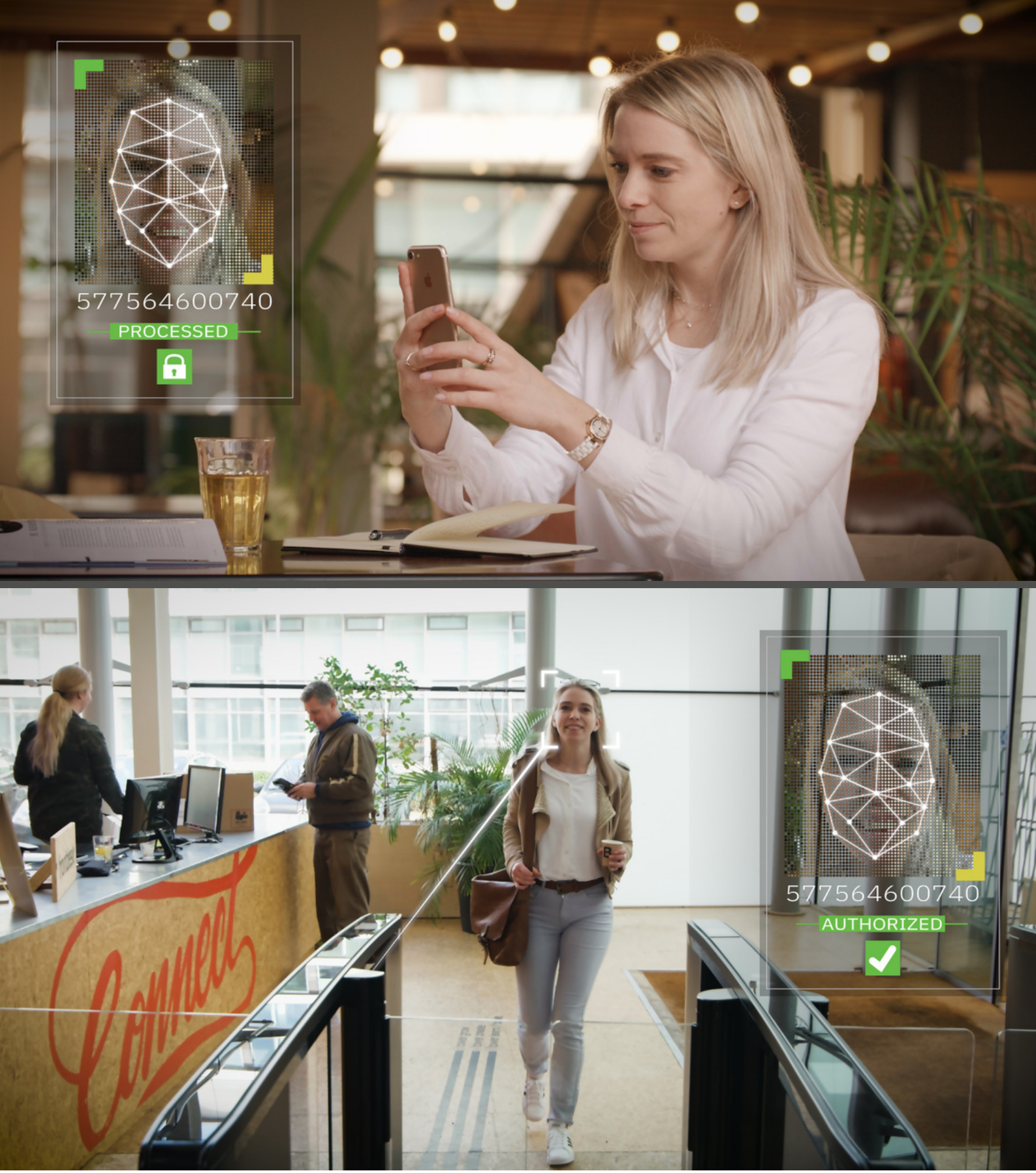


FACIAL RECOGNITION
IN ACCESS CONTROL.

