

BIOMETRICS

in Time & Space



TIME  SPACE

Best Together

spica

Biometrics is becoming mainstream technology for identification, authentication, authorization and access control, by overcoming some important limitations of traditional methods involving keys and passwords. The limitations can be best summed up by three problems:

1) THE PROBLEM OF KEY

By »key« we mean all modern versions like RFID tag, smart ID card, USB key or similar physical token. No matter how sophisticated the key is, it will always have one inherent weakness: since it is a physical object, it can be lost or stolen. Keeping the key requires special care. The key can also be borrowed and it does not tell who is using it, so it cannot be trusted for identification.

2) THE PROBLEM OF PASSWORD

For centuries, the problem of key has been avoided by using passwords. Password nicely solves the issue of losing or stealing, but it brings in some problems of its own. Being just a piece of information, passwords can be forgotten or disclosed. They are no good unless kept as secret. And they can be compromised by all kinds of means like eavesdropping, deception, threat, extortion or even simple guessing.

3) THE PROBLEM OF KEY PASSWORD COMBINATION

By combining key and password, security can be certainly improved. ATM cards (pin secured credit cards) are the most popular example. However, as we can see from numerous cases of credit card fraud, even such combined security can be compromised. Unfortunately, it is more or less obvious that keys, passwords, and even their combinations cannot provide the ultimate level of security and convenience.

Being based on the recognition of features unique to an individual, biometric identification offers **entirely new level of reliability and efficiency**. The main advantages are two, both directly related to weaknesses of keys and passwords:

1) CONVINIENCE ADVANTAGE

Biometric identification eliminates the need to carry around keys (or cards) or memorize passwords.

2) SECURITY ADVANTAGE

Biometric identification eliminates the risk of unauthorized access using borrowed, forged or stolen keys (or cards) and compromised passwords.

By popular notion, biometrics is almost always associated with high security. For some reason, huge practical advantages from easier and more convenient use, are still being grossly overlooked. Advantages of using fingerprint readers in access control applications are pretty self-evident. Besides providing higher security, they can eliminate the need to carry cards and memorize passwords.

When used in time recording applications, fingerprint readers will not only be more convenient to use than cards, they will also effectively prevent »buddy punching«, a popular way of cheating conventional time clocks.

Biometric identification is still relatively new and fast advancing technology and it is still coping with some challenges. There is still plenty of new methods hitting the market often before they are mature for practical use. Sometimes, the problem is unrealistic expectation that biometric identification is 100% accurate. That of course, is never the case, there is always some, even so small margin of error.

In some cultures, some people can have problem with using some methods of biometric identification. For example, central parts of Europe are particularly sensitive to fingerprint technology, probably because of associating fingerprinting with totalitarian experiences from the past. As irrational as these fears may be, they must be respected and taken into account. EU is



advocating »cautious« and »controlled« use of biometrics. The legislation in EU varies greatly from country to country, ranging from quite liberal (say, UK) to heavy regulated (say, Slovenia).

Over-regulation of biometrics is certainly a challenge. For example in Slovenia, there is de facto ban on use of biometrics for working time clocking. This applies to any kind of biometrics (face, fingerprint, vein pattern...) and any usage model, including the template-on-card model, which is widely recognized as most protective of privacy. In Slovenia, approval for »biometrics measures« will be granted by local Information Commissioner Office only after proved absolutely critical for security or safety.

TIME&SPACE BY SPICA

Time & Space system has been supporting biometric technology for more than two decades. During that time, Spica has become the leading supplier of biometric solutions in the region, with the largest installed base. Our systems based on fingerprint identification are today used by more than 100,000 users.

Spica employs biometric readers from the world leading biometric technology and solution vendors. Spica is partnering with Morpho (www.morpho.com) offering integration for their fingerprint and 3D face recognition readers. Spica works also with other vendors for providing more specialized and government biometric solutions.



IDENTIFICATION VS. VERIFICATION

Biometric readers normally perform matching of a live biometric sample against a number of pre-stored samples (called »templates«) taken from all participating candidates. Such method is called pure identification or **one-to-many matching**.

By reducing the number of candidates to a single one, the speed and accuracy of identification can be significantly increased. In that case we are talking about verification or **one-to-one matching**.

One-to-one matching is obviously easier to implement and not all biometric readers are accurate enough for one-to-many identification. Especially for larger number of candidates. For situations with hundreds or even thousands of candidates, the choice of suitable readers can be greatly reduced.

Time & Space provides support for both identification (one-to-many) and verification (one-to-one). Yet due to variations between devices and manufacturers, there may be limitations.

FINGERPRINT

Fingerprint identification or verification is classic biometric technology and, thanks to its maturity and affordability of fingerprint readers, also the most commonly used.

Spica access control solutions employ external fingerprint readers, either stand-alone or connected via a network of access terminals. For time recording, Spica device portfolio maintains time clocks with built-in fingerprint reader.



FACE RECOGNITION



Face recognition comes in many shapes and forms. Yet until recently, face recognition was not strong enough to be used in access control or even time recording applications.

All that changed quite dramatically with the advent of 3D face recognition technologies. The breakthrough in face recognition has been achieved by going beyond visible light photography and 2D pattern matching techniques. 3D face recognition combines various advanced technologies like stereoscopic imaging, surface modelling, infrared and laser.

The result is successful elimination of most major obstacles hindering earlier 2D readers:

- much lower sensitivity to camera angle, no need for precise face positioning
- much less affected by the hair (haircut, beard), clothes (scarf, hat) or even glasses

- much less dependent on lighting conditions and may even be used in total darkness
- much harder to cheat, because of much higher accuracy and sophistication

Vision access by Morpho is noted for its fast and reliable operation proven in real life applications. It is most used in environments where reliable and unobtrusive access control is needed, for example banks, insurance companies, corporate buildings or airports. It is usually combined with automatic gates or turnstiles ensuring smooth flow of people and easy surveillance.

IRIS RECOGNITION



Due to its high accuracy and high price, iris recognition has traditionally been used in very high security environments, for example, access to vaults, archives with sensitive information, military facilities and the like.

With prices falling, iris recognition is now spreading into lower security areas and time & attendance.

Iris recognition continues to be one of the most accurate identification methods, so it is reasonable to expect that it will persist and gain more grounds in the areas where reliability has priority over cost or convenience.

TEMPLATE MANAGEMENT

Biometric identification is based on comparison of live sampling and pre-stored samples called biometric »templates«. Since these templates have to be collected before the system can be used, all biometric systems need some kind of template management.

For larger systems with multiple readers and numerous users, template management can be a considerable and often underestimated challenge.

There are two approaches to this challenge, with two quite different strategies for template keeping. One is based on centralized template management and database storage.

The other solution called »template-on-card« (TOC) goes in opposite direction and utilizes smart ID cards for keeping templates. Because templates are kept on-card by their owners and not circulated around, TOC method may be better choice where privacy is an issue.

Obviously, TOC will not work without cards, so for systems relying only on biometric readers, centralized management is the only viable choice.

Both TOC and centralized management strategy have their advantages and disadvantages and it is impossible to tell which one is better without taking many factors into consideration.

Luckily, Time&Space offers support for both centralized template management and template-on-card. The two methods can even be combined within the same system.