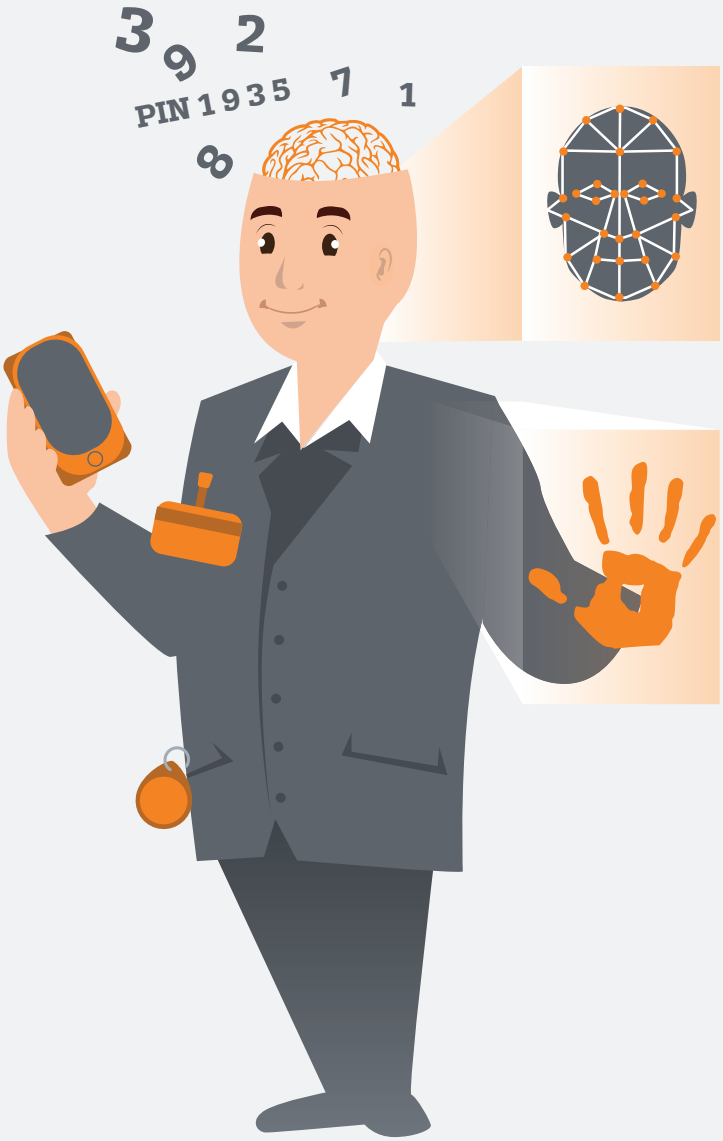
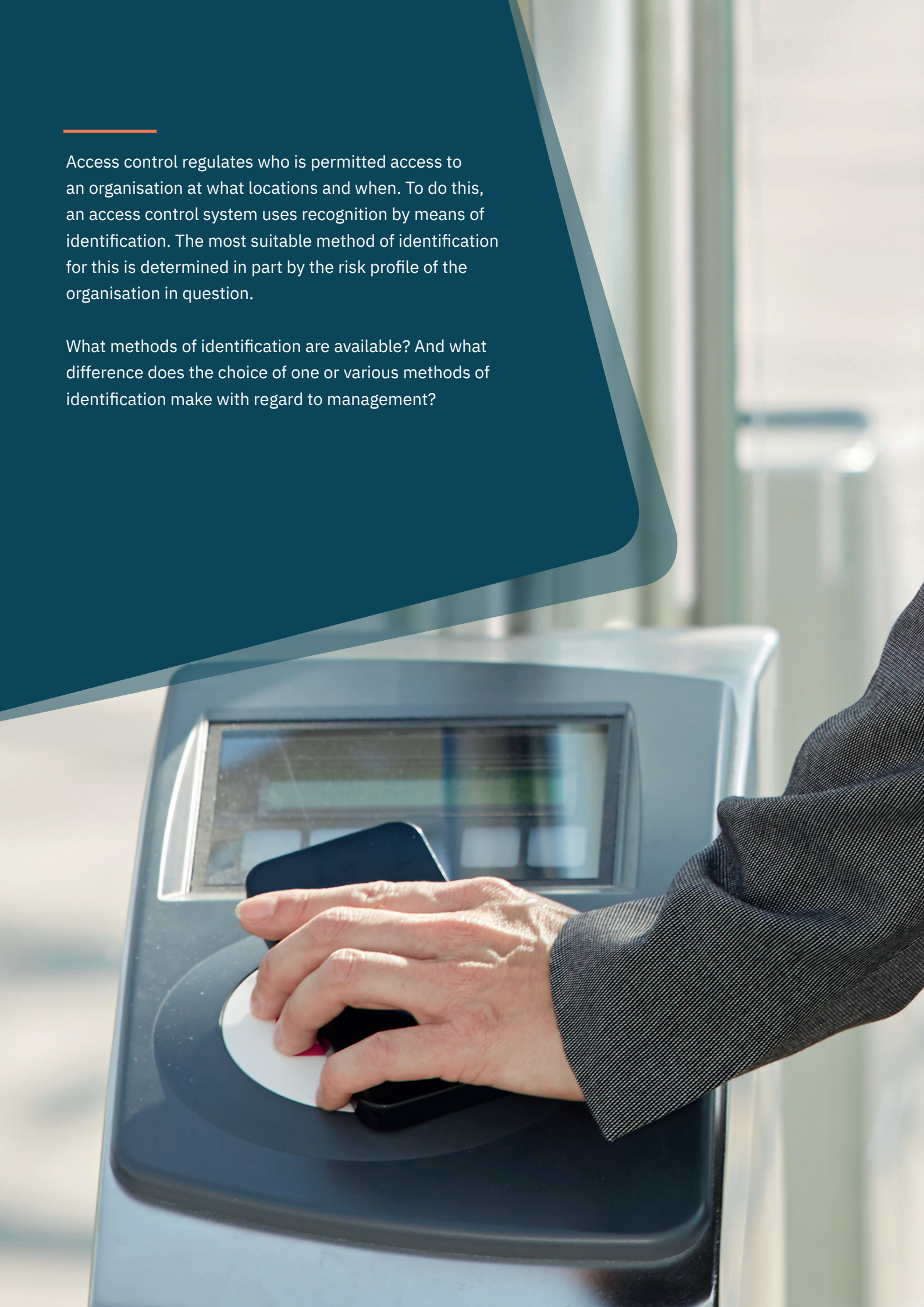
