FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

A Best Practices Guide to Fingerprint Biometrics

Ensuring a Successful Biometrics Implementation

A Frost & Sullivan
White Paper

Rob Ayoub, CISSP
Global Program Director,
Information Security
and
Chris Rodriguez,
Industry Analyst,
Information Security

www.frost.com

CONTENTS

EXECUTIVE SUMMARY

Biometrics is a unique approach to identity management that offers user convenience, increased security, cost-effective provisioning and a non-repudiated, compliant audit trail for the system operator. Traditional credentials or specialized knowledge—tokens or passwords—cannot guarantee that the person using the system is the authorized individual. In addition, these forms of identification can be frustrating for users and expensive for system operators.

Given the benefits of biometrics, why is it not pervasive or preferred? Simply put, the knowledge required to design and deploy a successful biometric system is not widely available. And, until recently, the technology was not reliable enough to provide the expected return on investment (ROI).

This paper encapsulates the best practices associated with the design and deployment of fingerprint biometric systems. The reader will learn how to avoid common pitfalls, ensure the system meets user and operator expectations, and deliver the required ROI.

Frost & Sullivan intends this paper to be approachable, informative, and understandable to senior executives that want to know more about what it takes to deploy biometrics in their organizations and reap the benefits of their investment. It is not a technical cookbook, but rather is a basis for asking questions and evaluating design choices to ensure that each fingerprint biometric deployment produces the expected returns from the first day of deployment.

CHALLENGES OF IDENTITY AND ACCESS MANAGEMENT (IAM)

Organizations are demonstrating a growing interest in identity and access management (IAM) solutions. This interest is fueled by compliance mandates, such as the Health Insurance Portability and Accountability Act (HIPAA) and the recognition that a higher percentage of organizations' assets are digital. Poorly controlled access to these assets can result in significant damage to the organization and its ability to effectively serve its customers. IAM systems provide a means to cost-effectively manage identities and the entitlements each person has to enterprise assets.

Identification and Provisioning

Properly securing organizations comes down to managing who can do what, when. The most important component in this equation is the concept of "who." Is the possession of a user ID/password pair equivalent to "who"? How about the possession of an employee badge and a password? Both are pervasive and accepted standards—but neither, in a non-repudiated sense, identify a person. It is this very fact that is the source of significant IAM vulnerabilities. These vulnerabilities, in turn, drive system complexity and cost.

Convenience and Costs

Traditional IAM systems cannot determine identity and instead use PINs and passwords as identity stand-ins. These stand-ins are vulnerable to exploitation; elaborate means to make them strong also make them forgettable and in convenient. Smart cards or employee badges add cost to system administration while effectively publishing a portion of the identity, making strong passwords even more important. Password loss, theft, and reissuance impose productivity costs and create security vulnerabilities.

The ideal IAM system would be one offering both security and convenience. A properly designed and implemented fingerprint biometric system is a viable way to accomplish both objectives.

IMPACT OF FINGERPRINT BIOMETRICS ON THE ROI OF AN IAM

It is imperative that organizations implement biometric solutions with strict adherence to industry best practices. If not, then the solution will not operate to its fullest capacity and will cost the organization time and money in the end. The IAM ROI revolves around the automation of identity management and provisioning so that manual processes can be eliminated while still ensuring that the overall system meets operating cost, user convenience, system security, and compliance objectives. There are some additional important factors that are not often considered in the IAM ROI equation:

- What is the productivity loss that is experienced each time someone's access credentials become lost or compromised?
- Can identity be challenged (repudiated) either by an employee accused of fraud or an auditing agency challenging the validity of internal controls? What does it cost the enterprise to resolve these disputes?
- What is the cost involved to create, manage, and replace physical credentials such as employee badges or smart cards?

Fingerprint biometrics improves the IAM value proposition by allowing a person's actual identity to become part of the identity management equation. Consider the following:

- A fingerprint can replace a badge or other physical credential and offer the same level of secure access while eliminating cost involved in creating, replacing, and managing the credential. Much of the potential IAM automation benefit can be found here.
- A fingerprint is a non-repudiated form of identification that cannot be challenged in the same way a user ID/password can.

