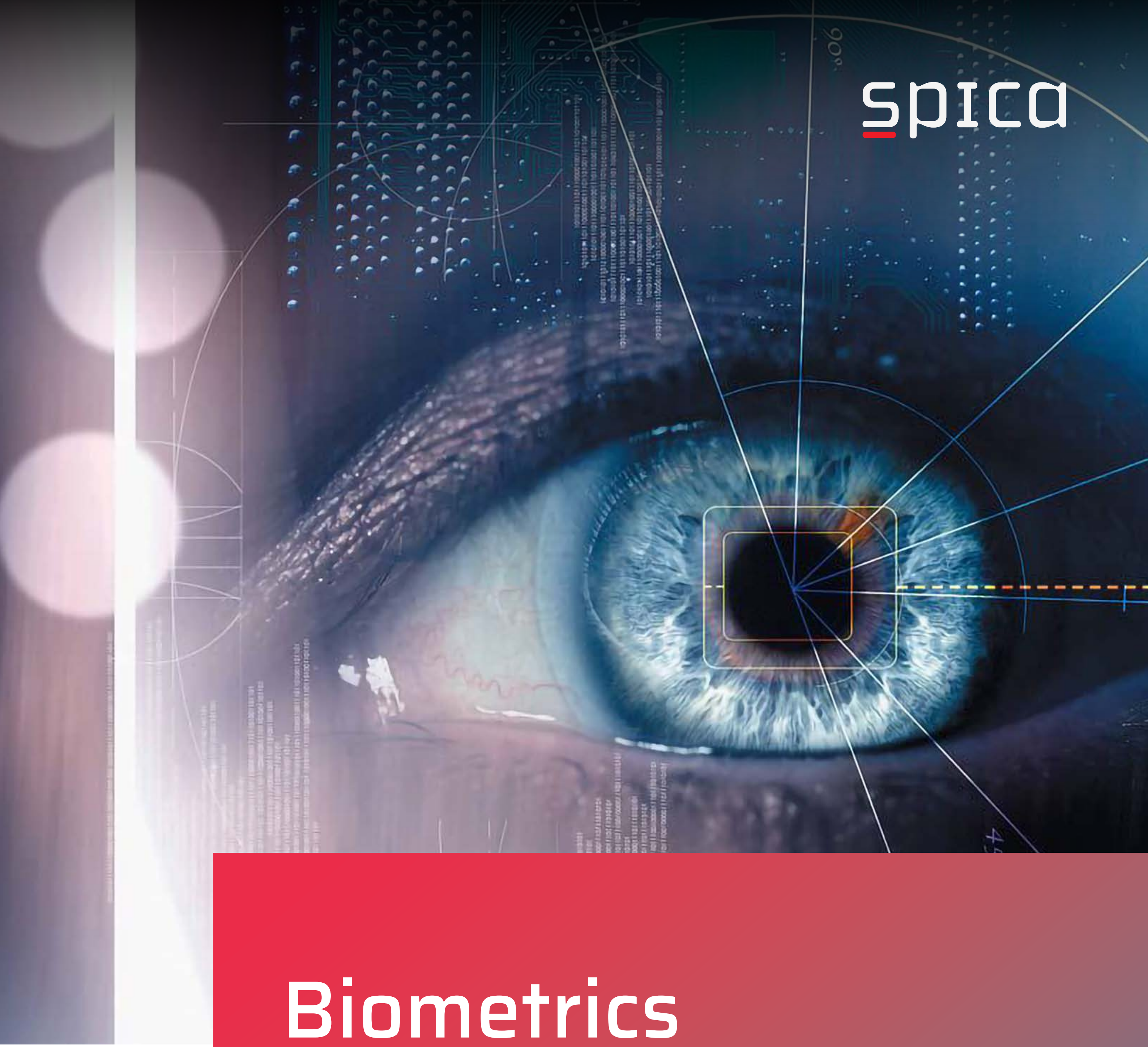
spica



Biometrics in Time&Space

TIME&SPACE

Best together

By overcoming some important limitations of traditional locking methods involving keys and passwords, biometrics has become mainstream technology for **identification**, **authentication**, **authorization** and **access control**, by. The limitations can be best summed up by three problems:

The problem of key

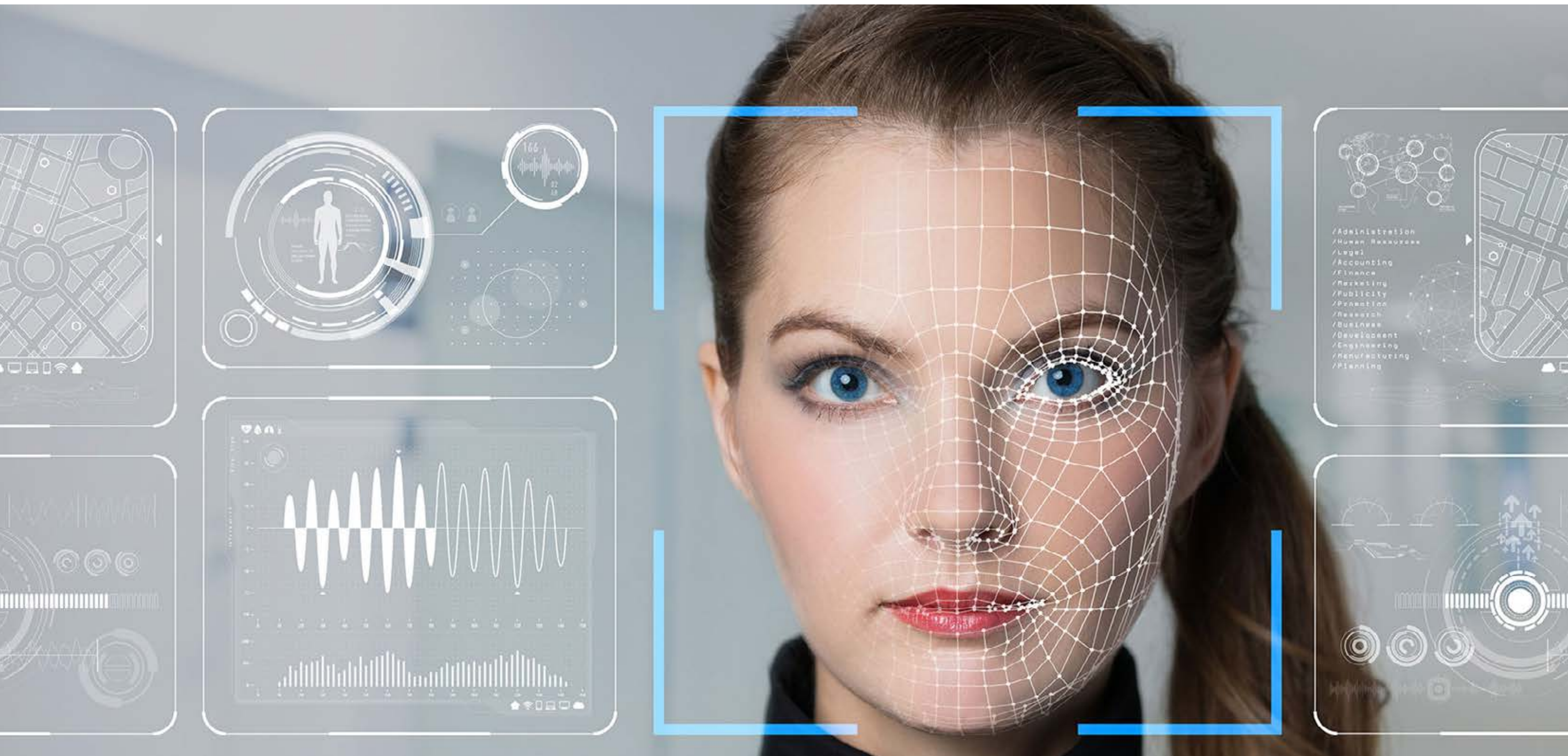
By »key« we mean all modern versions like RFID tag, smart ID card, USB key or a similar physical token. However, no matter how sophisticated the key is, it will always have one inherent weakness: since it is a physical object, it can be lost or stolen. Keeping the key requires special care. The key can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

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, password can be forgotten. It can be easily shared, yet it is no good unless kept as secret. It can be compromised by all kinds of tricks like eavesdropping, deception, threat, extortion or even by simple guessing.

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. While the key-password combination may improve security, it will also reduce convenience, since now we need to care about two things instead of one. And still, nothing has been improved regarding the identity. We still cannot know **who** the user is.



Advantages of biometrics

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 keys (or cards) or memorize passwords

Security advantage

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

These two advantages are huge and equally important.

Advantages of using fingerprint readers in **access control** applications are pretty self-evident. Besides providing higher security, they can eliminate the need to carry or memorize anything.

In **time recording** applications, fingerprint readers will not be just convenient to use, they will also effectively prevent »buddy punching«, a popular way of cheating conventional time clocks.

