



The Biometric Advantage

Biometric access control solutions combine security with convenience

A Bioscrypt White Paper
November 2007

The Biometric Advantage

Table of Contents

Misplaced Hopes	2
Biometric Solutions	3
Putting a Finger on Security	5
AFIS & Non-AFIS Systems.....	5
Access Control.....	5
Time & Attendance.....	6
Facing Facts.....	7
The Biometric Advantage.....	8
The Business Advantage	8
Compliance	8
Risk Mitigation.....	8
Less administration	8
Accurate payrolls.....	8
The Bioscrypt Advantage.....	9

The Biometric Advantage

Misplaced Hopes

Verifying people are who they say they are is no easy task. Many of the solutions to date — passwords, ID cards and tokens to name a few — have been far from adequate. They fail to properly secure information in a manner appropriate to the highly sensitive nature of data that a corporation may need to collect. Passwords are all too often forgotten or written down and can be stolen using keystroke loggers. ID cards can also be easily stolen, lost or forged and tokens, too, can go missing.

Biometrics is a much safer solution — a biometric can't be stolen, misplaced, forgotten or copied. Biometric solutions use what a person is rather than what they know or carry for identification purposes, making it more secure and convenient than other authentication methods that have come before.

This white paper explores the advantages of using biometric technology — especially the two most common form of biometrics: fingerprint and face recognition.

The Biometric Advantage

Biometric Solutions

There are many types of biometric technologies, such as face, iris, hand geometry, vein, or voice recognition, and the most common, fingerprint. Biometric solutions can be used either independently for single-factor authentication or in combination with other authentication standards for multi-factor authentication. They are being leveraged by many industries, such as financial services, healthcare and government, to verify that the person attempting to gain access to an organization's buildings or computers and software applications is the appropriate employee. Organizations in heavily regulated industries that take a leadership position in demonstrating they have the necessary measures to protect confidential information have been early adopters of biometric technologies.

Other organizations are also beginning to see the benefits of biometric identity and access management and there are a variety of biometric solutions available, each with their own set of advantages.

- **Fingerprint recognition.** Fingerprint recognition is the most common form of biometric identification and also the most mature biometric technology. Wide-scale deployment has also lowered costs, making it the lowest cost biometric solution currently on the market. It is widely used 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 widely deployed 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.
- **Iris recognition.** Iris recognition is being used for access, border and immigration control and is also being considered for e-passports and authentication onto mobile devices.
- **Hand geometry recognition.** Hand geometry verification is being used in locations where there is a very harsh environment. Currently, hand geometry applications can only do 1:1 identification though limited 1:N capability is currently being developed. Because hand geometry doesn't enjoy the same breadth of deployment that fingerprint recognition does, it remains a more expensive and less accurate technology.
- **Vein recognition.** Vein recognition is still an emerging technology. It has low data storage requirements and may be used in areas where there is a high volume of traffic.
- **Voice recognition.** Call centers and financial organizations are interested in voice recognition as a way to identify customers for remote access either over a phone or online.

The Biometric Advantage

Fingerprint and face recognition readers are currently the most popular types of biometric technology on the market with 38.1% and 19.3% of the non-AFIS biometric market revenue respectively, according to the International Biometric Group's *Biometrics Market and Industry Report 2007-2012*.



Bioscrypt's V-Station fingerprint reader and VisionAccess 3D face readers are among the industry's leading biometric readers for access control.

The Biometric Advantage

Putting a Finger on Security

Fingerprints are the most common biometric technology and therefore the most mature. The large-scale deployment of readers has also driven down costs, making it the most affordable biometric solution currently on the market.

AFIS & Non-AFIS Systems

There are two major types of fingerprint technologies: Automated Fingerprint Identification Systems (AFIS) and Non-AFIS.

AFIS solutions are used primarily by law enforcement officials in order to identify a fingerprint by checking it against a large database of fingerprints, known as one to many or 1:N identification. Non-AFIS systems, on the other hand are used for physical and logical access control. Here, fingerprints are used not to identify people but to verify that they are who they say they are. Fingerprints presented at a door are checked either against a small database of other employees in a small-scale 1:N search or against a previously-enrolled template stored on a smart card or accessed through a PIN code for 1:1 verification. Non-AFIS systems are used by the private and government sectors to authenticate employees.

The two systems — identification and verification — use different solution architectures and can complement each other. In large scale projects, such as the U.S.'s government's Homeland Security Presidential Directive 12 (HSPD-12) initiative, an identification system can be used to do background checks on employees and contractors and then to enroll them. A verification system can then be deployed to do the day-to-day authentication at the door. This gives organizations the ability to create best-of-breed environments and allows them to use the sensor, reader and matching algorithm most appropriate for a particular application.