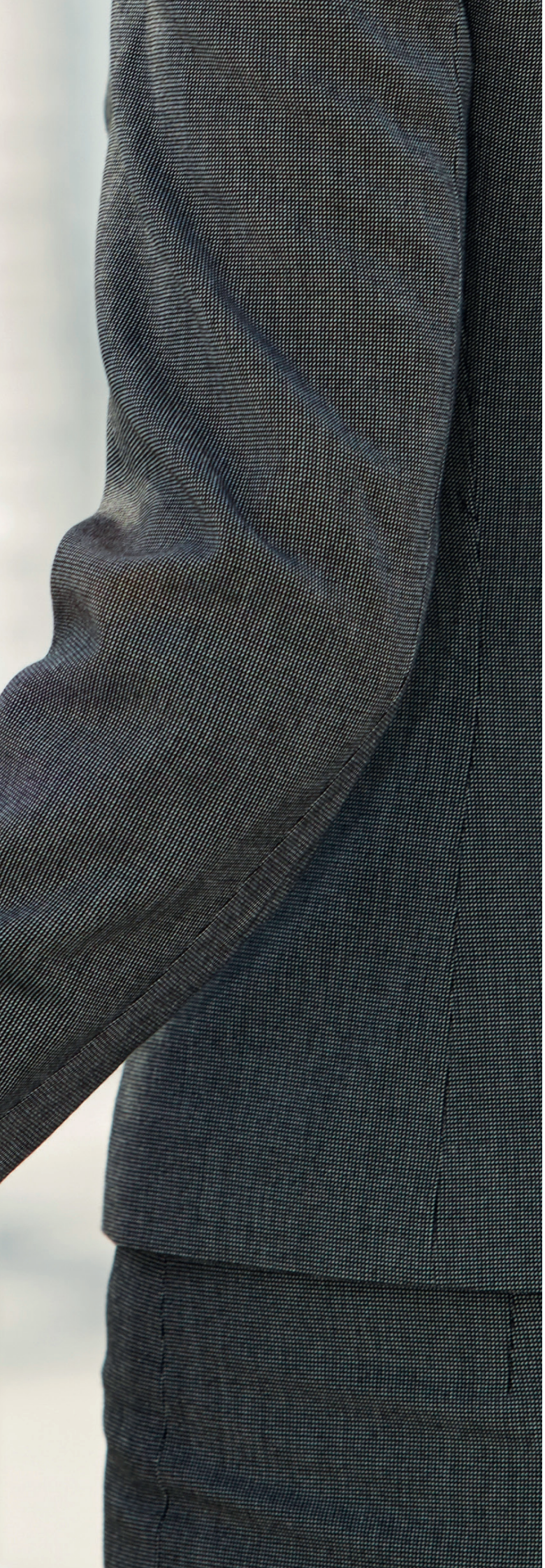
Access control systems and methods of identification



