Banks belong to critical infrastructure and as such they are subject to special security regulations (KonTraG, Basel II, MaRisk). The financial sector is of crucial importance to the social system, so a banking crisis can always pose a risk of catastrophe for society as a whole.
In terms of security, banks are therefore obliged to implement a risk management system and to set up an early warning system.

Use of palm vein scanners in the banking sector

#biometrics #palmveins #accesscontrol

The challenge

Banks carry great responsibility for their customers and the economy. They need industry-specific security solutions to reduce potential risks to a minimum. Money and material assets must be reliably and sustainably protected, and as they often constitute a risk factor, they also require preventive security measures. Banks and financial institutions usually feature intense customer traffic. In self-service areas, where no staff is present, there are repeated attempts to manipulate cash machines. Banks are threatened by vandalism or unauthorised transactions at the cash machines due to the high level of customer traffic. Here, appropriate precautions must be taken to ensure the necessary security.

The demands on the security management of access control systems are very high. Such systems must guarantee permanent availability for the customer as well as optimal protection against criminal acts. In particular, sensitive customer data, safe and locker rooms and the back office areas require reliable protection against unauthorised access.
An intelligent access control system enables user-optimised administration of all access rights and accurate documentation of access events, which ensures maximum security.

There can also be spatial and temporal restrictions, which require the setting up of different time profiles for different groups of users. For example, bank employees are only granted access to authorised areas during business hours, whereas cleaning staff is granted access at other specified times. Thanks to modern access control systems, banks can optimise security and service for both employees and customers.

In the event of a robbery or loss of sensitive customer data, the reputation and economic situation of financial institutions are threatened, as customer data are the most sensitive data of a company and also the basis for contractual relationships, bonuses, calculation of interest, premiums and the development of customer-oriented products and services.

Legal requirements / guidelines

"Banks implement high-quality systems of protection against burglary (strongrooms, safes, cash machines). Protective measures against robberies are required by accident insurance companies (DGUV), as the lives and health of bank employees are also at risk in the event of a robbery. The DGUV regulation 25 (formerly BGV C9 / GUV-V C9 or UVV "Kassen") applies. ***Source: https://www.secupedia.info/wiki/Banken-Sicherheit#ix z6Q6sWOMad***

iCOGNIZE GmbH
Justus-von-Liebig-Straße 9
63128 Dietzenbach

+49 (0) 6074 310 3600

https://www.icognize.de
info@icognize.de

Access authorisation to areas, buildings, parts of buildings or individual rooms must be performed at least by the verification of the:
- system affiliation of the person/ means of identification
- time restrictions (time zones)
- local access restrictions (spatial zones)

Access can be granted only if these criteria are met, i.e. if a correct means of identification (ID card or objects with machine-readable information) for a specific period and a specific area are presented.

Source: ***https://www.secupedia.info/wiki/Zutrittskontrolle#ixz-z6Q6xYEa34***

Unauthorised intrusion into security areas such as cash registers, vaults and the back office must be prevented, similarly to intrusion into the IT system, in order to protect sensitive data. Moreover, access must be regulated by authorised persons, and it should be recorded who had access to the premises and when. Section 9 of the DGUV regulation of the work insurance institution states that doors must always be locked and equipped must be protected against break-in and equipped with security locks.

Data protection

The General Data Protection Regulation plays a fundamental role in the banking sector since banks have to process personal data in order to fulfil their legal obligations (Article 6, par 1c. GDPR) and more and more data needing protection are being generated in the course of digitisation. Banks must comply with the German Banking Act, the Money Laundering Act, the Securities Trading Act and various tax laws. This requires, among other things, credit checks, identity and age checks, fraud and money laundering prevention, compliance with tax monitoring and reporting obligations, and the assessment and management of risks in the bank. If access to these sensitive data is not protected against unauthorised persons at both the digital and physical level, high fines may be imposed. Here, the combination of ID cards and biometric features provides greater security and convenience.

Solutions by iCOGNIZE

Hygienic and contactless access control by means of a handheld

The ManuScan handheld vein scanner is installed in a standard flush-mounted box. The effort required for the installation is comparable to that of a standard light switch. The scanner is supplied via Ethernet (PoE). The readers are connected to a top-hat rail-capable Authentication Unit (AU), which is operated in a separately secured IT room in a 19" rack.

"In this way, we can secure sensitive doors with handheld vein scanners without having to replace the entire access control infrastructure." – *Dr Alexander W. Lenhardt, CEO iCOGNIZE GmbH*
Thanks to the unique biometric feature "palm veins", the system offers the user not only maximum security but also the highest level of comfort. The ManuScan indoor palm vein scanner works contactlessly and non-invasively and ensures intuitive use and high acceptance with its unique optical palm positioning system.

Advantages of the ManuScan Indoor palm vein scanner

- RGB-LED User guidance
- More secure than iris scanning
- FAR < 0.00008% (False Acceptance Rate)
- FRR < 0.01% (False Rejection Rate)
- Sabotage detection (contact, vibration)
- Easy integration into existing systems
- Integrated PIN code reader
- Certified according to CE, BSI (components)
- Contactless operation and therefore very hygienic
- Operation with hygienic gloves possible
- Protocols for proving compliance with hygiene regulations are available
- Contactless scanners can also be used with hygienic gloves and thus a high standard of hygiene can be maintained
- Maintenance only needs to be carried out once a year