentication” that can protect corporate information assets from being accessed by unauthorized persons. As such, biometrics should be viewed as a “privacy enhancing technology”. Even so, organizations that choose to deploy biometric authentication also need to educate their user population, who may be unfamiliar with the science of biometrics, to explain how the biometric data itself will be protected against theft or inappropriate sharing.

### **Behind the Science**

The key to the protection of biometric data is based on the science of how biometrics work. Biometrics is the automated process of identifying a person by comparing their unique physiological or behavioral characteristics. In SAFLINK’s implementation of biometric authentication, the biometric data is not stored or transmitted in the form of an image of the original biometric representation. Instead, this image data (such as a fingerprint image) is reduced at the point of initial capture into the form of a binary data string (or “template”) that is derived from the image representation through an algorithm that is proprietary to the specific type of biometric used. The image data is then immediately discarded. One can think of the template as a “one-way” hash of the original image data that, by itself, cannot be used to ascertain information about a person such as appearance, age, sex, race, medical condition or any other personal characteristic either directly or indirectly. Biometric templates cannot be reverse-engineered to recreate the original image data. Therefore, biometric templates cannot be stolen and used to derive personal information and, standing alone, cannot be reconstructed into the original image to reveal identity characteristics.

Due to these inherent attributes, the use of biometrics is regarded by the European Union (EU) and other data protection experts to be the most powerful means to secure privacy and deter identity theft. Only biometrics can provide a protective shield sufficient to meet this standard.

### **Fingerprint Technology**

The most widely used biometric is fingerprint technology. Among the techniques offered for biometric fingerprint authentication are specific matching algorithms. Although each algorithm is unique to the manufacturer, in general these matching algorithms fall into one of two categories:

1. Minutiae-based algorithms measure points on the fingertip where ridges end and where a ridge splits into two ridges (bifurcations). These data points, and the relationships between the points, are then converted into a piece of binary data (a large number that expresses the locations of these points against an XY axis) and stored, encrypted, in the central repository. Even if the algorithm could be hacked and reverse-engineered, it would never yield a fingerprint – just a set of points with no indication of what the print actually looks like.
2. Pattern-based algorithms break the fingertip into a set of individual areas or cells and analyze specific attributes within each cell. Examples of attributes analyzed would include ridge angle, ridge spacing, and phase offset. This data is then compiled into an identifier and stored as the user's unique biometric template. Some pattern-based algorithms may also include minute sections of fingerprint image data.

There are examples where a fingerprint technology vendor (e.g., Precise Biometrics) has chosen to use a "hybrid" algorithm that incorporates components of both minutiae-base and pattern-based algorithms.

### **Additional Protections**

SAFLINK's implementation of biometrics for securing workstations and enterprise networks provides additional protections to ensure that the biometric templates are not compromised or inappropriately accessed.

First, the templates are fully encrypted immediately after they are created. When the templates are transported over a network, they are in encrypted using one-time keys that are time stamped and unique for each transmission event. When the templates are stored in a data file, they are stored using strong encryption methods such as triple DES.

As part of SAFLINK's comprehensive set of security features, SAFLINK also adds information to the stored enrollment template format to make these templates separate and distinct from the authentication templates created when the user logs on to the system. Therefore, even if the originally stored template was somehow stolen from the database, decrypted and played back to the system as a fraudulent verification attempt, it would fail because enrollment templates cannot be used as verification templates. The fraudulent attempt would be immediately rejected.

### **Privacy Principles**

Even with the preceding extraordinary protections provided for the biometric templates, it is important for data controllers to implement appropriate technical, organizational and

operational measures to ensure that biometric templates will be properly handled and used only for their intended purpose.

With biometrics widely confirmed to be the tool of choice to protect personal privacy and business information, it is critical to ensure that a high degree of user confidence is achieved when biometrics are deployed for use. To resolve confusion over unfamiliar technology and establish a uniform approach that is beneficial to both government and business, the International Biometric Industry Association (IBIA) adopted its Privacy Principles in 1999. IBIA is the biometric industry official trade association that provides public awareness and education about biometrics as well as advocacy to public policy makers. IBIA's Privacy Principles have been used to draft corporate policy, public policy, legislation and regulations that promote the responsible use of biometrics. SAFLINK is an active member of the IBIA, serving on its board of directors, and strongly supports the following IBIA Privacy Principles:

1. Biometric data is electronic code that is separate and distinct from personal information, and provides an effective, secure barrier against unauthorized access to personal information. Beyond this inherent protection, IBIA recommends safeguards to ensure that biometric data is not misused to compromise any information, or released without personal consent or the authority of law.
2. In the private sector, IBIA advocates the development of policies that clearly set forth how biometric data will be collected, stored, accessed, and used, and that preserve the rights of individuals to limit the distribution of the data beyond stated purposes.
3. In the public sector, IBIA believes that clear legal standards should be developed to carefully define and limit the conditions under which agencies of national security and law enforcement may acquire, access, store, and use biometric data.
4. In both the public and private sectors, IBIA advocates the adoption of appropriate managerial and technical controls to protect the confidentiality and integrity of databases containing biometric data.

The IBIA Privacy Principles have proven to be an excellent guideline for establishing policies that allow companies and government agencies to adopt biometrics in a manner that is transparent to the public, can be controlled by the person whose biometric has been captured, and can be safely stored by the user.