- Systems using a user ID/password pair can be changed to a user ID/fingerprint pair providing the same level of security while eliminating physical credential and password management costs.

- Knowing with certainty "who" the user is allows information services and data availability to be easily tailored to that particular individual, making the security solution one that enables productivity rather than blocks the user from getting the job done.

In summary, a fingerprint biometrics solution significantly improves the IAM ROI by offering system operators a higher level of security, non-repudiated identification for internal control and/or regulatory compliance, and increased user convenience and productivity—without the costs associated with physical credentials. The following sections explore in more detail how fingerprint biometrics is a cost-effective solution to IAM challenges.

FINGERPRINT BIOMETRICS AS A SOLUTION TO IAM CHALLENGES

Fingerprint biometrics identifies a user in a non-repudiated way. It can enhance user convenience, reduce (or even eliminate) credential management costs and provide user-specific provisioning. Biometric transactions are auditable and non-repudiated. As a result of these benefits, many organizations are adopting fingerprint biometrics for identity management.

A fingerprint is unique—and copies can be detected and prevented. This is in sharp contrast to user IDs and passwords, which can be easily replicated and used instantaneously by sophisticated electronic programs to gain access to valuable enterprise assets. Combining a credential (i.e., a badge or other token) with a password is much more secure. The credential can be perfectly identified with some electronic means to detect presence and authenticity. But who has the credential?

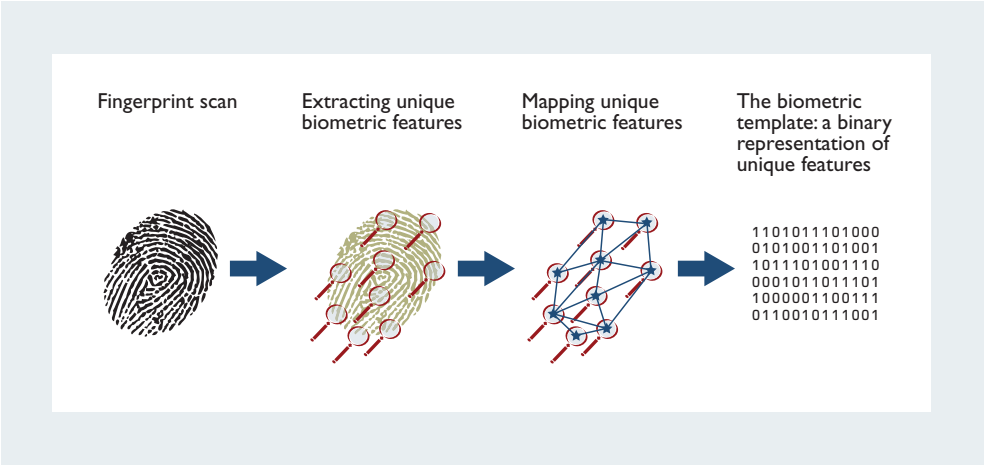
Fingerprint Biometrics Process Overview

Consider an overview of how fingerprint biometrics systems are used in identity management applications. The basic fingerprint biometric processes are:

- **Enrollment scans**—The user's fingerprints are scanned and associated with that user's identity in the system. This is normally a supervised process to allow for preventing false identity creation and propagation. In an enterprise scenario, enrollment would be done at the time a person becomes employed and only needs to be done once.

- **Template creation and storage**—A biometric template is created from biometric features derived from the scanned fingerprint. The enrollment template becomes the fingerprint biometric record for the user. In some solutions, the fingerprint scan itself may also be stored. See Figure 1.

