



smartⁱ

Security. Control. Comfort.

access control
time & attendance
building management

based on multimodal biometrics using facial and voice recognition

Samples of use:

Access Control

Introduction

Access control systems are one of the most important components of complete solutions for safeguarding of information and property. And in Access control only biometric solutions make a consistent and effective enforcement of security standards and recommendations possible.

Biometrics – a reliable means to recognize or authenticate the identity of an individual by measuring and statistically analyzing his unique physical or behavioural characteristics; like fingerprints, hand or palm geometry, retina, iris and facial characteristics, voice samples, gait... These biometric features are securely stored by the hardware and/or software and can later be used for identification of the individual.

Multimodal biometrics – the use of more than one biometric identifier to establish an individual's identity makes an ultra-secure and more than averagely accurate biometric identification system.

Besides the above mentioned characteristics such a system is expected to be easily integratable, versatile and all-round functional. The time stamped access register, which must be recorded by the system, can also be used to track attendance and presence for security and business purposes.

smarti is set to meet this challenge. It recognizes people based on several biometric parameters making it extremely secure and reliable. The biometric information about an individual is saved and encrypted in a database which can be securely kept on the **smarti**[®] unit or on a certified server.

This way the biometric patterns can not be lost, stolen, fraudulently acquired, damaged, misappropriated or lent to someone like per example ID cards, PIN codes, passwords etc.

smarti is a complete access control and time & attendance solution with numerous additional features: video intercom, video phone, video massaging, external I/O device control and tracking (proximity card scanners, different biometric scanners...).

smarti satisfies the contemporary security demands, standards and recommendations reliably and economically.

Case 1

The situation

An IT company which does a lot of work with the government implemented a biometric access control system for their server room where sensitive and confidential government data is stored. Because of data security issues only 15 certified and verified individuals have access to the server room and their presence in the room is always tracked. The access control system is also connected to the alarm system and to the fire alarm system.

The solution

To achieve a higher level of reliability and security the company wanted to use more than one biometric identifier to establish a person's identity. They needed a system which would also track when a person entered the room and when this person left the room. This is why they decided to use the **smarti** system supported by fingerprint readers.

The **smarti** unit was installed by the door which leads in to the server room. Two fingerprint readers were also connected to the **smarti** unit one was fitted below the unit and the other was fitted on the other side of the wall inside the server room.

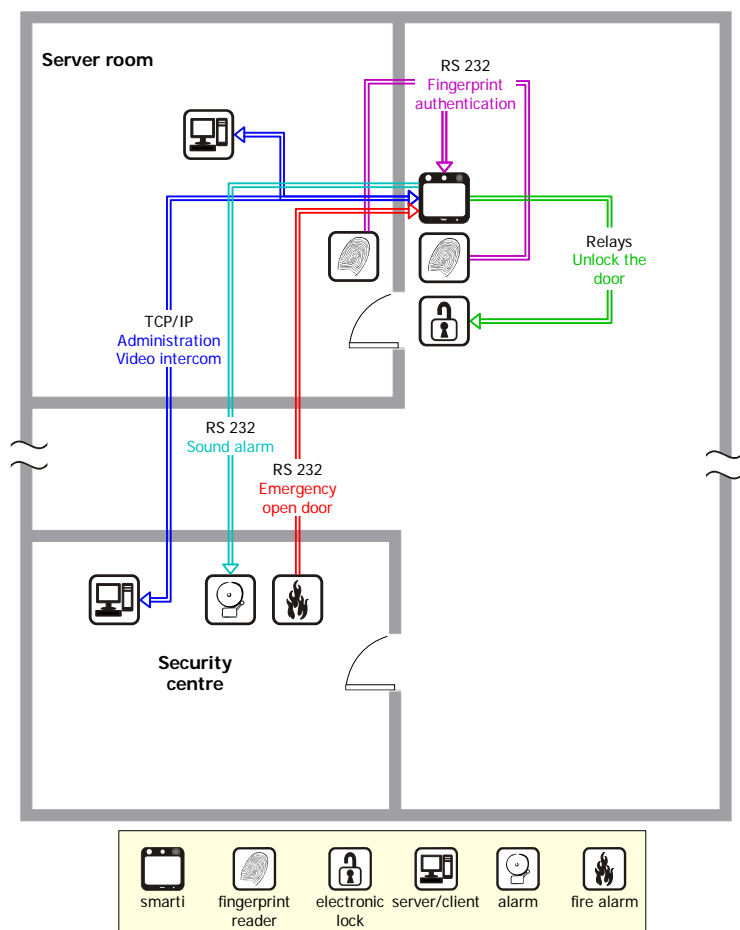
The alarm system and the fire alarm systems were connected to the **smarti** unit using the RS 232 ports.

The **smarti** unit was connected to a server in the server room and to a computer in the company's security centre via TCP/IP. All data about the authorized users and the events is saved on the server and the system is administered from the **smarti** client in the security centre. Access rights and schedules can be assigned and events can be tracked from a single location.

To enter the room a person must first authenticate himself by using the fingerprint reader. Then **smarti** starts the face and voice recognition if the person's face, voice and fingerprint are recognized the door is opened, the alarm is shut off, a photo of the person is taken and the time and date of entry are recorded.

When the person enters the room the door is locked behind him. To exit the room the person identifies himself using the fingerprint reader inside the server room **smarti** then unlocks the door, records when the person left the room and turns on the alarm.

If the person who wants to enter the server room is rejected **smarti** sounds an alarm in the company's security centre and opens a video intercom link to the **smarti** client in the security centre. The security guard can then check if it's a false alarm using the video intercom.



Since the fire alarm is also connected to the system the **smarti** unit can open the doors to the server room if a fire breaks out.

Below the line

With the use of the **smarti** the company fully met the above stated demands and an effective enforcement of security standards and recommendations was attained in the most reliable and economical way.

The use of the **smarti** system in combination with the fingerprint readers has proven it self to be very affective in achieving a higher security and reliability level with minimal additional costs.

The used solution prevented abuse; unauthorized and unsupervised access which is possible with more commonly used access solutions (ID cards, PIN codes...).

Summary

The advantages

- Multimodal biometrics, unlimited connectivity and numerous additional functions in one device.
- Simplifies, speeds up and automates authentication and identification of authorized individuals.
- Biometric identification is unobtrusive and reliable.
- Identity authentication based on previously acquired biometric patterns.
- Offers highly reliable identification - biometric patterns can not be lost, stolen, fraudulently acquired, damaged, misappropriated or lent to someone like per example ID cards, PIN codes, passwords etc.
- Provides a consistent and effective enforcement of security and privacy policy.
- Offers a realistic and correct evaluation of presence & attendance and labour costs.

The cost of ownership

smarti is designed:

- to reduce the cost of investment because it costs less than other widely used solutions which use ID cards...
- to reduce implementation costs with the completeness of the solution, which adapts to many different physical-access environments and needs.
- to easily integrate with existing access-management systems.
- for ease of use and maintenance during its life time.

The financial advantages

Security can impact your budget therefore you should consider the upfront costs and ongoing expense of managing a security solution. **smarti** the complete multimodal biometric access control solutions can:

- reduce security cost with automated, unmanned entry points.
- extend your budget to improve employee and constituent confidence in your security measures.
- reduce cost of data protection by verifying authorized users in secure areas.