The integration between Nedap system and FTF technology is to optimize user physical access control via facial recognition. The integration supports enrollment of user’s identity and authorize the access by creating a virtual badge into the AEOS access control system comparing a live image with the one associated to the badge.

FTF solutions works in a connected or disconnected mode to negate any connectivity issues.
The system has data privacy at its heart and is set to be fully GDPR compliant. Users will first need to enroll to be able to use the system and all data collected will be encrypted and securely stored. As part of this users will be made aware of the way their data will be processed and used while the system also allows data deletion upon request.

**Wesley Keegstra, Integration manager at Nedap Security Management said;**
“FTF managed to create a very flexible facial recognition solution. I was surprised by how hardware independent they are. They take a basic camera and use the live feed in their software to identify people. This is transferred to the Nedap AEOS access control system, where the person is authorized or not. Many thanks to the FTF team for all their effort, and for this great collaboration.”

What are biometric technologies? Biometric identification refers to the automated recognition of individuals based on their behavioural or biological characteristics. Biometric technologies are concerned with either physical aspects of the human body, for example the face or fingerprints, or the personal traits of human beings, for example a signature or voice pattern. To be useful, biometric technologies must recognise or verify these physical aspects or human traits quickly and automatically, in real time. There are two different ways to recognise a person via biometric technology: identification and verification. When applying biometrics for identification purposes, the system has to recognise a person from a list of users in a database. Verification, on the other hand, involves confirming or denying a person’s claimed identity, for example the user presents an ID card and is then asked to present a finger or face to verify his or her identity. Biometric technologies enable organisations to identify or verify the identity of individuals with a high degree of certainty. For that reason, it was first used in high-security environments. With the arrival of user-friendly and affordable systems, however, biometric technologies began being applied in a variety of systems and environments.

Biometric technologies have specific characteristics that help you to determine their benefits and shortcomings and enable you to select the most suitable technology for your organisation. The most important characteristics are discussed below. Accuracy: acceptance level versus error rate A biometric system should not reject authorised users (FRR, False Rejection Rate) or provide fraudulent access (FAR, False Acceptance Rate). Comparing the EER (Equal Error Rates where FRR = FAR) of the different systems available can be instructive as it demonstrates the relative strength of various biometric systems. Fraud All systems are susceptible to fraud, but defrauding modern systems takes significant knowledge and skills. The many differences in the various technologies make fraud even harder. Copying biometric characteristics is more difficult for some systems than others. Copying a fingerprint, for example, is easier than presenting a forged iris. Another threat relating to fraud involves sniffing data from the sensor and playing it back to the biometric system. Encrypting the data coming from the sensor can prevent this, as can changing the biometric data on a card or database.

Stability Biometric characteristics like faces and fingerprints can change over time causing errors in recognition performance. Hands and fingers can change due to fluctuations in weight, for example, and age can influence face recognition. While damage or illness can change fingerprints or the iris, even though these are usually more stable. Some biometric systems can overcome these changes by automatically storing updated templates. Usability The system should be easy to learn and simple to use in everyday practice. Particularly in situations where user training isn’t possible, the system should be intuitive to ensure that authorised people are being correctly recognised. Irritating lighting or an inconvenient location of biometric readers, for example, can also have a negative influence on practical use. Speed For convenient access control the decision to grant or deny access must be given within seconds, especially at places where many people require access, or where people pass through several times a day. Enrolment The majority of recognition failures in a biometric system are caused by improper enrolment. Good performance and accuracy can only be achieved when people’s characteristics are enrolled properly. For all systems, this starts with clear user information and guidance on how to enrol people and use the system. Vein, retina and iris systems demand extra effort as they’re less commonly used than fingerprint and face recognition solutions.

With FTF - 3D face recognition, a three-dimensional map of the face is created through infrared grids or the merging of multiple images. As with 2D face recognition, it’s very user friendly and people are identified quickly. 3D images contain more unique characteristics, so recognition accuracy is higher than with 2D face recognition. The drawback is that glasses and beards can have a negative effect on accuracy.