A **WHITE PAPER** POWERED BY BOON EDAM

150 YEARS BOON EDAM
YOUR **ENTRY** EXPERTS.

INTRODUCTION.

This white paper explains how facial recognition access control works. It also discusses what factors should be taken into account when selecting a facial recognition access control system. As facial recognition technology has only recently become available on the market, you may be wondering what aspects can play a role in the application. Reading this white paper will provide better insight into what facial recognition access control entails exactly, and what to consider when purchasing such a system.

TYPES OF **BIOMETRICS**

Biometric identifiers are all the measurable characteristics that can be used to describe human beings. Biometrics are increasingly popular in access control applications. These are the four most common forms:

IRIS SCAN

Every human iris has its own unique traits. An iris scanner identifies pits, furrows and striations in the iris and converts these into an iris code. Comparing this code to a database subsequently determines whether to allow access.

PALM VEINS

Near-infrared illumination exposes a palm's unique pattern of veins and capillaries. Some palm scanners also measure features such as creases and nodules. This information creates a unique profile that can be linked to an authorised individual.

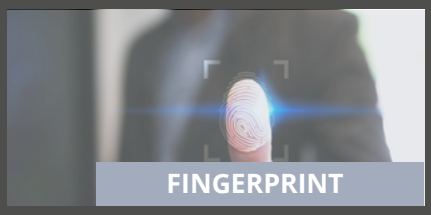
FINGERPRINT

There are various types of fingerprint scanners in existence. These all work by registering the unique pattern of lines on the skin. The resulting data can be used to determine whether to allow access.

FACIAL RECOGNITION

The final type of biometric access control employs facial recognition. An algorithm is used to filter a human face from a video or photographic image. In only a few milliseconds, the face's characteristics are recorded and converted into a unique code.

Then the facial recognition software compares the code to a database. If it finds a match, this can be used to identify the individual in the image and determine whether or not to allow access.



FACIAL **RECOGNITION**

Facial recognition can be useful in various applications. This white paper concentrates on access control. Differences between the areas of application are discussed briefly below.

MASS SURVEILLANCE

Mass surveillance uses facial recognition to pick individuals out of a crowd. This requires specialised hardware and powerful software in order to be effective.

PERSONAL AUTHENTICATION

This type of facial recognition is commonly employed in mobile devices such as smartphones, with relatively simple software and hardware requirements. Here the face is used as an alternative to a passcode.

