



**smart<sup>i</sup>**

Security. Control. Comfort.

access control  
time & attendance  
building management

based on multimodal biometrics using facial and voice recognition

Samples of use:

Facial recognition  
in a bank

### 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 behavioral 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 then averagely accurate biometric identification system.

Besides the above mentioned characteristics such a system is expected to be easy to integrate, 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**<sup>®</sup> unit or on a certified server.

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

## Samples of use: Facial recognition in a bank

---

**smarti** is a complete access control and time & attendance solution with numerous additional features: video intercom, video phone, video messaging, 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 STUDY

#### The Situation

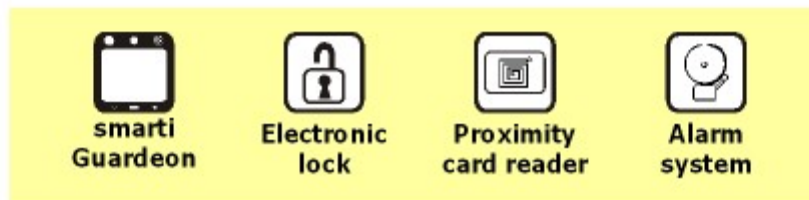
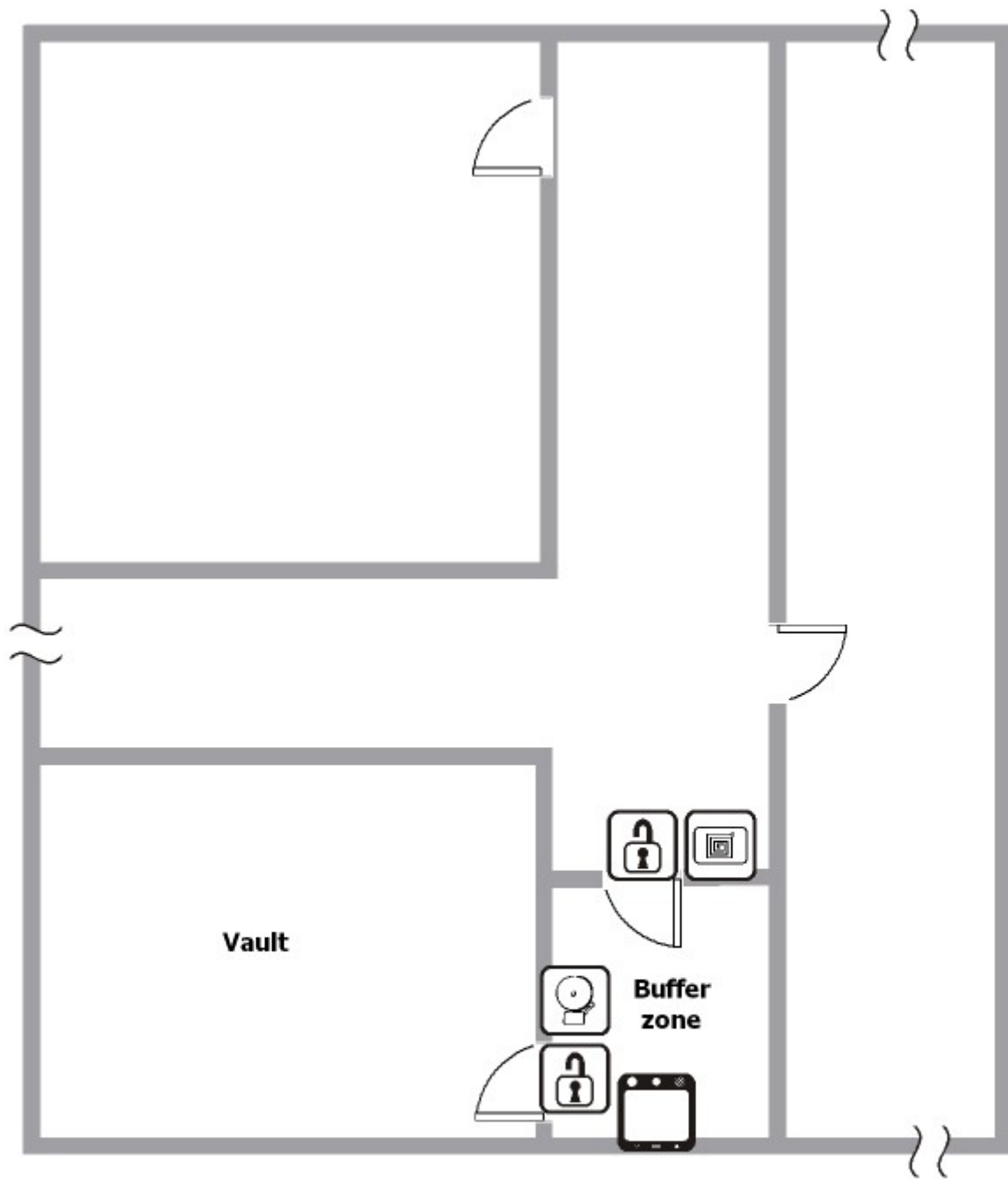
A short while ago, a bank wanted to equip a vault in one of their branches with a biometric system which would control access and ensure entry of only one person at a time. We employed a small buffer space between two safety doors controlled by **smarti** Gardeon to accomplish this. Of course there are quite a few sensors connected to the **smarti** system which guarantees that the two doors can never be opened at the same time.

#### The Solution

As already stated above we employed a small buffer space between two safety doors one leading to the vault and one to the corridor. Both doors are equipped with sensors which detect if the door is open or closed. The sensors are linked to an independent alarm system and to the **smarti** system. The two safety doors cannot be open at the same time.

In the buffer zone we mounted the **smarti** Gardeon unit which has a built-in proximity card reader; this unit controls the vault doors. The buffer zone is also equipped with video surveillance cameras.

The safety door between the corridor and the buffer zone is controlled by a proximity card reader. After a valid proximity card is presented the card holder can enter the buffer zone. After the first safety door is closed the card holder wishing to enter the vault can use the **smarti** Gardeon unit to open the safety door to the vault. The card holder will be identified first by a PIN code, then he will present his proximity card and then by facial recognition (1:1 identification). If the person is identified successfully and the door to the corridor is closed **smarti** will unlock the vault door. If the door to the corridor is not closed a warning is given and if in the second attempt the corridor door is still not closed an alarm is sounded.



### **Below the line**

With the use of the **smart**i system the bank 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 facial recognition in combination with PIN codes and proximity cards has proven itself to be very effective 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.