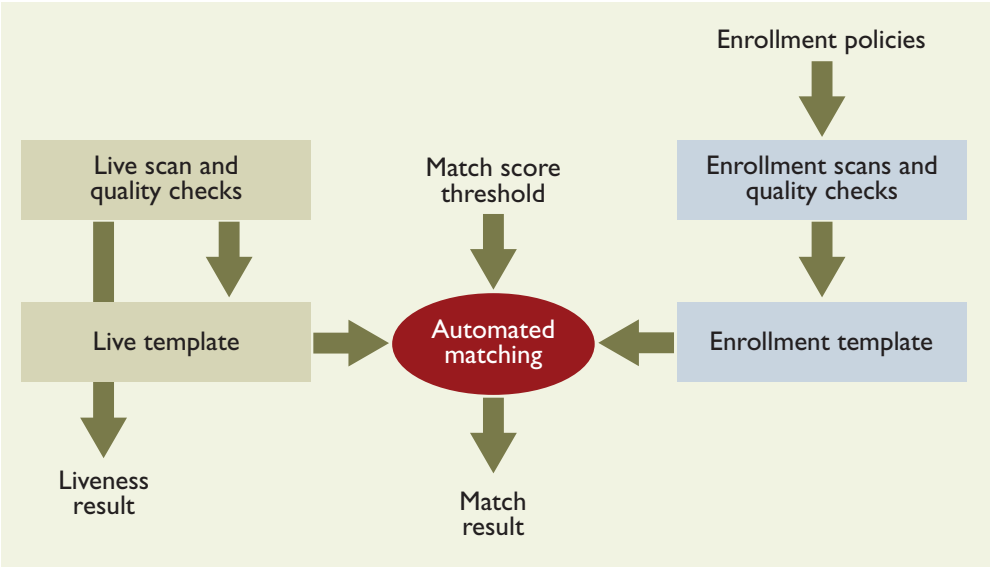
Figure 1—Biometric Template Creation
Fingerprint scans cannot be reconstructed from templates.



- **Live scan**—Each time a person requests access to the system, a live scan of the fingerprint is made and a live template is derived from that scan. The scanner may also perform a liveness measurement, which can distinguish between an artificial copy of the fingerprint and a "live" finger and thus validate the authenticity of the fingerprint.
- **Automated matching**—The live template is compared to a specific enrollment template and a matching score is generated. Scores greater than a threshold are considered a match.

The basic fingerprint biometric processes are shown in Figure 2.

Figure 2—Fingerprint Biometrics Process Flow



Ways to Implement Fingerprint Biometrics in IAM Systems

There are several different ways to use these basic biometric operations in an identity management system. Some examples are:

- **Physical credential with biometric template**—The biometric enrollment information is stored on a credential—for example a card or ID token—in a format that can be automatically authenticated and cannot be copied. After the credential is presented to the system and an authenticity check is performed, a live scan of the cardholder's finger is taken and compared against the enrollment template for a match. This two-factor[1] approach is self-contained and can be used in situations where network access to the IAM system is not present by design or by outage.

- **Password replacement**—Users are assigned user IDs and their fingerprints are used as passwords. At enrollment, the user ID is associated with the enrollment template. Each time a user ID is presented by a user requesting access, the system retrieves the enrollment template associated with that user ID and compares it to the user's live scan. This is another example of a two-factor system. Compared to passwords, fingerprints allow faster transaction times and eliminate password management productivity losses and reissuance costs.

- **Single-factor authentication**—The fingerprint is used as both the user ID and the password. At enrollment, the user's enrollment template is added to a database containing all other user enrollment templates. Each time someone presents a finger to the system, the entire database is searched and the user credentials are retrieved. This approach can be called a one-to-many search or 1:N. A single-factor fingerprint system maximizes convenience and eliminates the need for a physical credential or the need for a user to remember a user ID. However, it becomes less accurate and less secure as the number of enrolled users increases.

Accuracy Requirements

As we have just illustrated, there are several ways to implement fingerprint biometrics in an identity management system. The choice of approach is largely driven by the accuracy requirements of the application. Accuracy—the ability to reliably authenticate an individual—depends upon the amount of biometric data collected as well as the reliability of collecting that data each and every time a fingerprint is scanned. Accuracy requirements vary from application to application.