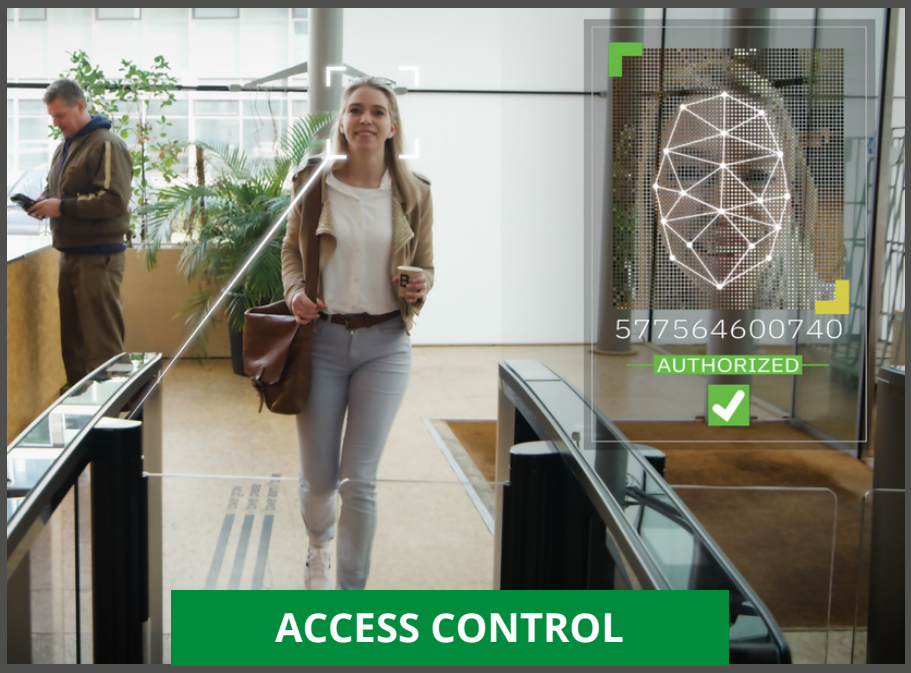
FORENSIC INVESTIGATION

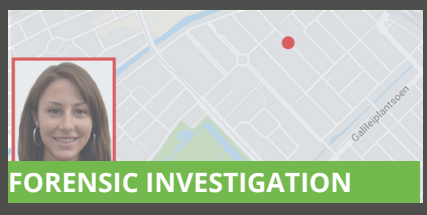
Facial recognition can also be used to reconstruct an individual's route based on video images. For example, such data can help identify where a fugitive was located over the past 24 hours.

ACCESS CONTROL

Finally, facial recognition can be used within access control. It is important to have the software set up to compare information from multiple cameras with the database in real time. Based on the database size, a server is installed that can verify the authorisation with sufficient speed and then the access point can be opened.

