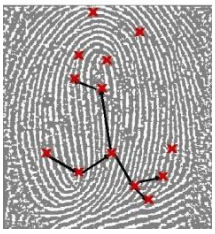
Statement Biometric Identification and Privacy

Difference between Afis and commercial systems.

When talking about privacy and biometrics one should look directly at what kind of system one is talking about. https://en.wikipedia.org/wiki/Automated_fingerprint_identification. Government systems (police, passport, etc.) are based on a system where images are stored (Afis systems). These systems can violate people's privacy if they fall into the wrong hands or are used incorrectly.

The commercial systems, such as DMS®, use an algorithm and cannot be traced back to a real printout. These systems are used in business for time, access, and attendance systems, for example. But also in healthcare, such as patient recognition, at schools for exam registration, subscriptions for tanning beds, access to server rooms, etc.



From body feature to template.

DMS® scans a fingerprint, this image is already transformed into a template in the scanner. This template is the result of an algorithm and consists of a number of 364 positions. Besides being patented, the algorithm is also protected by encryption (aes256, the highest form of encryption).

Even if the code were cracked, you would still have to crack the algorithm. And even if the algorithm were cracked, it would be impossible to make an original printout of the stored result.

Therefore, it is impossible to make an image of a stored DMS® template from a fingerprint that could then be compared to another database or image that was found.

Biometrics means the determination of measurable characteristics of living creatures, such as average life span and racial characteristics. Since the end of the 20th century, it refers to one of the identification methods based on unique body characteristics of persons (see below). It is in fact a continuation of dactyloscopy, the science of fingerprint identification, which, as well as identification based on DNA characteristics, is mainly used in the fight against crime.

Biometrics, however, has a much broader application and is ideally suited as a security method, for example. Many application methods are possible or under development. Biometrics can, in principle, replace cards, keys, passwords, codes, or in combination with these, strengthen security. The starting point of biometrics is that the person is inseparable from his/her body. The most important advantage of a biometric identification method is, therefore, that it does not depend on possession (key card) or knowledge (pin code or password):

the body itself contains characteristics that are so unique that identification is possible. Fingerprints are unique and personal, as are the patterns on the palms of the hands, soles of the feet and toes. The uniqueness is determined by the papillary lines of the finger, which are formed between the 100th and the 120th day after fertilization. The pattern is formed by genetic and stochastic environmental factors, and is thus unique to everyone, even identical twins. Fingerprints can be divided into 9 main groups, namely:

1. simple arch
2. tended arch
3. ulnar loop (to the right)
4. radial loop (to the left)
5. double loop
6. whorl to the right
7. whorl to the left
8. plain whorl
9. combination pattern
0. missing finger

A fingerprint can be classified into one of these main groups. A fingerprint can be identified when it has at least 12 points of similarity, *without* any discrepancies. Think of a starting ridge, splitting ridge, circle, short ridge, etc. The fingerprint method is one of the most reliable methods in biometrics to identify persons.

Companies are making increasing use of biometric applications in information and access security. This is due to the need for security, convenience, and reliability that biometric technology has to offer.