Access Control

Often used in conjunction with smart cards or PIN protocols, non-AFIS fingerprint authentication technology is one of the best ways to keep intruders or unauthorized personnel out of building premises or areas within an organization that only a few select employees should have access to.

Physical access through biometrics can also be tied into logical access into computer systems and applications. By tying the two together, companies can create an extra layer of security. They can, for example, deny access to someone who is supposedly logging onto his or her computer but who has not yet entered the building.

After 9/11, the U.S. government looked to biometrics to further secure federal buildings and this has become one of the driving forces behind biometrics adoption. The U.S.'s HSPD-12 mandates the use of strong authentication technology for government employees and contractors. As a result of HSPD-12, the National Institute of Standards and Technology (NIST) created the Federal Information Processing Standard 201 (FIPS 201), which states that federal employees and

The Biometric Advantage

contractors must use multi-factor authentication to access buildings and computer applications. Many industry observers believe that the FIPS 201 model will likely also be employed by the private sector.

Bioscrypt Inc. is a uniquely placed vendor that offers both physical and logical access.

Bioscrypt has two types of fingerprint authentication readers for physical access — the PIV-Station and Veri-Series readers. The FIPS-certified PIV-Station fingerprint reader can be used in conjunction with both contact and contactless smart cards and PIN protocols to create multi-factor authentication. Bioscrypt's PIV-Station uses FIPS-standardized minutiae fingerprint matching, which detects and maps the placement of minutiae points such as ridge endings and bifurcations, to make a match.

Bioscrypt also offers fingerprint pattern matching solutions through its Veri-Series fingerprint readers. Bioscrypt's patented algorithm is based on fingerprint ridge pattern recognition, a novel technique pioneered by Bioscrypt specifically for commercial applications. The pattern-based approach can work with lower quality images from sources such as worn or scratched fingerprints, while maintaining a high level of accuracy.

Bioscrypt also offers VeriSoft, a logical access solution which supports fingerprint authentication and can verify a user's identity before giving them access to computers and applications. Companies can draw on the data logs of the identity and access manager for auditing purposes and to ensure they are meeting compliance regulations.

While fingerprint authentication is a widely accepted and deployed technology, fingerprint matching isn't the only biometric solution Bioscrypt offers. Bioscrypt recently expanded its biometric product set by adding 3D facial recognition through the acquisition of A4Vision. The merger solidifies Bioscrypt's place as the leading vendor of biometric access control technology.

Time & Attendance

Face and fingerprint biometric readers are also used for time and attendance purposes. Biometric readers can increase the accuracy of payrolls, eliminate cumbersome paperwork and lead to increased productivity. Workers no longer have to fill out time sheets and the payroll department doesn't have to worry about inaccuracies creeping into the system during data entry. Biometric time and attendance solutions also eliminate buddy punching since one employee can no longer punch in for another.

The Biometric Advantage

Facing Facts

Though fingerprint scanning technology is highly accurate and widely deployed, it's not always the right identity verification solution. In locations where employers prefer hands-free authentication, or in labs where workers wear gloves, facial recognition may be a more appropriate solution.

Bioscrypt's structured light 3D facial recognition system for identity and access management — featuring the VisionAccess 3D Face Reader — is uniquely placed within the industry. Other facial vendors offer either 2D facial recognition, which is not designed for access control or stereo 3D, which adds unnecessary complexity to the enrolment and verification process.

2D facial technology is also not geared towards access control. It requires lighting conditions to be just right and its accuracy can be affected by factors such as shadows. In UK trials for biometric passports, for example, only 69% of able-bodied volunteers and 48% of disabled participants were correctly authenticated.

With 3D facial recognition technology, it's possible to collect many more data points than with 2D technology — up to 40,000 with Bioscrypt's 3D technology. Many of the data points collected by 3D — such as the curvature of the forehead — are more valuable than the data points used for comparison in 2D. Scars, facial swelling as a result of an accident or weight loss and gain (unless it's extreme) won't affect the accuracy of 3D identification.

There are two approaches to 3D facial recognition for access control: stereo and structured light.

With stereo technology, at least two cameras are needed to take multiple photos of someone in order to synthesize the 2D photos into a 3D image, making the applications more compute intensive than in the structured light approach. With the structured light approach, a structured grid pattern is projected onto the subject while a camera takes a picture of the modification of the pattern caused by the person's face. The image is converted into a template. Because the structured light approach uses its own light source, it is not hampered by poor lighting conditions, can accommodate different facial positions and can authenticate someone in under a second.