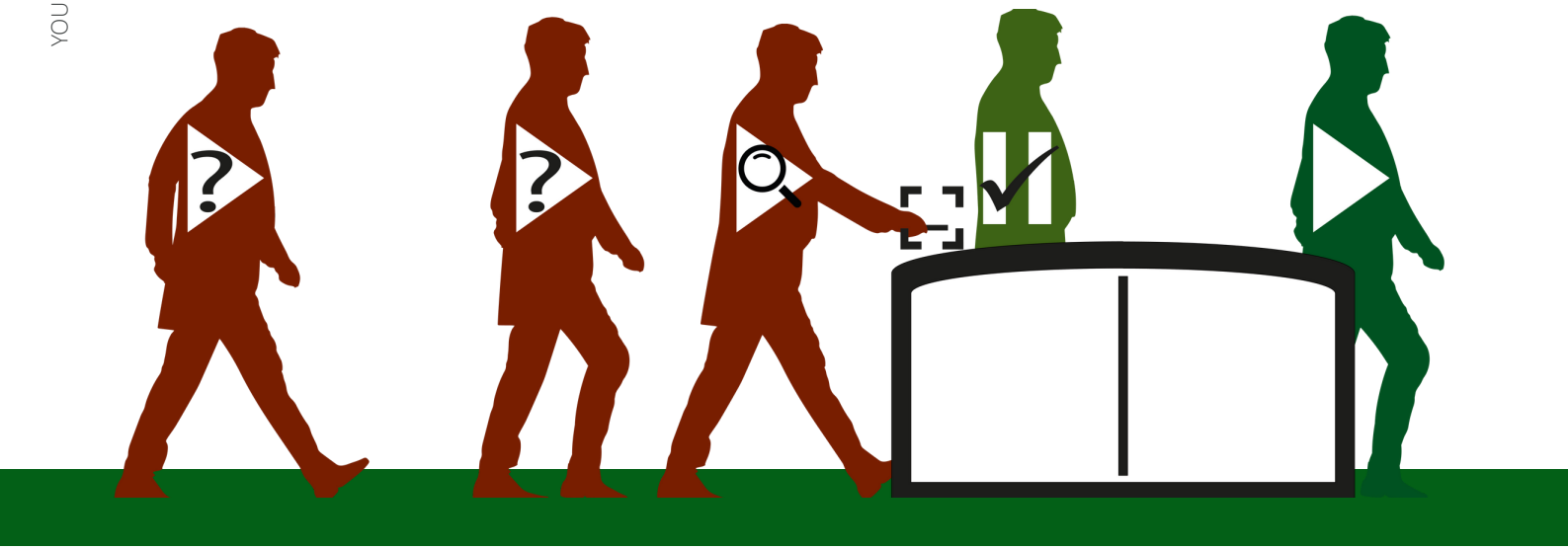
IN THIS **WHITE PAPER:**



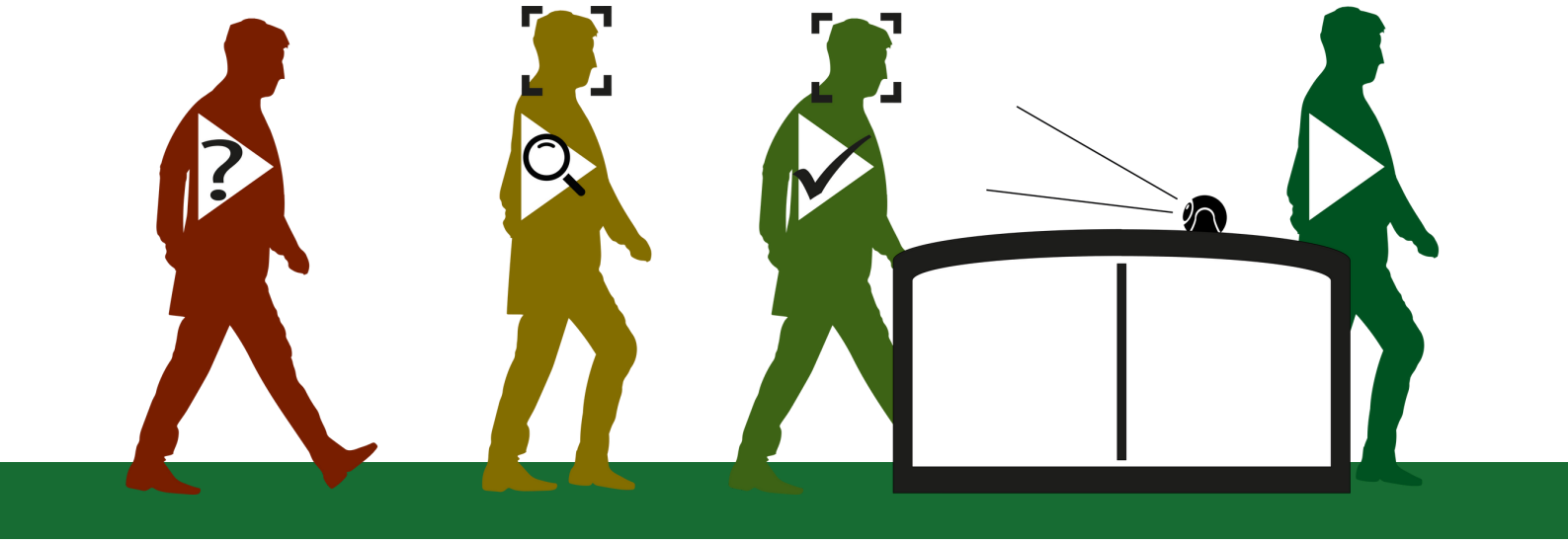


ADVANTAGES OF FACIAL RECOGNITION.

'TRADITIONAL' **CARD READER**



FACIAL RECOGNITION



IMPROVED **FLOW**

One of the major advantages of facial recognition access control is the lack of waiting at the access point. The software will register a person's face as they approach and can determine whether to allow access in the time needed to arrive at the gate. When the authorised person is near or at the access point, the system opens the gate. This prevents unauthorised individuals from slipping in through the open gate. Also, the person can proceed smoothly through the access point.

QUICK ACCESS AT ALL TIMES

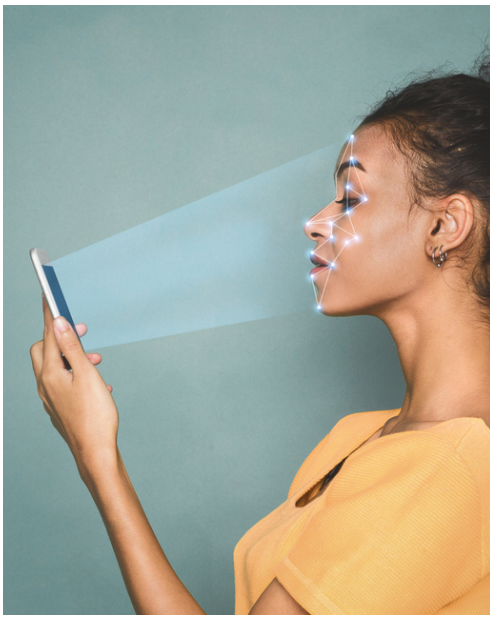
Because biometric facial recognition is based on something people always carry with them, they will never face a closed door. As all faces are unique, people can be distinguished from one another and identified by means of their facial features.

