dormakaba

Security is not optional:
Why high-security credentials are critical to protecting your people, data, and facilities

Access control credentials have evolved significantly over time, offering increasing levels of security, functionality, and flexibility. When comparing 125 kHz credentials, 13.56 MHz credentials, and DESFire EV2 credentials, the differences clearly illustrate a "good, better, best" progression—culminating in why high-security DESFire technology is the preferred choice for modern access control.

Summary:

- **125 kHz:** Simple but insecure and outdated
- **13.56 MHz:** More capable, but security depends on implementation
- **DESFire EV2:** highest security but with flexibility and future-ready performance for modern access control systems

125 kHz Credentials – Good

125 kHz proximity credentials have long been the industry standard due to their simplicity and affordability. They provide basic access control functionality and are easy to deploy across a wide range of facilities. However, these credentials transmit data in an unencrypted format, making them highly vulnerable to cloning and duplication. Low-cost tools and widely available knowledge make it easy for unauthorized individuals to copy cards, posing a significant security risk. While suitable for low-risk environments, 125 kHz credentials no longer meet the demands of today's security-conscious organizations.

13.56 MHz Credentials – Better

13.56 MHz smart credentials represent a step forward in both capability and security. These credentials support higher data transfer rates and can store more information, enabling multi-application use such as access control, time and attendance, and cashless payments. Some 13.56 MHz technologies offer basic encryption and mutual authentication, improving protection compared to 125 kHz cards. However, not all implementations are created equal—many legacy or lower-end 13.56 MHz credentials still rely on outdated or proprietary security methods that can be compromised. While they provide improved versatility and moderate security, they may not be sufficient for high-risk or compliance-driven environments.

DESFire EV2 Credentials – Best

DESFire EV2 credentials set the benchmark for high-security access control. Built on advanced 13.56 MHz technology, they utilize AES-128 encryption, mutual authentication, and secure messaging to protect every transaction. Each credential can support multiple secure applications, segmented file structures, and dynamic data exchange, making them ideal for complex, multi-use environments. Unlike lower-frequency or legacy smart cards, DESFire EV2 credentials are specifically designed to resist cloning, eavesdropping, and data manipulation.

In addition to superior security, DESFire EV2 credentials offer scalability and future-proofing. They integrate seamlessly with modern systems, support mobile credentials, and enable secure key management practices. This ensures organizations can adapt to evolving threats without needing to replace their entire infrastructure.

Factsheet

	125 kHz "Proximity" credentials ("Good")	13.56 MHz "Smartcard" credentials ("Better")	DESFire EV2 "High-Security Smartcard" credentials ("Best")
Frequency:	125 kHz (low frequency)	Frequency: 13.56 MHz (high frequency)	13.56 MHz (high frequency)
Encryption:	None (unencrypted, fixed ID transmission)	Varies (from none to basic/proprietary encryption depending on card type)	Advanced (AES-128, 3DES, DES support)
Authentication:	None	Limited or optional (depends on technology, e.g., iCLASS, MIFARE variants)	Mutual authentication with secure messaging
Cloning risk:	Very high – easily duplicated with inexpensive tools	Moderate – secure versions exist, but many legacy formats are still vulnerable	Extremely low – designed to resist cloning, sniffing, and replay attacks
Read range:	Typically 2–10 inches (5–25 cm)	Typically 1–4 inches (2–10 cm)	Typically 1–4 inches (2–10 cm)
Data capacity:	Very limited (card number only)	Higher (supports multiple applications and data storage)	High (segmented memory, multiple secure applications)
Communication:	One-way (card to reader)	Two-way (card and reader exchange data)	Fully secure two-way communication with encrypted data exchange
Use case:	Legacy systems, low-security environments	Multi-application environments (access, payments, ID badges)	High-security facilities, enterprise systems, government, healthcare, and campuses
	HID 1326 HID 1386 PROXKEYIII HID 1391 CS-125-36	HID iCLASS iCLASS SE HID Seos K-SECURE	C-CSC-2 K-CSM-2P K-CSK-2 K-DE2-125 (dual migration) K-TX2-EV2 (transmitter)

Conclusion:

While 125 kHz and standard 13.56 MHz credentials may meet basic needs, they fall short in protecting against today's sophisticated security threats.

DESFire EV2 credentials provide the highest level of protection, flexibility, and long-term value—making them the clear choice for organizations that prioritize security, trust, and resilience.

EAD_1817_FS_EN CEI 0426

Any questions? We would be happy to advise you.
Contact us at: 1 888 539 7226

dormakaba USA Inc. | 6161 E. 75th St. Indianapolis, IN 46250 | dormakaba.us