3D face recognition technology is ideal for situations in which employees have their hands full when leaving or entering premises or in locations where there is a high volume of traffic — such as at public transportation turnstiles.

Bioscrypt's structured light 3D facial scanning solution is simple and elegant, increasing accuracy over 2D facial recognition technology and decreasing cost and complexity in comparison to stereo 3D approaches.

The Biometric Advantage

The Biometric Advantage

As the amount of information organizations collect about their customers grows and privacy and compliance laws compel them to ensure the information is secure, companies are looking for new methods to safeguard their buildings and data systems. Passwords, ID cards and tokens have proven to be unreliable since they're prone to loss and theft. Biometrics allows enterprises to be sure of who is entering their premises and networks in a way that could not be achieved before.

The Business Advantage

Compliance. Regulations such as Sarbanes-Oxley (SOX) in the commercial sector, the Federal Financial Institutions Examination Council (FFIEC) for banks and other financial institutions, the Gramm-Leach-Bliley Act (GLBA) in the financial sector and the Health Insurance Portability and Accountability Act (HIPAA) in the healthcare sector require organizations to carefully control and monitor access to confidential and private information. Biometric solutions require employees to authenticate themselves with a factor only they have access to, such as their face or fingerprint. The systems also create audit trails that can be used for reporting purposes.

Risk Mitigation. Biometric solutions significantly reduce the risk and costs associated with data breaches. A 2005 study by the Ponemon Institute of 31 data loss cases found the cost of a breach to be extremely high — averaging \$4.7 million per incident at an average loss of 26,000 records, each costing \$182. Just over half of that cost — \$2.5 million — represents lost business. In contrast to this high cost, Ponemon found that organizations only spent an average of \$180,000 to prevent future data losses.

Less administration. One of the most cumbersome aspects of administering a card-based access control system is keeping track of cards and dealing with lost cards. Cards must be retrieved from departing employees, reported and then cancelled if lost, and temporarily replaced and then returned if forgotten. Such hassles are either eliminated or greatly reduced with the introduction of a biometric factor of authentication, since employees can neither forget nor lose their finger or face. Even in dual-factor authentication systems that incorporate smart or prox cards, concerns about lost cards are significantly mitigated as a found card cannot be used without the second factor of authentication — a biometric.

Accurate payrolls. Biometric readers can eliminate buddy punching and time-consuming paperwork when tied into time and attendance solutions. This creates more accurate payrolls and leads to higher productivity. Large organizations with a substantial number of part-time workers have been able to significantly reduce payroll expenses with the introduction of a biometric time and attendance solution.

The Biometric Advantage

The Bioscrypt Advantage

Bioscrypt's innovative identity and access management solutions have made it the market leader for biometric physical access control readers, according to IMS Research and the leader in physical access control and time and attendance according to Frost & Sullivan. Bioscrypt has also garnered a number of awards for its solutions, including the top spot in the 2002 and 2004 International Fingerprint Verification Competitions. VeriSoft access manager received the Best Buy award in *SC Magazine's* Biometrics Tools 2007 review and its V-Station fingerprint reader and VisionAccess 3D Face Reader also received five out of a possible five stars in all categories. Bioscrypt's solutions have been deployed in organizations where security is the utmost priority, such as government buildings, space agencies, airports, banks, biopharmaceutical companies and Fortune 500 corporations.

Bioscrypt offers both minutiae- and pattern-matching fingerprint readers. The PIV-Station minutiae-based reader is a FIPS 201-certified contact and contactless reader designed to help government organizations meet the HSPD-12 requirement. The Veri-Series pattern-based fingerprint readers are designed specifically for access control applications and can make accurate matches in under a second even with worn or scratched fingerprints. Like its fingerprint scanners, Bioscrypt's VisionAccess 3D Face Readers combine security with convenience and are a simple and elegant way to verify someone's identity in under a second. VeriSoft, which supports all major authentication factors, including fingerprints and face, enables systems administrators to set the access control policies for various applications depending on the level of security required.

The Biometric Advantage

About Bioscrypt Inc.

Bioscrypt is an enterprise access control solution provider, enabling the unification of physical and logical access with its Door to Desktop® products. Bioscrypt's hardware and software solutions deliver strong authentication processes to facilities, equipment, IT networks and computer applications and allow organizations to administer unified identities across the enterprise. Building on its proven expertise in biometric technology and its unique multi-factor authentication platform, Bioscrypt integrates all major secure authentication standards, transforming how organizations are bridging the gap between physical and logical access to create secure working environments. More information is available at www.bioscrypt.com.