An additional advantage is that only minimal active cooperation is required of the user at the access control point. As soon as a face enters the camera's focus range, the software can check the authorisation. As access passes are no longer necessary, they also cannot be forgotten. Moreover, there is no more need to wait for a colleague to dig through their things for a pass and hands are free to hold coats and bags.

NO SHARING OF PASSES

One common issue in access control is the sharing of personal passes with colleagues. Such improper use can lead to unauthorised people entering the premises. Using facial recognition prevents unknown individuals from passing through access control just like that.

Furthermore, facial recognition access control makes it impossible to steal or copy an access pass. The result is an improvement in the level of security overall.



BIOMETRICS ARE TOUCHLESS

Many people hesitate for just a moment before having their iris or finger scanned. Their (subconscious) hesitancy is due to a lack of familiarity with the system or a reluctance to actively present a body part to the scanner. In addition to disrupting the flow, this can lead to the access control being experienced as less user-friendly.

Another major benefit of facial recognition is the fact that it records users from a distance using a camera. Users needn't assume an awkward position or physically touch the access point. As soon as they enter the camera's specified range, it will verify their identity and can allow them to proceed through the access point uninterrupted.

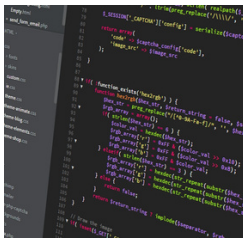
COMPONENTS OF FACIAL RECOGNITION.

When opting for facial recognition access control, one thing to consider is that the system will contain multiple components. These components are often supplied by different parties and must interact with each other. It is therefore important to investigate which suppliers can build a smoothly functioning system together. Generally, the following components will need to interact:

CAMERA & OTHER SENSORS

The camera is an important element in the reliable application of facial recognition software. There are various high-quality cameras available on the market. Experience has shown that a careful selection based on both technical and aesthetic factors can contribute to user-friendliness and acceptance.

The selection process concerns more than just the number of megapixels; light sensitivity, the type of lens and the chip's processing power are important considerations as well. It is also possible to opt for additional sensors, to be able to distinguish a face from a photograph for instance.



FACIAL RECOGNITION SOFTWARE

Also known as the heart of the system, facial recognition software converts facial features into a code for comparison with a pre-established database. Recognition is achieved using a series of algorithms. Facial recognition software frequently operates independently of other forms of access control software. This allows for the creation of a stand-alone system running the software on an external processor.

It is important to ensure that the software and system are in compliance with the General Data Protection Regulation (GDPR) and have the correct encryption standards.

ACCESS CONTROL SYSTEM

Access control systems often combine multiple software solutions. Frequently, these solutions are integrated with a Security Management or Building Management System. The facial recognition software may therefore need to be compatible with such a system as well.

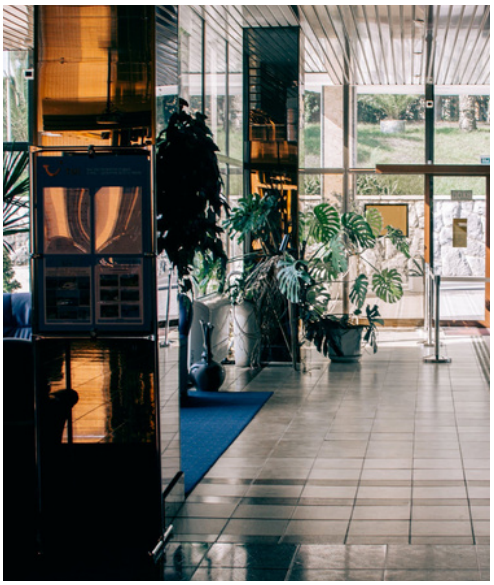
In practice, this will involve the linking of various modules for subsequent control by a single, central program. In that case, the "facial recognition software" module will be integrated by means of an API.