---

[1] Factors, in the context of authentication, refer to the type of information the user is required to provide in order to be authenticated. Typically, the factors answer the question "something the user ___ ". For example, a password is something the user knows, a card is something the user has, and a biometric is something the user is.

A single fingerprint scanned with a high-quality scanner will produce 30 to 50 unique biometric features that are stored in the biometric template (Figure 1). If the system uses a two-finger scanning approach, the amount of information collected is doubled. Such a system is more accurate than a single-finger system. Single-finger, two-finger, four-finger, and palm scanners are available on the market today.

Increasing the number of authentication factors also increases accuracy. For example, a two-factor system where a single-finger scan is compared against a single enrollment template contained in a smart card or accessed via user ID is considered strong enough to accurately support an unlimited number of users. The smart card approach has the added benefit of being usable when the identity database is unavailable, as in the case of a remote physical access device without a network connection.

When a one-to-many (1:N) search is used, performance is reduced as users are added. Performance can be improved if the amount of data per person is increased. For example, a single-factor system where each user enrolls with one finger is considered sufficiently accurate when the number of users is 1,000 to 3,000. A two-factor approach or a two-finger approach should be used when the number of users is larger than this. A two-factor system is always more accurate than a single-factor system.

Table 1 illustrates the accuracy, given the number of users, of a variety of single-finger solutions.

Table 1—Relative Accuracy of a Biometric System Based on Number of Users

Accuracy Level	Single-Finger Usage Case
High	Two-factor fingerprint system: • Physical credential plus fingerprint • User ID plus fingerprint (password replacement)
Medium	Single-factor fingerprint; fewer than 3,000 users
Low	Single-factor fingerprint; more than 3,000 users

Major Factors Affecting Fingerprint Biometric System Accuracy

While fingerprint biometric systems are known for their ability to accurately authenticate an individual, there are numerous factors that affect this ability. Users must consider the following factors as they choose a fingerprint biometric solution:

- **Live scan quality**—Live scan quality directly affects the number of biometric features that can be extracted from the fingerprint. Remember that the number of features is directly related to overall biometric system performance. The scan device must reliably deliver high-quality fingerprint scans each and every time the scanner is used and under all use scenarios.

- **Enrollment scan quality**—Poor enrollment scan quality permanently degrades accuracy for that user and drags down overall system performance. Thus, a higher standard of fingerprint scan and biometric template quality should be applied to the enrollment process.

- **Scan device usability**—The location and orientation of the scanning device should be such that the user can quickly and accurately place their finger in a manner that reliably leads to a high-quality live scan with one touch.

- **User skin condition**—Many types of scanners are sensitive to user skin conditions and placement pressure since they rely on a measurement approach that only differentiates areas in contact with the scanner (fingerprint ridges) from areas not in contact (valleys). As a result, dry or damp skin can degrade the quality of the live scan, as can surface contaminants or variability in pressure applied to the sensor by the user.

- **User fingerprint expression**—Some individuals have poor fingerprint expression or very fine fingerprint features. In addition, as a person becomes older, the collagen level in the skin is reduced enough to cause complications in fingerprint scan reliability.

- **Closed vs. open biometric systems**—An open system is one where a variety of fingerprint scan devices, biometric template generators, and automatic biometric template matchers are used. Open or interoperable systems offer convenience in the design and implementation of the system. However, open systems have lower performance because of least common denominator effects.

- **Liveness detection**—A scanner with liveness detection is one that prevents the use of copies of the fingerprint to be used. This includes means to prevent the activation of a latent print, the use of a 2-D paper copy, or the use of a sophisticated 3-D copy. A scanner lacking this capability will accept copies, and this would result in a system breach similar to a stolen user ID/password pair.