Access control regulates who is permitted access to an organisation at what locations and when. To do this, an access control system uses recognition by means of identification. The most suitable method of identification for this is determined in part by the risk profile of the organisation in question.

What methods of identification are available? And what difference does the choice of one or various methods of identification make with regard to management?





The purchase of an access control system is preceded by a very detailed process; you not only consider the existing risk profile of your organisation, but also (if the risk profile is favourable) the future developments of both the organisation and technology.

Access control systems use recognition by means of identification. This is why it is important that you also consider carefully which identification methods suit your organisation best, both now and in the future, when making your final choice for an access control system. This is because identification is possible using a variety of methods and different means, ranging from an access code, an access card, a mobile telephone (which is being increasingly used for this purpose) to the use of biometric data. This article describes the most commonly used methods of identification.

Access code

A simple method of opening doors is to use an access code. Care institutions in particular often use this form of granting access. The advantage of using an access code is that it is not necessary to issue separate passes, which eliminates the issues of loss or wear and tear. The disadvantages are that users cannot pass through quickly and may forget the access code. Access code can also be easily shared within a group of users. However, this also restrict the ability for an access control system to identify the in individuals.

Access card

Most access control systems, however, use physical information storage media in the form of cards, passes, key fobs and tags. For the ease of reference, in the following session, we name all different storage media as access cards. Before examining the different variants, there are a number of characteristics that you need to take into account.

- **Data:** The quantity of data that can be stored on a card varies. If you only use the card for access control, several bytes of data are sufficient. But if you also wish to use the card for contactless payment in the company restaurant or for follow-me printing, for example, then more capacity is needed.
- **Security**: When choosing an access pass, you need to take into account of two risks. First of all, there is the risk of cloning, whereby malicious parties produce duplicates of the cards. The second risk is the 'replay' of access cards, whereby the data between the card and the card reader is stored, such as on a laptop. The stored data can then be used to simulate the functioning of the original card. Effective encryption can prevent both cloning and replay.
- **User convenience**: An increasingly important factor is user convenience. Consider the presentation of the card to the card reader and the speed with which the door opens.
- **Standardisation**: ISO standardisation makes communication possible between cards and card readers of different suppliers. This means that an organisation is no longer dependent on one supplier.
- **Durability**: Access passes are used intensively. Therefore, susceptibility to wear and tear is an important factor in the final choice. Commonly used proximity and hands-free systems avoid physical contact between the card and the card reader, which minimises wear and tear.

