

Spica International d.o.o.

Pot k sejmiscu 33
1231 Ljubljana
Slovenia

Tel: +386 1 568 08 00
Fax: +386 1 568 08 88

www.spica.com

SPICA

TIME SPACE



Biometrics in Time&Space

BIOMETRICS IS RAPIDLY BECOMING THE KEY IDENTIFICATION TECHNOLOGY FOR IDENTIFICATION, AUTHENTICATION, AUTHORIZATION AND ACCESS CONTROL, BECAUSE IT OVERCOMES THE LIMITATIONS IMPOSED BY TRADITIONAL METHODS INVOLVING KEYS AND PASSWORDS.

The problem of key

By »key« we understand also modern versions like RFID tag, smartcard, USB key, or similar physical token. No matter how complex, and thus secure, the key is, it will always have one inherent weakness: Since it is a small object, it can be lost or stolen. Keeping the key requires special care.

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 compromised so they need to be memorized and kept secret. They can be revealed by all kinds of means like eavesdropping, deception, threat, extortion or even simple guessing.

The problem of key with password

By combining key and password, security can be certainly improved. ATM cards (or PIN secured credit cards) are the most popular example. However, as we can see from numerous cases of credit card frauds, even such combined security can be compromised. Unfortunately, it is more or less obvious that

keys, passwords, and even their combinations cannot offer really high level of security.

Advantages of biometric identification

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:



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



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 of biometrics, like easier and more convenient use, are still being grossly overlooked.

Challenges facing Biometric identification

Biometric identification is relatively new technology still facing some challenges. There are still many new methods hitting the market, often before they are mature for practical use.

Sometimes, there is a problem of unrealistic expectation that biometric identification is 100% accurate. That of course, is never the case, there is always some small margin of error. In some cultures, some people can have problem using some methods of biometric identification. For example, some parts of Europe are particularly sensitive to fingerprint technology. Probably because of associating fingerprinting with totalitarian police control. As irrational as these fears may be, they must be respected and accounted for.

Biometric identification in Time&Space systems

Time&Space system has been supporting biometric technology for more than a decade. During that time, Spica has become the leading supplier of biometric identification systems in the region, with the largest installed base. Our systems based on fingerprint identification are today used by more than 50,000 users.

Spica's solutions predominantly utilize the technology from the world leading technology provider Bioscrypt (www.bioscrypt.com) by adopting their range of advanced fingerprint readers with embedded intelligence. As Bioscrypt's OEM, Spica also builds Bioscrypt readers into its own products.

In 2007, Spica has adopted Bioscrypt's new and promising biometric technology - 3D face recognition.

At about the same time, we broadened our range of products by including iris recognition devices. Iris recognition is a well established biometric identification technology in high security environments. With the recent reduction in prices, it is now becoming more affordable.

Spica is also engaged in scientific and research projects in the area of biometrics. Spica invests extensively in its own R&D and closely collaborate with educational and scientific institutions of the University of Ljubljana, among them are the Jozef Stefan Institute, the Faculty of Computer and Information Science and the Faculty of Electrical Engineering. Spica R&D team is registered with the Slovenian Research Agency and participates in the major national projects involving biometric technology.



Fingerprint identification

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

The advantages of using fingerprint readers in access control applications are pretty self-evident. Besides providing higher security, they 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«.

Spica access control applications include external fingerprint readers, either stand-alone or connected via a network of access terminals. In time recording applications, a fingerprint reader is often built into time-recording terminal.



Much like any other biometric device, fingerprint reader works with set of pre-recorded fingerprint samples or »templates«, that are matched against live fingerprints. Time&Space supports two methods of managing biometric templates. First one requires that the templates are stored centrally in the database, i.e. the device itself. With the other method, templates are stored on cards. Depending on the selected method of template storage, there are actually four ways of using a fingerprint reader:

| Usage method | Template storage | Identification | Verification | Number of users* |
|------------------|------------------|----------------|----------------|------------------|
| Finger only | Device** | Fingerprint | (not required) | up to 500 |
| Finger/PIN | Device** | PIN | Fingerprint | up to 4000 |
| Finger/card | Device** | Card | Fingerprint | up to 4000 |
| Template on card | On card*** | Card | Fingerprint | (unlimited) |

* The limitation applies to individual reader in the system. Since every reader can have different group of users, the overall number of users may be much higher.

** If there are several readers in the system, templates can be stored also in the database to allow centralized administration.

*** Smart cards such as HID iClass, Mifare or Legic are required.

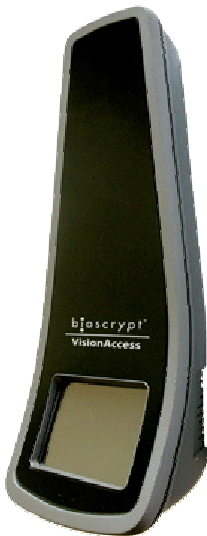
Face recognition

Face recognition is not an entirely new method. We have seen many attempts in this direction over the past years, and although several face recognition systems have been around for some time, their reliability was below the level required in an access control system. A giant leap forward has been made only recently with the appearance of 3D systems.



The breakthrough in face recognition has been achieved with 3D imaging and analysis of facial features by eliminating some major obstacles hindering earlier 2D systems:

- i** Much less sensitive to camera angles, no need for precise face positioning.
- i** Much less affected by the hair (haircut, beard), clothes (scarf, hat) or glasses.
- i** Much less dependent on lighting conditions and may even be used in total darkness.
- i** Much harder to cheat, because of much higher accuracy.



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

At Spica, we are confident that 3D face recognition will soon appeal to customers and become one of the most practical biometric methods.

Iris recognition

So far, iris recognition has found widest application in very high security environments, for example, access to vaults, archives with sensitive information, military facilities and the like. Although it is an extremely accurate identification method, it has not been widely accepted. One reason is that people generally are not comfortable with the idea of scanning eyes, especially with lasers. Another reason is the costs, since iris scanners can be many times more expensive than fingerprint readers.



However, the latest generation of scanners is not using laser beam any more. Furthermore, the prices are falling and soon iris scanning could be much more affordable.



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.