PHYSICAL ACCESS

In access control applications, facial recognition is always used in combination with a physical access control product. After all, it isn't possible to deny access to unauthorised individuals without such a barrier in place. There are various barrier options available, each with its own security implications.

The components can be configured in various ways. There are physical products with fully integrated facial recognition available, for instance, but components can also be purchased separately.

TECHNICAL ASPECTS.



LIGHTING CONDITIONS

One of the most important factors in successful facial recognition is the amount of light in the area where the camera is located. In the case of access control, facial recognition often takes place indoors and the lighting conditions are easily adapted.

Overexposure can be a real challenge. Examples include bright sunlight, glare due to reflections or high glass ceilings. Fluctuations in the lighting can be difficult to handle for the camera and facial recognition software.

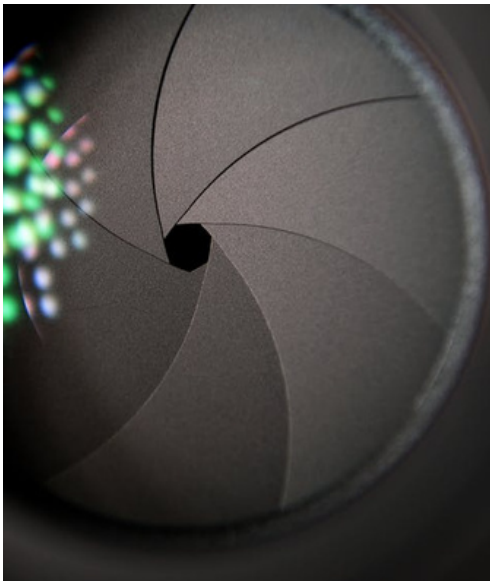
Underexposure is much easier to correct. Often, adjusting the camera settings can be enough to achieve good recognition. It is advisable to engage an expert to establish the correct settings.

CAMERA PLACEMENT

When mounting the camera, carefully consider the recorded image. The closer the camera is to the person seeking access, the higher the quality of the image will be.

The position of the camera in relation to the user is also relevant. It is best to position the camera in such a way that the user is already looking in that direction as they prepare to pass through the access point. That way they will not need to perform any additional manoeuvres to be recognised.

Finally, it can be desirable to integrate the camera in the access control product or to mount it externally for aesthetic reasons.



CAMERA FOCUS

When installing the camera, carefully consider the focus. This should be set to where the facial scanning will take place. The focal distance must not be too far from the access point (to prevent people slipping in), nor too close (resulting in a wait).

The camera focus also determines the range within which faces will be recognised. This can be adjusted by selecting in the software an area of the image within which facial recognition should take place.

Our experts will be happy to help you choose the right technical specifications for your situation.

IN PRACTICE.

USER FLOW

In practice the use of speed gates naturally encourages users to assume a forward-facing position. People will move through the product in a straight line, looking ahead. The result is a relatively small zone through which all users' faces will pass.

Another great advantage of facial recognition access control is the improved user flow. This is because the users are all headed in the same direction, moving through the speed gate in a steady stream. Facial recognition ensures the authentication process is fast enough to maintain a speedy flow of people.

PRESENTING THE FACE

Earlier in this white paper it was noted that users needn't perform additional manoeuvres with facial recognition access control. This is, however, dependent on the user's awareness of the fact that the facial recognition software must be able to scan their face.

In practice this means users must present their faces to the camera more or less unconcealed. They will not be able to enter the access point while wearing a face mask or looking backwards, for example. Users must cooperate for the system to function.

INTERACTION WITH THE USER

In the use of facial recognition, and access control in general, good feedback to the user is important. When multiple individuals use an access point in rapid succession, visual and audio signals can communicate the software's conclusions to the user.

Facial recognition is well-suited to situations with many repeat users. After registering once, a user can be granted access for as long as needed. Repeat users will also grow accustomed to the interaction with the access control product.