Fingerprint Biometric Performance: A Primer

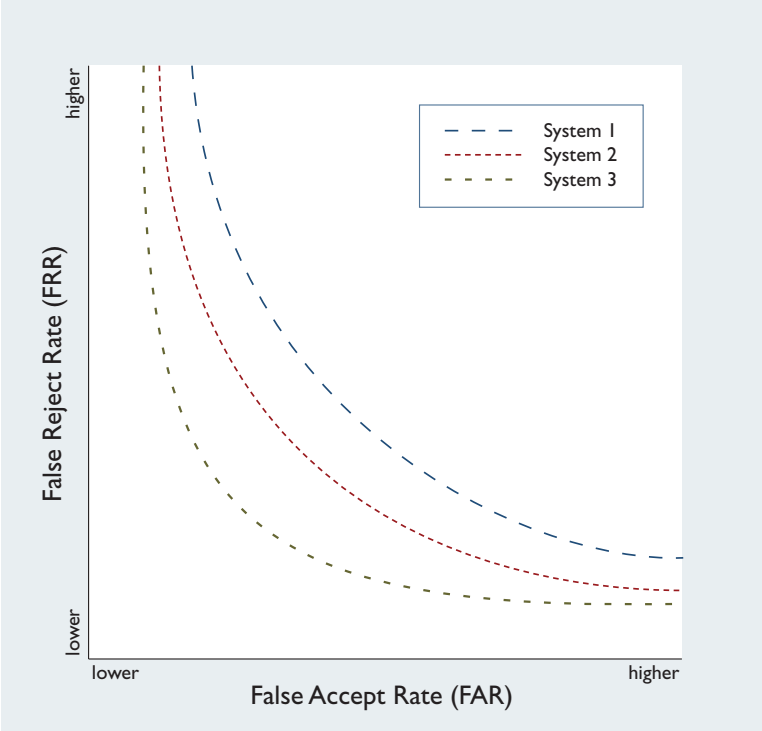
Before presenting the Frost & Sullivan best practices for implementing a fingerprint biometrics solution, we recommend becoming familiar with how biometric performance in automated systems is discussed and evaluated.

Automated biometric matching produces a match score that represents how similar the live scan is to a particular enrollment template. The higher the match score, the higher the probability that the live scan is from the enrolled individual (a genuine match); a low score may indicate that the live scan is of someone who is not enrolled in the system (an impostor). An automated system accepts all live scans with a match score above a match score threshold and rejects all live scans with a match score below that threshold.

The genuine and impostor probability distributions overlap to some extent. This is one source of system errors; sometimes a genuine user is rejected (false reject rate or FRR) and sometimes an impostor is accepted (false accept rate or FAR). The match score threshold is selected and set by the system administrator to minimize the FRR and the FAR.

It is important to understand the relationship between these two errors. For any one system, if the match score threshold is set lower, the FRR goes down and the FAR goes up; if the match score threshold is set higher, the FAR goes down and the FRR goes up. One way to represent this relationship is to plot FRR vs. FAR on a receiver operating characteristic (ROC) curve as shown in Figure 3. System performance can be tuned by setting the match score threshold to achieve a specific FAR, which will yield a specific FRR. (Note that FRR affects usability and convenience, while FAR represents a security risk. Thus, the FAR level, not the FRR level, is generally used to set the match threshold.)

Figure 3—Receiver Operating Characteristic (ROC) Curves for Three Different Fingerprint Biometric Systems



Also shown in Figure 3 is how biometric performance can vary from system to system. High-performance biometric systems produce a more significant separation of the genuine and impostor probability distributions than low-performance systems and hence have lower error rates. System 3 is the highest performing system in Figure 3 because for any given FAR, it has the lowest FRR.

Additional system errors to consider include failure to acquire (FTA), where no fingerprint scan is returned from the scanner, and failure to enroll (FTE), where a person cannot successfully enroll in the system.

One measure of system performance that takes all system errors into account is the total acceptance rate (TAR), which is represented mathematically as 1 – ({FRR@FAR} + FTA + FTE). A TAR greater than 99 percent can be achieved with modern equipment and the application of the best practices covered in this paper.

To achieve an accurate view of system-level performance, all elements of that system must be tested together under representative conditions with a representative sample of the user population. A theoretical test in the lab will not predict the behavior of the deployed system. For this reason we highlight scenario testing as a key best practice.

