The Evolution of Credential Technology in Physical Access Control

For decades, physical access control has been critical to security strategies. While these systems have evolved to offer more security and convenience than ever before, many organizations still use outdated, vulnerable access control systems. For these organizations, the time has come to prioritize upgrade plans.

Access Control Systems: A Brief History

To fully appreciate today's capabilities, it is important to understand the history of access control.

1980s – Swipe Technologies: Swipe technologies were an administrative improvement over manual locks and keys. Primary technologies included Magnetic Stripe Cards and Wiegand Swipe Cards, which required users to physically swipe or insert a card through a reader. Because the credential is unencrypted, these technologies are highly vulnerable.

1990s – "Prox": Featuring 125 kHz low frequency technology, Prox introduced a contactless experience to access control. This widely deployed technology also allowed the use of fobs and other form factors beyond the ID-1 card standard.

Despite this convenience, Prox has major security vulnerabilities. For example, Prox credentials are unencrypted, static, and can be read in the clear, making them easy to clone or forge. Prox credentials also cannot be encoded with multiple IDs or other data attributes.

Late '90s-2010s – First-Generation Contactless Smart Cards: More sophisticated high frequency technology (13.56 MHz) then emerged to address the limitations of Prox. First, the reader and credential could mutually authenticate, increasing data privacy and security. Second, cards could store information beyond an ID number, enabling more advanced multi-application use cases. As time passed, however, hackers exposed vulnerabilities in the mutual authentication algorithms, triggering the development of more secure credential technologies.

Today – Next-Generation Smart Cards and Mobile Devices: Today's credential technology leverages cryptographic standards approved by a broad research community. These standards deliver superior data integrity and enhanced privacy protection to create a highly secure environment.

Modern credential technology offers new levels of mobility, including the use of mobile devices as a form factor, as well as enabling applications beyond physical access control.

Seos® – The Next Generation of Credential Technology from HID Global

Seos provides the ideal mix of security and flexibility for any organization. Thanks to highly advanced encryption and a software-based infrastructure, Seos secures trusted identities on any form factor and can be extended for applications beyond physical access control.

Seos supersedes legacy and existing credential technologies by providing:

- **Security:** Best-in-class cryptography offers unrivaled data and privacy protection, resulting in a more secure environment than other credential technologies.
- **Mobility:** Seos is software-based and independent of the underlying hardware chip, offering new levels of form factor flexibility, including use on mobile devices, smart cards, tags, and more.
- **Applications:** Seos can be extended for use on applications beyond physical access control, including use cases tailored for enterprise, education, government, hospitality, and more.

These advanced capabilities provide more security protections to organizations while giving them the flexibility to choose the right mix of form factors and applications to meet their unique needs. ●