

Industry: Banking

Client: Volksbank

Application: Biometric access control

Solution: smarti[®] Guardeon a complete solution for access control based on facial recognition

Case Study

Volksbank installs smarti[®] facial recognition for access control to their vault



The Customer

Volksbank has been operating successfully on the Slovenian market since 1993, when the Volksbank AG (VBAG) took over the Styrian crafts and business bank (founded in 1991).



The present Österreichische Volksbanken-AG was established in 1922 as the central institution of the Austrian Volksbanks in order to support them in fulfilling their service

mandate. Its primary role was to offset fluctuations in liquidity among the Volksbanks, which had been established as early as 1850 as commercial cooperative credit associations.

Back in the year 1991, Volksbank AG (VBAG) became one of the first banks to initiate an expansion drive in the promising Central and Eastern European growth markets, setting up a subsidiary bank in Slovakia.

Today, Vienna-based Volksbank International AG (VBI), of which a majority shareholding is owned by VBAG, manages a successful and expanding Bank Network consisting of 582 sales outlets in 9 Central and Eastern European countries: Slovakia, Czech Republic, Hungary, Slovenia, Croatia, Romania, Bosnia-Herzegovina (VB BH, VB Banja Luka), Serbia and, since January 2007, the Ukraine.

VBI's banking activities focus on small and medium-sized businesses as well as retail banking customers, project financing and referral business. Standardized products and processes ensure a unified quality of service in the Central and Eastern European markets.

The Solution

To meet Volksbank's challenging requirements of an integrated biometric access control system for a vault in two of their branches with which they 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 a **smarti**[®] Guardeon unit 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.



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**[®] Guardeon 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**[®] Guardeon 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.

With the use of the **smarti**[®] 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, fingerprint readers and proximity cards has proven itself to be very effective in achieving a higher security and reliability level with minimal additional costs.



Kranjska 14, 4202 Naklo
Slovenia - Europe
Tel: +386 4 598 10 00
Fax: +386 4 598 10 10

smarti@tab-systems.com
www.tab-systems.com

The used solution prevents abuse; unauthorized and unsupervised access which is possible with more commonly used access solutions.