ELATEC
RFID Systems

PHYSICAL ACCESS CONTROL (PAC)

Setting up the ideal physical access control (PAC) solution involves many decisions: selecting the appropriate access technology, determining the scope of applications that will be covered, and addressing user requirements and security concerns. Here are ten things to consider when designing a PAC system for your organization.

10 SYSTEM DESIGN CONSIDERATIONS

01

Scope and Applications

What locations, systems and applications will be included?

A universal access system could include some or all of the following:

- Locations: Exterior and interior doors, gates and turnstiles, elevators, parking, secure areas, etc.
- Physical assets: Cabinets and lockers, production machinery, vending machines, medical or laboratory devices, etc.
- IT infrastructure/digital assets: Computers, printers, login to business systems and applications.

02

Access Technology

Physical RFID badges or virtual credentials?

Modern access systems utilize Radio-Frequency Identification (RFID) or smartphone-based access credentials using Near-Field Communication (NFC) or Bluetooth® Low Energy (BLE)

- If an existing technology is in place for front door access, it can often be leveraged for "beyond the door" applications.
- Choose a system that works for the intended user base.
- It may be necessary to support multiple technologies to meet the needs of different user groups.

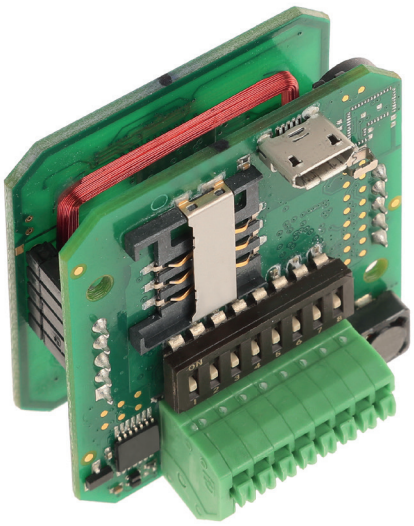
03

Transponder Technology

Which transponder technology will be used?

There are dozens of RFID transponder technologies (e.g., MIFARE, DESFire, Prox/HID Global, LEGIC) in use in addition to smartphone-based NFC or BLE credentials.

- Look at technologies already in use for related applications.
- HF RFID and NFC are more secure than LF RFID or BLE solutions.
- Multi-tenant buildings and large organizations may require universal readers to accommodate multiple transponder technologies.



04

User Groups and Access Levels

What level of access do different users/groups need, and at what times?

RFID readers can connect with a centralized access management system to:

- Set access levels for different user groups or individuals.
- Change or revoke access as needed.
- Track who has entered a location or used an asset.

05

Digital Security

Does the system meet modern cybersecurity standards?

PAC systems must adhere to high cybersecurity standards to protect places, people and physical assets.

- Use appropriate encryption standards (e.g., AES, 3DES, ECC) to protect data stored on the card and during communication between the card and reader.
- Consider multifactor authentication (MFA) for higher security applications (e.g., integrated keypad for PIN access, biometric authentication built into the smartphone).

For more information contact our Application Specialists at the locations below:

elatec.de

EMEA
Puchheim, Germany
+ 49 89 552 9961 0
sales-rfid@elatec.com

AMERICAS
Palm City, Florida, USA
+1 772 210 2263
americas-info@elatec.com

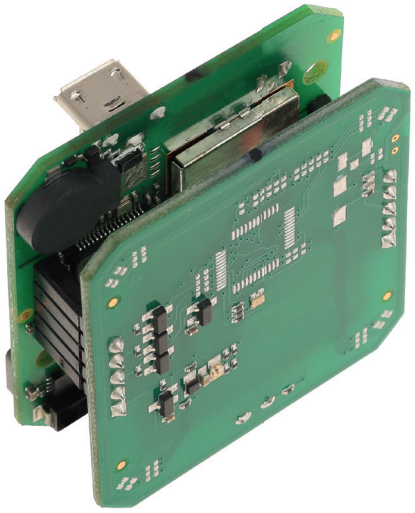
ASIA PACIFIC
Shenzhen, China
+86 755 2394 6014
apac-info@elatec.com

ELATEC
RFID Systems

UNIVERSAL READERS FOR PAC FROM ELATEC

ELATEC's TWN4 line of universal, multi-technology readers makes setting up the ideal PAC system easy.

- Support for 60+ RFID technologies plus NFC/BLE smartphone credentials
- Available in a range of form factors for various PAC applications
- Robust DevKit for fast configuration and customization
- Remote update capabilities
- Backed by ELATEC's unbeatable service and support



10 SYSTEM DESIGN CONSIDERATIONS

06 **Physical Security**

How is the reader secured against tampering?

It is important to secure the reader itself to prevent tampering or disabling.

- Readers used externally should be securely mounted and in a tamper-proof housing.
- Outdoor readers should be weather-resistant.

07 **System Integration and Interoperability**

Is the PAC system compatible with current infrastructure?

Consider how the PAC system will integrate with IT networks, video surveillance, alarm systems and building management systems.

- Use industry standards and protocols (e.g., OSDP, Wiegand) to facilitate seamless integration and interoperability between different systems.
- Look for APIs and software development kits to enable custom integrations and extensions.

08 **Reader Functionality and Customization**

Does the reader support the functionality you need?

Look for a reader with the appropriate physical functionality and a robust software development kit for customization. Consider functions such as:

- Custom encryption
- User feedback (e. g., lights, sounds or displays)
- Third-party integration

09 **Updates and Future-Proofing**

How easy will it be to update the system to meet future requirements?

Consider how the PAC system will handle updates and future advancements.

- Updates will need to be made periodically to address emerging security threats, add new transponder technologies or modify functionality.
- Remote update capabilities make this process much faster and easier.

10 **Service and Support**

Will you have support through the installation and beyond?

Effective implementation and maintenance of a PAC system require robust support services from the provider. Look for:

- Access to a dedicated technical support team, detailed installation guides, and help with system integration.
- Regular firmware and software updates to address security vulnerabilities and add new features.
- Training programs for installers and integrators.
- A robust warranty and technical support program.

For more information contact our Application Specialists at the locations below:

elatec.de

EMEA
Puchheim, Germany
+ 49 89 552 9961 0
sales-rfid@elatec.com

AMERICAS
Palm City, Florida, USA
+1 772 210 2263
americas-info@elatec.com

ASIA PACIFIC
Shenzhen, China
+86 755 2394 6014
apac-info@elatec.com