Challenges of biometrics

Biometric identification is still relatively new and fast advancing technology and it is still coping with some challenges. Probably the biggest one is the lack of stability, being the victim of constant and rapid development. Users are often confronted with their existing system soon becoming obsolete or incompatible. And, there is still plenty of new methods and technologies hitting the market even 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. The problem is also that experienced margins of error are often significantly worse than those advertised. The lack of understanding of basic accuracy principles such as FAR and FRR (Fales Acceptance and False Rejection Rate) does not help either. For example, upon purchase, the user may be fine with the FRR of 1% and FAR of 0,01%. For 3000 employees averaging 3.3 clockings per day, this would amount to 100 rejected clockings each day, some of them even when repeated. Much worse, they will need to tolerate one clocking recorded for a wrong employee per day. That would actually mean two serious, hard to manage errors each day: one wrong and one missing clocking.

Another challenge is that due to natural variation, some people would have less recognizable biometric characteristics than the other. Some will have very slight, hard to detect fingertip grooves, or very common face recognition features. Such employees would then require some alternative method of identification.

Regulation

Unfortunately, it does not end there. In some cultures, people may have problem with using certain methods of biometrics. For example, central parts of Europe are particularly sensitive to fingerprint technology, probably because of associating fingerprinting with totalitarian experiences from the past. They may feel devalued, criminalized and offended with very adverse effect on viability of the system. In some other parts of the world, fingerprinting is associated with criminal record with similar effect. All such concerns must be respected and taken into account. For example, 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).

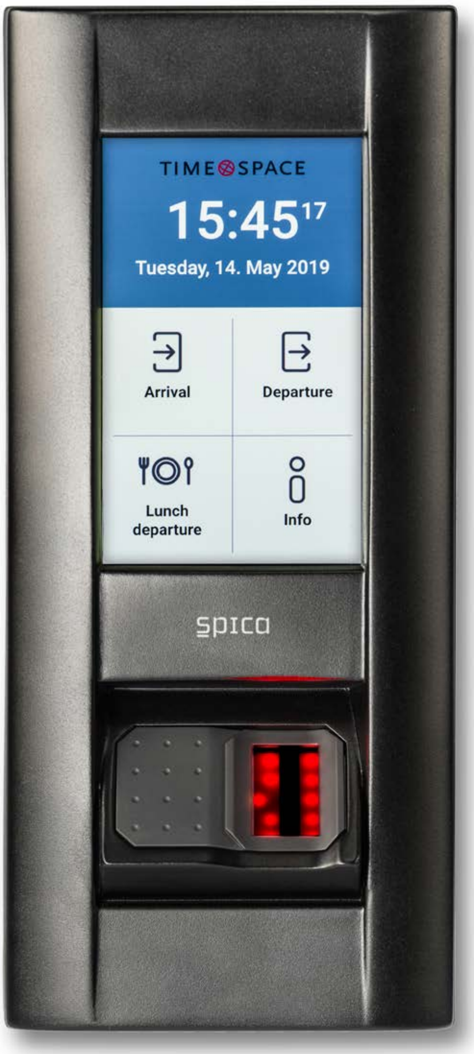
Over-regulation of biometrics is certainly a challenge. For example in Slovenia, there is de facto ban on use of biometrics for working time clocking. This applies to any kind of biometrics (face, fingerprint, vein pattern... any kind) and any method of use, including the template-on-card model, which is widely recognized as most protective of privacy. In Slovenia, approval for »biometrics measures« will be granted by local Information Commissioner Office only after being proven absolutely critical for security or safety, or being essential for the business. No wonder, not a single permit for employee time recording has been granted since the regulation has been enforced in 2006.

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. Spica's systems based on fingerprint identification are today used by more than 100,000 users.

Spica employs biometric technology from the world leading biometric technology and solution vendors. Spica is partnering with Morpho (www.morpho.com, now owned by Idemia) offering integration for their fingerprint readers and time clocks. Spica's own Zone Touch FB time clock features built-in fingerprint reader from Morpho.

Spica works also with other vendors for high-security and government biometric solutions.