DIGITAL SECURITY.

ENCRYPTION

To prevent data and images transmitted over a network from being easily hacked, facial recognition software makes use of encryption. Encryption involves the coding of digital (image) information. Without prior knowledge of the encryption process, it will be impossible for outside parties to read the data.

Various data encryption methods are available. The existing infrastructure and (current) video management software platform will determine the most appropriate solution. For instance, it makes a difference whether the data is transmitted over a closed or open network. Our experts are happy to answer any questions you may have on this subject.

FRAUD DETECTION

When it comes to fraud detection, facial recognition is constantly evolving. The aim is to prevent the system from being "fooled", by presenting a photograph to the camera, for example. There are currently two methods to detect and prevent fraud:

- Hardware-based detection by means of 3D sensors that scan the faciaL structure. One version involves a sensor that registers the pattern of coloured rays of light reflected off a face.
- Software-based detection that picks up on minuscule discrepancies in the video image. This requires a great deal of (video) processing power, necessitating larger and more powerful servers.

GDPR

Earlier in this white paper it was noted that facial recognition makes use of biometric data. In the context of the General Data Protection Regulation (GDPR) it is important to know that biometric data belongs to a special category of personal data. Data in this category may be used for personal identification under certain conditions. The data must be used exclusively for authentication or security purposes. Additionally, the system administrator must be able to prove that the data processing is in compliance with this regulation. Employing facial recognition in access control applications is therefore legally permitted.

CONCLUSION.

The aim of this white paper is to offer some initial insights on what is involved in facial recognition access control and what considerations will determine the most suitable facial recognition system for your business. It explains the differences between various types of biometrics and facial recognition methods. Additionally, it describes the advantages of facial recognition when compared to traditional access control systems.

We also introduce the various components of facial recognition systems used for access control, as well as the most important technical and practical aspects of facial recognition systems. Finally, this white paper briefly touches on facial recognition's use in the context of digital security and the current GDPR regulations.

RECOMMENDATIONS

With this white paper, Boon Edam has attempted to offer you some insight into facial recognition's associated conditions and requirements. We believe that facial recognition technology has proved its value in recent years and that its future use will only increase. Furthermore, we wish to point out that facial recognition is suitable for access control at nearly all levels of security. Based on your own wishes concerning the implementation of facial recognition and your specific circumstances (such as the number of people the system must recognise, access point location(s), etc.), we will be happy to help you select and implement the most optimal system for your needs.

For more information about facial recognition access control, please contact your local entry expert. We will be happy to visit you for a no-obligation consultation.

FAQ.

If, as a user, I approach an access point with facial recognition, this encodes my facial details and compares them to a database. Does this mean it will store my photograph?
No, database creation does not require storage of users' faces; a list of hash codes is sufficient. Nor will the use of an access product require photographs to be stored for comparison purposes. In practice, however, facial recognition installations may (temporarily) store photos on occasion in order to optimise the software. These are located on a stand-alone server and cannot be shared with third parties.

Is any other data stored in addition to the hash code?
Generally speaking, traditional access control systems register the time when an authorised user enters the premises and this also applies to facial recognition installations. It is possible to adapt the settings to prevent the storage of such data.

Is this type of facial recognition suitable for use with other entrance solutions besides gates?
Yes, this type of facial recognition is also suitable for use with various other entrance solutions. We'd be happy to discuss the possibilities with you.

OUR REACH **IS GLOBAL.**

We have been in business for 150 years, manufacturing premium aesthetic and security entrance solutions in The Netherlands, the United States of America and China. We can confidently say that we cover every corner of the globe with subsidiary companies in major cities across the globe. Furthermore our global export division not only partner with our distributors, but also offer direct sales and service to every territory. This wide net allows us to have a strong global footprint and a personal grasp of local markets and their unique entry requirements.

To find your closest Boon Edam expert, please go to:
www.boonedam.co.uk/contact

Boon Edam Limited
T 01233 505 900
E uk.contact@boonedam.com
I www.boonedam.co.uk

V1-2212

BOON EDAM
YOUR **ENTRY** EXPERTS.