Bar code

Access cards with a bar code are a good choice for visitor management where user convenience is paramount. The cards can be printed easily and at low cost. What is more, the authorisation only applies for a limited time and the visitor is no longer required to hand in the card. A disadvantage is that the cards are easy to duplicate, which means that they are not suitable for situations where strict security requirements apply.

Contact smartcards

Contact smartcards containing a chip are often used for accessing IT equipment such as laptops. The advantage is that it is possible to combine physical access and access to IT equipment in a single pass. The disadvantage is that this card is not suitable for all types of physical access control.

RFID

Most modern access control systems use RFID technology. RFID or Radio Frequency Identification is a technology for reading information remotely from RFID tags in access cards. The advantage of this technology is that, in addition to access control, the card can also be used for other applications, such as contactless payment or logging into an IT network. The technology is also suitable for use if user convenience is important, if strict security requirements apply and if strict security requirements apply and in difficult conditions such as cold or heat.

The following RFID technologies are available and are used in access cards.

Low-frequency (LF) RFID

An access pass with LF RIFD is reliable, offers a reading distance upto 10 centimetres and data transmission is not affected by moisture or dirt. The problem, however, is that suppliers of these passes do not use ISO standards, which means that a combination of cards and card readers from different suppliers is not possible. Furthermore, their data speed is low and only a small quantity of data can be transmitted.

High-frequency (HF) RFID

Mifare and Legic are the most well-known HF RFID cards. The use of ISO standards makes it possible to combine cards and card readers of different suppliers. The cards hold a large memory and the use of DES encryption makes them especially secure. The maximum reading distance is between 10 centimetres to 1 metre.

Ultra high-frequency (UHF) RFID

Cards with UHF RFID have a reading distance ranging from 1 metre to well over 30 metres. They can be used in combination with HF RFID technology. This means it is possible to grant access both to vehicles remotely and to individuals who stand next to the reader. It is important to note that the distance to the reader cannot be too great; this, in fact, makes it less secure, as multiple people are able to enter at the same time while the door is open. The disadvantages are susceptibility to dirt and that the UHF signal will not pass through metal.

Microwave RFID

Cards with this technology are used by access control applications that require a large identification distance up to 200 metres. This technology is suitable for vehicle identification on company sites with multiple entry lanes, for example. The advantage of this technology is that recognition of individual vehicles remains possible, but it is also the case that its use is less secure if the distance to the reader becomes too great. What is more, the cards require a battery, although this may last for years.

Mobile telephone

A recent development is that the mobile telephone is able to function as an access card. It is simple and easy to use, because most people nowadays carry a mobile telephone with them.

Access control with a mobile telephone uses the following two technologies:

Near Field Communication (NFC)
NFC is similar to RFID, but there are specific characteristics such as user convenience, reading distance and durability that depend on how NFC is implemented in the access control system. When NFC is used, the mobile telephone contains a unique ID number, and this may be incorporated in the hardware by building it into the device itself, into the SIM card, or into the NFC microSD card. This requires a partnership with the handset manufacturer or the network operator. Another possibility is the use of host-based card emulation, in which software-based encryption is used.

Bluetooth Low Energy (BLE)
BLE is a wireless signal over short distance, but it has a larger range than NFC. The advantages of this technology are user convenience, possible combination with RFID card technology and a reading distance of several metres. What is more, it is possible to use with both Android and iPhone. The disadvantage is that the technology is still developing. As a result, there is a wide variation in mobile phones, which may give rise to compatibility issues.

Biometrics

Organisations with a high risk profile may opt for an additional form of identification or verification, such as biometrics. Biometrics is a method of establishing or verifying the identity of a person based on physical characteristics, for example.

In the case of biometric identification, the system will automatically recognise a person from a list of users in a database.

