



Strategic Deployment of Biometrics for Access Control

By **Neil Rowlands**, Sales Director, Enterprise Access Division (formerly Bioscrypt), L1 Identity Solutions

The Indian security distribution market has undergone a dramatic change in recent years with the entry of MNC distribution houses with their rich knowledge of security distribution and vendor relationships.

ADI is an organization that has spearheaded this initiative and brought many industry players, both existing and new entrants, into this value chain of service/product delivery.

One such company, L-1 Identity Solutions, talks about Biometrics and some of their specific products.

Enquiries/product details:

Ashutosh Srivastava, Product Marketing Manager, ADI Global Distribution.
Ashutosh.srivastava2@adi-intl.com

Executive Summary

Throughout large enterprise and global governments — federal buildings, agencies, and military installations — the adoption of new sophisticated biometric devices is well underway. While they are just now beginning the deployment of readers at building access points, entrance gates, and other areas that need additional security, they also must contend with compatibility to the vast legacy of previous authentication and biometric initiatives. That means new readers must also be able to understand how to identify and read the hodgepodge of legacy human interface devices, RFID proximity cards, old magnetic strip readers, and the newest generation of smart credentials.

Just as important as choosing a backwards compatible and flexible biometric device is choosing a biometrics system that is also designed precisely for variable threat environments. A system that must be capable of adjusting swiftly to higher security thresholds during peak-threat periods, while also lowering security demands to maximize

user-throughput and convenience during periods when threat levels are low.

The goal of this paper is to help you weave through these complexities and bring a new heightened level of clarity about how to leverage biometrics strategically for maximum value. In fact, there are many biometric options available to help you configure a base access control system that is best suited for a flexible threat environment, and that integrates smoothly with building access control systems, so that both usability and security are maximized continuously.

Typically, there are three accepted ways to authenticate or prove identity to a system or an authorized person: something you have, like an ID card; something you know, such as a PIN number; and something you are — a biometric, such as facial features, fingerprints, or iris scans. When two or more of these are used together for an identification decision, it is called multi-factor authentication. The PIV program is using, at a minimum, a dual factor: card plus biometric, which offers a very secure solution that exceeds using cards alone.

The need: flexible biometric and authentication levels best designed for the task

While many mainstream authentication methods utilize fingerprints as the biometric, there are many authentication modes (such as 3D face recognition) that can be implemented, and limited only by the capabilities of the reading stations. This makes it possible for facilities to implement site-specific security levels that provide ways to enhance throughput for desired access points, vet visitors against watch lists, and add additional layers of protection for high-value assets.

On military bases, embassies, and other strategic installations where threat and risk levels rise and fall based on war-footing and geopolitical tensions, it is crucial to have in place a holistic access system that is able to respond accordingly. These authentication modes should be able to change dynamically, as needed. For instance, during times of low threat level, a base could use single-factor Card

Choose the Best Biometric for the Objective

Installations need to select biometric methods ideally suited for each application.

Perimeter Gates (Foot Traffic and Vehicles)

- **Requirement:** Handheld readers capture biometrics, or verify identity of foot traffic and next to stopped vehicles
- **Solution:** Integrated face recognition-enabled surveillance cameras catalog all site visits and search watch lists for known targets

Outdoor Building Access

- **Requirement:** Select weather-hardened readers capable of withstanding harsh elements
- **Solution:** Fingerprint readers with three-factor authentication capabilities

Interior Lobby Access (Turnstile)

- **Requirement:** Biometric well suited for high throughput
- **Solution:** 3D face recognition reader is hands-free

Office Access

- **Requirement:** Allows quick access during lower threat levels and is tightened during elevated threat levels
- **Solution:** Multi-factor fingerprint readers

Secure Locations

- **Requirement:** Biometric access that is greater than single- or two-factor authentication at the entrance to general premises
- **Solution:** Three-factor fingerprint reader with integrated card reader and PIN pad; or having 3D face recognition as an additional layer of authentication.

Only for verification, while an intermediate threat level would call for two-factor authentication of card authentication plus PIN. And high threat levels will grant access only to those capable of presenting three-factor authentication – a card, plus PIN, plus their biometric.

The goal is to choose the best biometric, or combination of authenticators, for each access point based on the best technology for the application. Only this approach will produce a system that meets security needs and the specific traffic flow of the facility.

Real-world biometrics deployment

Consider the approach for a fixed military base that needs to update its access systems to enhance security throughout the installation. Security officers need a way to identify anyone approaching the site on foot, as well as manage contractors, suppliers, visitors, and several thousand stationed military personnel for both physical access to, and within, the base.

An integrated biometric access control system is required that is

capable of reading legacy and new access cards with fingerprint biometrics. This card provides access through most outside gates and internal checkpoints, where required. In addition, 3D face identification installed at these locations enhances security whenever needed, and as a secondary form of authentication in the case of personnel who have been injured recently and may be unable to remove gloves, or other conditions that may make getting a clean fingerprint scan problematic.