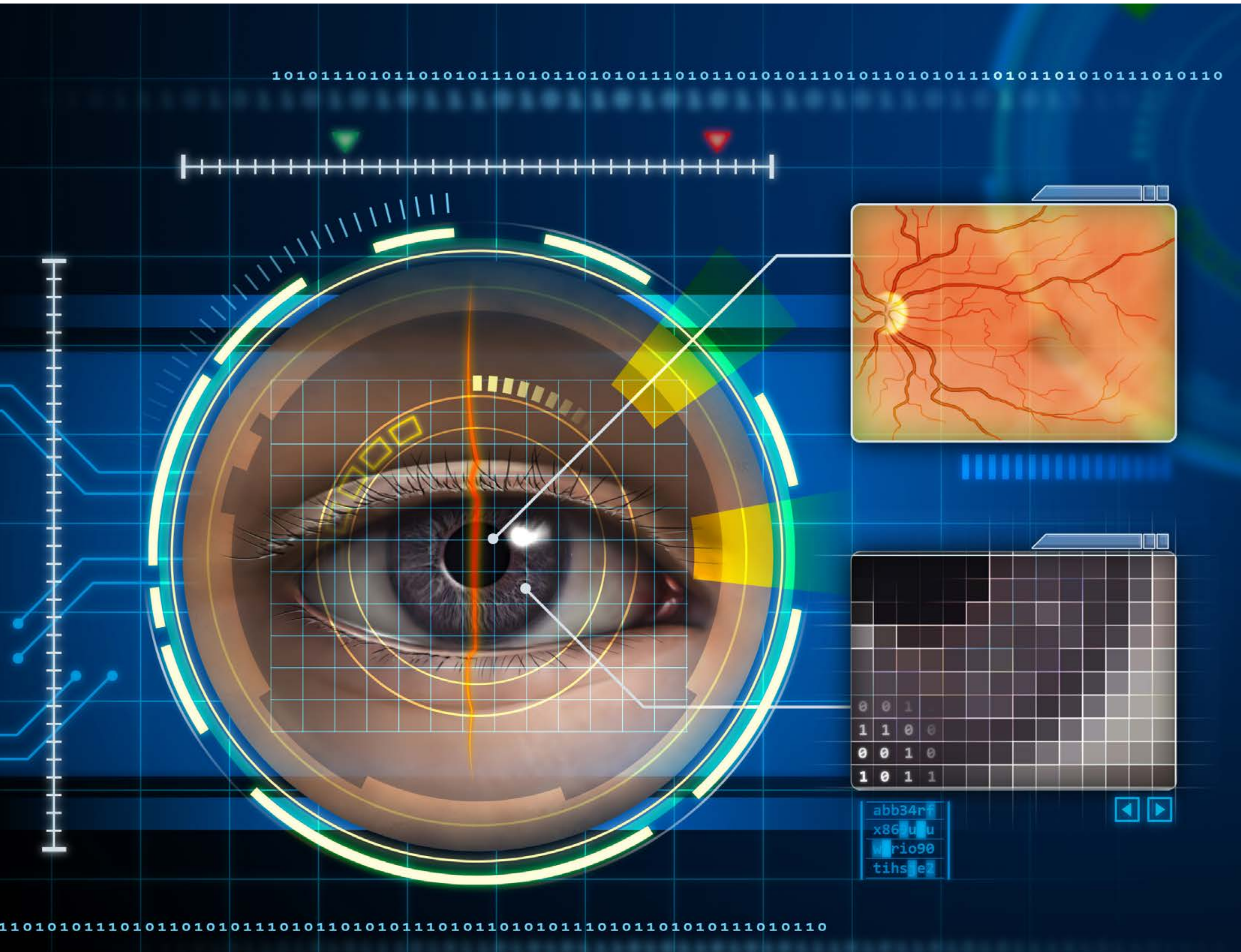
Identification vs. verification

Biometric readers normally preform 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. For situations with hundreds or even thousands of candidates, the choice of suitable readers performing pure identification 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 and other biometric methods

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

Spica works predominantly with fingerprint with support for two technology leaders, Morpho (www.idemia.com, USA) and TBS (www.tbsbiometrics.com, CH). Spica offers support for their line of readers and time clocks, and uses Morpho's fingerprint module for Spica's own Zone Touch FP time clock.

Occasionally upon request, Spica also implements readers from other biometric vendors such as Suprema, and other biometric methods, such as iris or face recognition.

Template management

Biometric identification is based on comparison of a live fingerprint to the pre-stored samples called biometric »templates«. Since these templates need to be collected before the system can be used, all biometric systems require 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.

Smartphones, smartphones!

With the recent advent of biometrically guarded smartphones, we are getting some new and exciting possibilities. With the right kind of a smartphone app, smartphone's own biometric technology can be utilized for the access control or time recording. Being entirely under control of the user, the usage scenario is very similar to fore-mentioned template-on-card.

Spica supports Mobile Access smartphone enabled card readers from HID. Their app can be guarded with phone's own biometrics. Spica also develops its own mobile apps which also can be guarded in the same way.

Being able to perform its own biometric verification is just one of the many advantages of smartphones vs. cards. Smartphones are now replacing cards with accelerating pace and we may be already witnessing their mass extinction.

Špica International d.o.o., Pot k sejmiscu 33, SI-1231 Ljubljana, Slovenia · www.spica.com · www.timeandspace.eu · T: +386 1 5 68 08 00 · info@spica.com