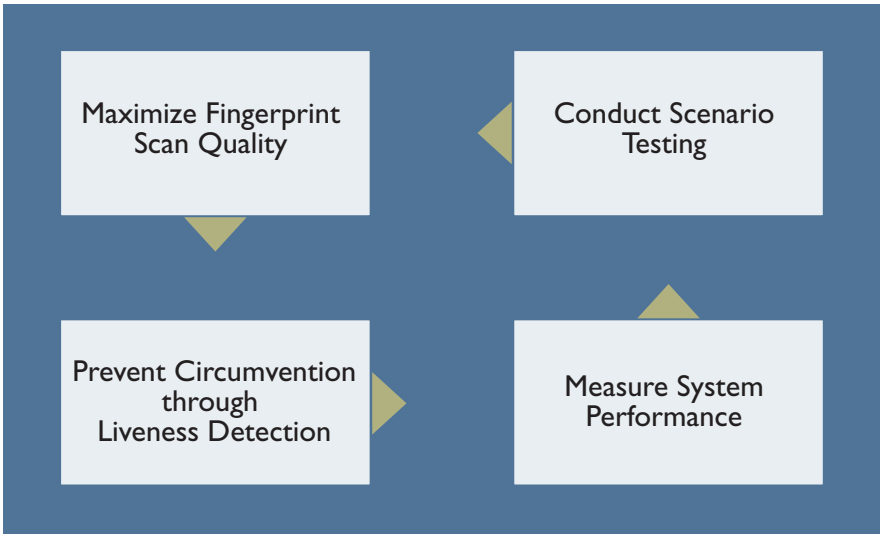
The best practices in this paper are intended to ensure that the performance characteristics of your system are high enough to meet your objectives and deliver the expected return on investment.

BEST PRACTICES AND RECOMMENDATIONS FOR IMPLEMENTING A FINGERPRINT BIOMETRICS SOLUTION

This section identifies a set of best practices associated with the design and deployment of a fingerprint biometric IAM system. They are intended to ensure that common mistakes are avoided and that the deployed system achieves the objectives of convenience, security, and compliance.

The successful implementation of a fingerprint biometrics solution involves a continuing process with four fundamental best practices, shown in Figure 4. Each will be discussed at length.

Figure 4—Fundamental Best Practices for Implementing a Fingerprint Biometrics Solution



Maximize Fingerprint Scan Quality

Fingerprint scan quality is by far the most important aspect of a fingerprint biometric system design. There is no other single controllable design element that is as important or so poorly understood. There are four interrelated aspects involved:

- **Scanner resolution**—Measurement systems have a resolution limit within which finer or smaller features may not be accurately resolved. Most scanners describe pixel resolution in dots per inch (dpi).
- **Scanner measurement area**—If the scanner measurement area is smaller than the full area of the fingerprint, the amount of biometric data available will be reduced. In addition, when the measurement area is smaller than a complete fingerprint, the placement of the finger effects which subset of features is scanned. While the live scan itself may be high quality, a mismatch is possible between the fingerprint enrolled and the live scan fingerprint.
- **Scanner measurement technology**—Most scanners use one of two measurement methods: semiconductor capacitive or optical total internal reflectance (TIR). Both measurement approaches are contact-based and rely on differentiating the areas in contact with the scanner (fingerprint ridges) from areas not in contact (valleys). Other scanners use direct imaging and are immune to contact-related effects. Also available are multispectral scanners, which collect subsurface fingerprint detail.
- **Human and environmental factors**—These are a very broad set of issues related to how the user and the user's skin interact with the measurement system under all expected conditions.

A high-quality fingerprint scan is a scan that, when passed through an automated biometric feature extractor, yields a large number of true biometric features. A high-quality fingerprint biometric system is one that reliably produces such scans each time the user interacts with the scanner.

