smarti®
Security. Control. Comfort.

TAB Systems
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

Industry: Banking
Client: HSBC
Application: Biometric access control
Solution: smarti® Diadem a complete solution for access control based on facial recognition

Case Study

HSBC bank upgrades access control to their card printing room with facial recognition

The Customer

HSBC
The world's local bank

Headquartered in London, HSBC is one of the largest banking and financial services organizations in the world. HSBC's international network comprises around 7,500 offices in 87 countries and territories in Europe, the Asia-Pacific region, the Americas, the Middle East and Africa.

With listings on the London, Hong Kong, New York, Paris and Bermuda stock exchanges, shares in HSBC Holdings plc are held by over 221,000 shareholders in 127 countries and territories. The shares are traded on the New York Stock Exchange in the form of American Depositary Receipts.

HSBC provides a comprehensive range of financial services to around 95 million customers through four customer groups and global businesses: Personal Financial Services (including consumer finance); Commercial Banking; Global Banking and Markets; and Global Private Banking

The Solution

HSBC needed to upgrade their existing Wiegand access control system for entry to the Card printing and PIN creation rooms in one of their EU branches. The existing system was based on proximity cards. They wanted a system that could ensure entry to the rooms was granted only when two authorized employees were present at the same time. To meet HSBC's challenging requirement the **smarti®** DIADEM unit was chosen. The unit can be connected to Wiegand system and can

TAB Systems
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

be set up so that multiple users must be recognized in the correct order and in a limited amount of time before access is granted.

The card printing and PIN creation rooms are located one beside the other. Each room has its own door. Beside each door two card readers were mounted. The card readers were connected to a Wiegand access controller. To enter the card printing or PIN creation room two proximity cards had to be presented at the two readers beside the entry to the room. If the cards were valid the access controller opened the door to the room.

To upgrade the existing system with facial recognition we removed one reader from each door and mounted a **smarti**® Diadem unit between the two doors. We connected the Diadem unit to the existing access controller with our two-way Wiegand to RS232 converter. The Diadem unit can be administered from a desktop computer which is located in a secure control room through TCP/IP.

To enter the card printing or the PIN creation room two authorized employees have to be present and identified. The identification procedure is now as follows: first they present a proximity card on the appropriate card reader. The card data is sent to the access controller which sends it to the **smarti**® Diadem unit to initialize it. If the card is not authorized the Diadem unit is not initialized and cannot be used. When the Diadem unit is initialized the two employees have to identify them self's one after another in an allocated amount of time using facial recognition. If they are not both identified in the allotted time or if one is rejected the identification procedure fails and they will not be granted access and the security officer can be notified. If the identification procedure is successful **smarti**® Diadem sends a command to the access controller and the door to the right room is unlocked automatically.

With the use of the **smarti**® system we fully met the banks requirements 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 proximity cards has proven itself to be very affective in achieving a higher security and reliability level with minimal additional costs.

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