

Evaluating your access control credentials

Why organizations must balance cost and convenience with security.



Advantages at a glance:

- **Advanced encryption security** Uses AES-128 encryption with mutual authentication and dynamic, secure communication. This eliminates the vulnerabilities of unencrypted 125 kHz proximity cards, which can be easily cloned, and makes duplication or interception extremely difficult.
- **Multi-application capability** Supports multiple secure applications on a single credential, enabling use cases like access control, cashless payments, parking, and time tracking.
- **Future-proof technology** Aligns with modern security protocols and is compatible with mobile credentials and NFC-enabled devices.
- **Faster transaction speeds** Improved processing and communication speeds.
- **Enhanced Privacy Protection** Supports randomized identifiers helping protect user identity and prevent tracking.
- **Scalability for high-security environments** Trusted access solutions from dormakaba is ideal for enterprises, healthcare, education, and government facilities requiring robust, scalable security.

Three common options offer very different levels of protection and functionality

- Good -> 125 kHz proximity cards
- Better -> 13.56 MHz iCLASS
- Best -> DESFire EV Series

Upgrading from 125 kHz proximity credentials to a stronger platform delivers a major leap in security, flexibility, and long-term value. Security has evolved — your readers and credentials should too. Here's why:

125 kHz proximity credentials often referred to as "Prox" are the most basic and widely deployed. They operate using unencrypted radio frequency technology. Essentially they transmit a fixed card number to a reader.

While affordable and easy to deploy, they are highly vulnerable to cloning and unauthorized duplication. Tools to copy these cards are inexpensive and readily available, making them less suitable for environments requiring strong security. These credentials are often found in low-risk applications or legacy systems due for upgrade.

13.56 MHz credentials represent a significant step up in capability. These credentials include iCLASS and MIFARE classic and MiFare Plus cards support encrypted communication between the card and reader. They also offer higher memory capacity, enabling multiple applications such as access control, time and attendance, or cashless payments.

However, older variants have known vulnerabilities if not configured with enhanced security features, meaning organizations should ensure proper implementation or consider newer alternatives.

DESFire EV series (EV1, EV2 or EV3) credentials are considered among the most secure options available today. These credentials use advanced AES encryption and mutual authentication, protecting against cloning, eavesdropping, and data manipulation. The EV series also supports secure key management and multiple applications, making it ideal for high-security environments such as corporate campuses, healthcare facilities, and government buildings. Additionally, these credentials are well-suited for mobile access and future-proof system designs.

In summary, while 125 kHz credentials offer low cost and simplicity, they pose significant security risks. The more suitable options provides improved security and flexibility, while DESFire EV series delivers best-in-class protection and scalability for modern access control systems.

Overall, moving to higher security platforms like DESFire EV series transforms access control from a vulnerable, legacy system into a secure, flexible, and future-ready platform – often utilizing the same infrastructure.

Credential types:

- **ISO Cards:** Standard credit-card-sized plastic credentials, often printable for use as employee IDs.
- **Key Fobs:** Small, durable tags that can be attached to keyrings for convenient, frequent entry.
- **Adhesive Tags/Discs:** Small stickers that can be attached to the back of a phone or other personal items to turn them into a credential.
- **Mobile Credentials:** Utilizes NFC or Bluetooth on smartphones (via Apple Wallet, Google Pay, or dedicated apps) to replace physical cards.
- **Wristbands:** Often made of silicone, these are used in environments like gyms or water parks where carrying a card is impractical.