Frost & Sullivan recommends the following fingerprint scan quality best practices to improve overall system performance:

- Use scanners with at least 500 dpi resolution. If children younger than 3 years old will use the system, consider a 1,000 dpi system.
- Use scanners that can scan the entire fingerprint area and do so with a wide range of placement freedom. In other words, if the placement must be perfect every time, the system will be overly sensitive to human factors.
- Use scanners that are not based solely on contact-related measurement technology to mitigate skin condition, contact pressure, and environment-related effects.
- Use scanners that can scan subsurface detail features reliably enough to mitigate the effects of poor user fingerprint expression.
- Ensure your system design allows for collecting and logging fingerprint quality metrics such as NIST NFIQ[2]. This is valuable for system testing, diagnosis, and continuous improvement.
- Enforce a minimum level of fingerprint quality for enrollments. If using the NIST NFIQ metric, enrollment scans should be a 1.
- At least three enrollment fingerprints should be scanned and matched against each other to ensure that the primary enrollment biometric template self-match score is significantly higher than the match score threshold used for verification.

Prevent Circumvention through Liveness Detection

A copy of an authorized person's fingerprint may be used to attempt to bypass a biometrics system. This is analogous to the theft of a password in a conventional identity management system. There are three categories of fingerprint copies and each has a related level of effort and expertise required to make the copy and use it.

---

[2] The National Institute of Standards (NIST) has developed a measurement method called the NIST fingerprint image quality (NFIQ) metric that can assess fingerprint scan quality in a way that is predictive of biometric feature extraction performance.

In contrast, standards such as the FBI/IQS standard for personnel identity verification (PIV) only measure scanner resolution and geometric accuracy independent of human factors, and as a result are not predictive of matching performance.

- **Activated latent print**—Each time a person touches a scanner, finger oils are left behind along with those of previous users. Normally this composite of users' fingerprints is not useful. However, a clean latent print can be left if the scanner surface is cleaned immediately before use. If the scanner can be triggered to scan this latent print, it is possible to gain fraudulent access.

- **Two-dimensional (2-D) copies**—A paper copy of a fingerprint can be created from a latent fingerprint lifted from an object such as a glass or a faucet handle. Additionally, in an identity management system that stores fingerprint scans, copies of these prints can be illegitimately accessed and used to print 2-D copies.

- **Three-dimensional (3-D) copies**—Like 2-D copies, 3-D copies can be created from latent prints. However, the fingerprint ridge and valley detail are additionally simulated to make a 3-D copy. Contact-based scanners in particular are susceptible to this form of copying.

Any copy method is imperfect and requires many attempts or, in the case of latent activation, has a recognizable pattern. Many identity management systems use event recording and sophisticated pattern detection algorithms to detect atypical or specific fraudulent events. In addition, a two-factor identity management system is protected against system breach in the event one factor is compromised.

Liveness detection or copy protection provides the assurance that a copy of an authorized person's fingerprint cannot be used in the system. Liveness detection can help prevent many of the copy attempts described. Here are some best practices for liveness detection:

- Use scanners with, at minimum, built-in latent and 2-D copy protection.

- Protect electronic copies of fingerprints or simply do not save copies of live or enrollment scans.

- If the potential for fraud is high, use scanners with built-in 3-D copy protection.

- Use a two-factor approach, such as a combination of fingerprint and user ID or fingerprint/credential.

- In addition to built-in protections, consider the use of system-level pattern detection and copy prevention technologies similar to those in use today for password fraud prevention.

Measure System Performance

In a fingerprint biometric system, it is important to continuously measure and understand system performance and adjust this performance to meet overall system requirements. To facilitate this, the ability to measure system performance attributes should be part of the overall system design.

It is also critical that enrollment of users is implemented in a way that ensures the highest-quality biometric templates are collected and used in the system. Enforcing strict guidelines at user enrollment will ensure greater accuracy and a better user experience throughout the lifecycle of the system.