Biometric verification is also possible. This is then a case of confirming or denying the identity of a person who, for example, presents an ID card and is then prompted for a fingerprint in order to confirm his or her identity.

When choosing the most suitable biometric technology, you need to take account of the following characteristics:

- **Accuracy:** EA biometric system must not identify an authorised user as an unauthorised user, or vice versa.
- **Fraud:** All systems can be defrauded. But the level of vulnerability is different with different biometric technology. For example, an iris scan is more difficult to copy than a fingerprint.
- **Stability:** Biometric features such as face and fingerprints may change over the course of time, which may give rise to errors in recognition.
- **User-friendliness:** The system must be simple and intuitive in everyday use so that authorised persons are recognised effectively. Poor lighting or an awkward location of biometric readers may be detrimental in this regard.
- **Speed:** The decision to grant or deny access must be made within a few seconds. This is particularly the case in locations where many people require access or where people may pass through several times a day.
- **Recording:** Good performance and accuracy are only achieved if the features of persons are properly recorded. This starts with clear user information and guides on how to use the system.

The biometric technologies most commonly used for access control are:

2D face recognition
2D face recognition involves taking a picture of the face with a camera. This image is converted into a unique mathematical code and is stored as a template. The technology is suitable for identification or as a verification measure, is easy to use and offers high speed of recognition, but is less accurate.

3D face recognition
3D face recognition involves creating a threedimensional map of the face using infrared grids or by combining multiple images. This technology is suitable for identification or as a verification measure, is easy to use and offers high speed of recognition. A major difference compared with 2D technology is the higher level of accuracy.

Iris recognition
Iris recognition involves taking a picture of the eye with a near infrared camera. Iris recognition offers a very high level of accuracy and is therefore often used in organisations with a high risk profile. The disadvantage, however, is that the lighting during scanning is a very important factor in the final outcome. The iris may also be damaged, or be harder to read due to the user wearing spectacles.

Fingerprint recognition
Fingerprint recognition is a most commonly used biometric technology, whereby a person's fingerprint is compared with the template in the database. The method is accurate, although dirty or injured fingers may pose a problem. For this reason, it is recommended that prints of two or three fingers are recorded per person.

Hand geometry
Hand geometry involves producing a threedimensional image of a person's hand. This technology is not highly accurate, but it is easy to use. For example, large numbers of users can be processed rapidly and dirt or moisture has a minimal impact on the performance of the hand reader.

Vein pattern recognition
Vein pattern recognition involves recording the blood vessels of a body part, such as the palm of the hand, the finger or the eye, which are then used to identify a person. Vein pattern recognition only works with living persons, is highly accurate, and dirt or moisture has a minimal impact on the performance of the reader. The disadvantage of the technology is that recognition may be affected by low temperatures.

Management

It is evident in practice that an organisation often cannot manage with a single identification method, whether because different risk profiles exist, or because new developments need to be anticipated. It should therefore be carefully considered that only access control systems with open standards are suitable for using a combination of different identification methods.

It is also important for you to realise that the choice for one or more identification methods has implications for the management thereof. Imagine that you will use different methods of identification; how do you manage them? For example, will an employee who holds several means of identification appear as many times in the system? You can optimise management by linking together the different information systems, such as the staff information system, the facility management system and the access control system. Obviously, the staff information system should then be used as the source, and this centrally managed information should also be used as the basis for management of the means of identification. If an employee leaves the organisation, you will only need to amend his or her data once centrally in the staff information system, and all his or her means of identification will be automatically blocked.

Conclusion

An access control system with open standards offers you the freedom to choose how to implement the different identification methods that exist within your organisation. Furthermore, you can adapt the methods of identification over the course of the years and you can expand the system using other methods of identification.
Finally, your management task is made easier because you can link the access control system to the other information systems within your organisation.

Want to know more?
Just get in touch with us.

Nedap Head Quarters
Parallelweg 2
7141 DC Groenlo
The Netherlands
+31 (0)544 471 111
info@nedapsecurity.com