Seos® Credential Technology

Overview

Seos is a breakthrough credential technology that powers secure identity solutions. Seos gives the freedom to use the device of choice for secure access to more applications with the confidence that identities are secure and privacy-protected. Credentials powered by Seos® can be delivered in:

Smart Cards **Tags** **Key Fobs** **Smart Phones** **Tablets** **Wearables**

Why Choose Seos?

More confidence

- Best-in-class security and privacy
- Proven, standard cryptography
- Evolving to meet end-user needs today and in future

More choices

- Hardware independent, allowing identification from smart cards, smartphones, tablets, wearables and beyond
- Not tied to a specific communication standard, enabling use of ISO14443 RFID communication, NFC, Bluetooth and more
- Can be loaded to a wide variety of smart devices, supporting both the popular iOS and Android operating systems
- Can be read by HID Global's iCLASS SE® readers or a growing number of devices (printers, time & attendance terminals, etc…) from 3rd party manufacturers

More applications

- Seos credential technology drives access across the enterprise, university, hospital, home or hotel
- Securely access data in the cloud using the built-in One Time Password (OTP) feature

> *"I think Seos® goes beyond just door access; it allows us to manage the credentials better and put the destiny of the department back into their own hands."*
>
> **Danny Anthes**
> Senior Manager of Information Technology,
> George Mason University

Security & Privacy

- ✓ Multi-layer security model
- ✓ Seos applet is loaded to a tamper proof secu microcontroller with full memory encryption, security sensors and secure booting
- ✓ Seos uses open standard encryption algorith like 3DES, AES, SHA-256 and secure authentication
- ✓ Custom data are encrypted, digitally signed stored in a Secure Identity Object (SIO) insi the Seos vault to ensure privacy

Technology Comparison: Seos® vs MIFARE® DESFire EV1

	Seos Technology	MIFARE DESFire EV1
Hardware platform	Seos is platform independent, implemented in software. It is adaptable and can be run on numerous devices - smart cards, smart phones, tablets, wearables, etc…	DESFire EV1 relies on a specific chipset and is limited to delivery on smart cards or fobs. No gateway to mobile.
EEPROM data memory	Flexible, up to 32kB, depending on the chip. 32kB used for smart device applications, cards delivered with 8kB or 16kB EEPROM	8kB maximum, cards delivered with 256B, 2kB, 4kB, and 8kB EEPROM
Applications	Manages unlimited number of applications and unlimited files with object oriented data structure. Seos cards come with access control identity and One-time-password (OTP) feature as standard.	Maximum 28 applications and 32 files per application. No application is prepared and ready to be used from the manufacturer.
Standards	Based on open, global standards. The iCLASS® Seos card supports ISO14443A and ISO7816-4. Crypto algorithm used is 3DES and AES128. Seos is also ready to support future algorithms.	DESFire EV1 supports ISO14443A and ISO7816-4 but it still uses lot of proprietary commands. Crypto algorithm used is primary 3DES and AES128. The credential is Common Criteria EAL4+ security certified.
Data access	Seos credentials always communicate sensitive identity data in highly secure manner.	DESFire EV1 cards can potentially be very insecure if deployed with “UID reading only” or if security is implemented incorrectly.
Privacy	Random card serial number (UID) is used by default assuring privacy protection.	The default serial numbers (UID) are not random and can contribute to compromise of privacy. Credential security and privacy is *highly* dependent upon the system integrator.
Read range	Seos technology is independent of underlying communication protocol – it is communication agnostic. Read range can vary based on application from centimeters (when ISO14443 standard is applied) to meters for long-range Bluetooth Smart communications.	Typical read range is 2-6 centimeters.
Future proof	Because Seos credential technology is software-based, it can be upgraded to combat new security threats as they arise. This dynamic credential technology also offers backward compatibility, for legacy HID Global access control formats.	Because DESFire EV1 is a chip-based and relies on a specific chipset, it lacks flexibility once deployed. The more static nature of the system may require full replacement in the event of emerging security threats.
Identity management	Full identity management (access control data encoding and key management) IS INCLUDED in the price of the credential. Secure, controlled credential manufacturing, with documented chain of custody, ensures trust in HID Global’s supply chain management.	Full identity management (access control data encoding and key management) IS NOT INCLUDED in the base price of a credential. Privacy protection, encoding and key management along with the entire security assurance process is wholly dependent on the system integrator.
Credential provisioning	Credentials can be programmed at point of manufacture (without surcharge) or using in-field programmers. Over-the-air provisioning and management of secure identities including change of artwork is available for mobile applications powered by Seos.	Identity data is typically provisioned by system integrators using in-field programmers only.
Supplier	Seos technology is a registered trademark of ASSA ABLOY. Products powered by Seos are manufactured by HID Global, Yale, VingCard, and other ASSA ABLOY companies as well as by a number of HID Global’s OEM partners. Products are supplied by HID Global partners worldwide.	The MIFARE DESFire EV1 chipset is a trademark of NXP and it is manufactured by NXP. Products are manufactured and supplied by NXP partners.