Frost & Sullivan recommends the following best practices to ensure accurate user enrollment:

- Set the enrollment match threshold to be at least 20 percent higher than the live scan threshold to ensure enrollment provides a solid baseline.
- Enforce enrollment scan quality.
- Provide a means of alternate authorization for users that cannot enroll in the system for any reason.
- In a system that uses multiple authentication modes of operation, monitor how often each type is used.
- Use a two-factor approach if security is an important consideration and the number of users is greater than 3,000. Alternatively, consider a multiple finger scanner.

Similar to a conventional identity management system, change control and change management is core to both compliance as well as performance. Any time a component of the system is changed—from the scanners to the biometric feature extractors and matchers, or even as the overall enrollment database evolves—analysis of performance monitoring information should be reviewed to qualify changes.

Frost & Sullivan recommends the following best practices for performance monitoring and tuning:

- Implement a monitoring system that can capture performance information from the system continuously.
- Implement a change management process for all elements of the identity management system and require that each change is proven with scenario testing (see next section) or by monitoring results.
- Measure the single-touch failure rate—the total number of times the single touch of an enrolled user fails to produce a match score greater than the match threshold. This rate includes situations where the scanner does not return a scan (FTA), times out, or rejects an enrolled user (FRR).
- Measure the failure to enroll rate (FTE)—the number of users that cannot use the system reliably and therefore must use an alternate form of authentication.

- Provide for the ability to cross-validate all live scan templates against all enrollments to generate a ROC curve.
- Determine an acceptable FAR level for the system and use the ROC curve to determine the match threshold. Periodically recalibrate the threshold setting based on new enrollments collected over time.
- Do not assume that system performance can be determined from vendor data sheets or testing of individual components; continuously measure overall system performance characteristics and periodically tune performance using the match threshold to achieve your FAR requirement.

Conduct Scenario Testing

It is not possible to predict system performance based on vendor promises, information aggregated from multiple vendor data sheets, or the performance of other systems with different requirements. This is true even for IAM systems that do not use biometrics. Thus, scenario testing should be viewed as requisite and part of the implementation costs of the system.

The best practices outlined in previous sections of this paper are intended to ensure that there will be few surprises discovered during this phase of system deployment. Without careful consideration of those best practices, it is possible that scenario testing will uncover issues with vendor selection or system design that will make it impossible to achieve your performance and return on investment goals without modifications.

Scenario testing is a live test of the entire system with a representative set of users conducted under conditions that represent the system deployment environment. This testing is used to characterize the performance of the overall system and perform final vendor selection using comparative results. It is also the point in time where initial performance tuning can be accomplished.

A sample set of users is enrolled in the system using the enrollment rules that have been selected and verified in the system under representative conditions. This is the first time all the components of the system are used together and system-level performance can be determined.

The ISO and ILO references (see sidebar) offer substantial information on best practices and methods for scenario testing.

Frost & Sullivan recommends the following best practices for scenario testing:

- Review the ISO standard 19795-2:2007 section on scenario testing and develop test plans consistent with the best practices in this standard.
- Consider using contracted biometric system design and/or testing services available from a variety of sources, including the International Biometrics Group (IBG).

The ISO standard 19795-2:2007 and the International Labor Organization's (ILO) Seafarers' Identity Documents Convention 185 are good examples of biometric identity management system scenario testing methods.

CONCLUSIONS

Biometrics is a unique identity management approach that offers the combination of user convenience, cost-effective provisioning and a non-repudiated compliance audit trail for the system operator. These advantages incorporated into a conventional IAM system magnify IAM benefits and ROI—but only if the biometric elements are designed and implemented from an informed perspective.

The best practices outlined in this paper provide the means for senior executives with no knowledge of biometrics to understand the key considerations and ask the appropriate questions of those vendors and contractors who are designing and implementing the system. It is imperative that an organization considering the deployment of fingerprint biometrics at least consider the following three critical factors mentioned throughout this paper:

- Fingerprint scan quality and careful scanner selection
- Performance monitoring and scenario testing
- Performance and accuracy requirements for your application

Frost & Sullivan believes that by starting from a position of knowledge and setting an expectation of adherence to best practices, the result will most likely satisfy the organization's requirements or expectations of ROI.

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041