As a result, the base not only meets its objective and is much more secure, and is always highly aware of who is on base at any moment. Just as important, the base can increase security quickly by adding new levels of authentication, such as requiring PIN or a primary or secondary biometric, to pass through access points during times of rising threat. This entry control system database will grow over time, as it collects and catalogues information about contractors, suppliers, and other visitors. And as users pass through entry points, the system logs and tracks their activity.

Layering biometrics: the strategic approach

Many components need to be considered in order to build a flexible biometrics and access control management system. One of the most crucial decisions is selecting a card reader that understands modern card technology, as well as legacy cards. These access systems should also be able to provide contactless single-factor Card-Only two-factor authentication, such as card authentication plus pin; and then three-factor authentication: card, PIN, plus biometric. The systems also needs the flexibility to register and manage visitors and others to the system quickly, either by issuing temporary credentials valid for several hours or for several weeks and months without expiring.

To avoid time consuming, and costly, physical upgrades in the future, it is absolutely essential that readers and biometric stations be extensible and dynamic. For instance, it is very likely that credential standards will be enhanced and updated in the future. Readers need to be able to adapt to these updates, as well as understand other forms of credentials likely to be presented to them. Also, while the threat level at most installations is low at most times, it is important to be able to balance high-traffic throughput (low-threat periods) at access points with single-factor, or card only, authentication. But when threat levels rise, security teams need to be able to adjust the system quickly to require additional forms of authentication, such as PIN and fingerprint. This includes managing authentication not only at the gate, but also at high-value areas throughout the base that may require card plus iris, or facial recognition for enhanced security.

Obviously, this system needs to

Biometric Technologies in Depth

Though fingerprint scanning technology is deployed widely and is highly accurate, it is not always the most efficient way to verify identities. For instance, in locations where employers prefer hands-free authentication, such as in harsh conditions where workers wearing gloves are common, or personnel are at risk of hand injury, or in dirty and moist conditions, facial recognition may be a more appropriate solution.

Fingerprint recognition

Fingerprint recognition is the most common form of biometric identification and also the most mature biometric technology. Wide-scale deployment also has reduced costs, making it the lowest cost biometric solution currently on the market.

It is used widely for physical access control, logical access control, time and attendance, and civil identification, and is also being adopted for consumer identification. Fingerprint readers have been deployed widely by the government, financial services and health care sectors — industries that need to increase security and meet compliance regulations.

New sensors are making it possible to place fingerprint readers in extremely harsh environments.

Face recognition

Face recognition follows fingerprint technology as the second most widely deployed technology. 3D face recognition is being used for physical access control and time and attendance applications for verification, while 2D face recognition is being used by the law enforcement sector for identification.

The civil ID market has begun adopting face recognition technology. Face recognition is also used in situations where workers' hands are dirty or greasy or where they wear gloves.

communicate and integrate tightly with the installation's building access control system, which provides the front-end interface for installation personnel who control many aspects of physical security. This capability requires strong integration with the biometrics and user privileges database as well as being able to correlate that information across readers throughout the installation.

Protecting and securing personal identities and assets, L-1 identity solutions

L-1 Identity Solutions helps government meet new PIV-card standards and put into place the most flexible biometric authentication capabilities possible. A key component is the L-1 Bioscrypt V-Series fingerprint readers.

Designed from the ground up to meet stringent security requirements, the V-Series Fingerprint readers increases security at any installation. Additionally, so that those installations that must maintain compatibility with previous generation infrastructure, as well as visitors who carry identification cards based

on legacy standards, the PIV-Station supports all standard card reader protocols, such as DESFire and MiFare. In fact, the PIV-Station has received GSA approval as a FIPS 201 compliant contact and contactless CHUID Reader — the first fixed Physical Access Control reader to be certified in both categories.

Areas where security needs to be tightened can achieve this goal through additional levels of biometric authentication, such as with the addition of 3D face recognition for access control. Also, during high-threat periods, the use of a PIN on the PIV-Station's integrated PIN pad can be required to gain access through all entry-points, while also increasing the number of entry-points that would require an additional biometric to gain access.

The enterprise access division of L-1 Identity Solutions can provide the technical capabilities to deliver effective, flexible biometrics and access control systems required for government agency and military installations. The division helps organizations navigate effectively through the complexities of

biometrics and PIV-based access control to legacy systems not yet updated for PIV requirements. And L-1 provides the most comprehensive, flexible array of biometric stations needed to strategically deploy an access control system that will defend a base or installation with the right level of security aligned with threat levels.

About L-1 Enterprise Access Solutions

www.L1ID.com

The L-1 Enterprise Access Division helps enable businesses to secure their premises with the most advanced and robust off-the-shelf biometric readers. L-1 Fingerprint Reader Solutions



use advanced pattern- and minutiae-based biometric algorithms for fast and secure verification. L-1 3D Face Reader Solutions use three-dimensional face geometry-based algorithms for authentication in under a second.

Together with the L-1 Identity Solutions portfolio of companies, they offer a comprehensive set of products and solutions for protecting and securing personal identities and assets. ■

