Seos® Credential Technology from HID Global

HID®


seos

The Next Generation of Credential Technology

Security threats have evolved over the years, with technology maturing along the way to counter growing threats. When it comes to physical security, however, most organizations continue to use legacy access control technologies that leave them open to unnecessary vulnerabilities. Not only do organizations need to quickly close security gaps, they must also find modern technology solutions that provide the flexibility and scalability to meet the demands of today's dynamic world.

This is why HID Global created Seos, the next generation of credential technology.

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 these key benefits:

- **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, providing 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.

seos

Seos provides the ideal mix of security and flexibility for any organization.

Unrivaled Data and Privacy Protection

Seos offers best-in-class security, providing higher levels of data and privacy protection than legacy and competing credential technologies. This is because Seos takes a layered security approach and uses stringent best practices for data protection, including well-researched open standards.

Layered Security and Secure Identity Object

Seos and its corresponding platform of iCLASS SE and multiCLASS SE readers leverage a layered security approach, meaning the technology combines multiple mitigating security controls to protect resources and data.

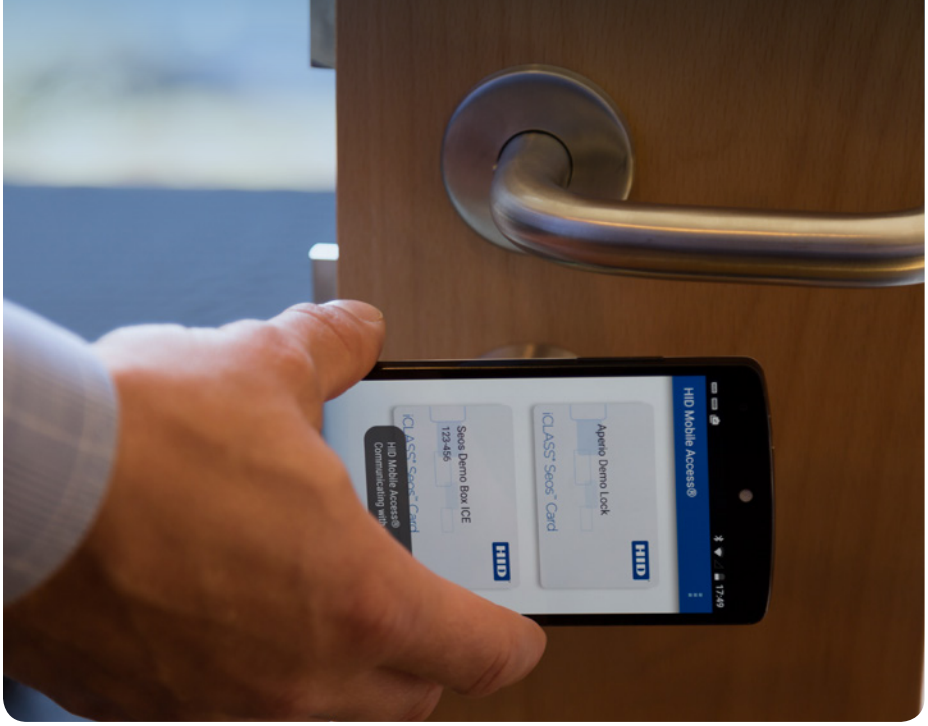
One of these security layers comes from the Secure Identity Object, or SIO, which is a cryptographically protected data model for the storage of secure identity data, such as a user ID.

The SIO is designed using industry standards to increase the level of security, regardless of the security level of the underlying device. Even more, the SIO is a portable ID that can be programmed on a number of physical credentials and can be leveraged by third-party applications and products.

The SIO used with Seos is unique as it contains four defining characteristics that provide enhanced security protections:

- The SIO contains unique digital identity information for the user
- The SIO is cryptographically bound to the device
- The SIO is signed at the time of creation and this signature is validated each time the credential is used, which ensures the SIO comes from a trusted source
- The SIO is encrypted, preventing an unauthorized party from reading the User ID embedded in the SIO

These capabilities provide the foundation for a more sophisticated security environment as compared to legacy or competing technologies.



The Seos Core

In addition to the inherent security provided by the SIO, Seos credential technology is centered on the Seos Core. The Seos Core is a secure vault that provides a consistent model for storing and using digital credentials and is agnostic of the underlying form factor, hardware (smart card, mobile device, wearable, etc.,) and communication protocol.

The Seos Core consists of a secure vault that can be thought of as being compartmentalized into multiple containers. Each container is referred to as an Application Dedicated File (ADF) that has a unique Object Identifier (OID) and is used to store a digital credential.

Each ADF is privacy protected, which highlights how the Seos Core respects the principles of privacy: it does not reveal any unique identifier that would enable the carrier of a Seos credential to be tracked by an unauthorized party. It also does not reveal any information on the types of digital credentials stored on the Seos Core to an unauthorized reader.

The Seos Core is a secure vault that provides a consistent model for storing and using digital credentials and is agnostic of the underlying form factor, hardware, and communication protocol.

Best Practices in Data and Privacy Protection

Seos truly differentiates itself from other credential technologies thanks to its strict adherence to best practices for data protection and widely reviewed open standards. These highly detailed best practices include key management, mutual authentication, secure messaging, and a standards-based design model.

Key Management: Seos uses a key management model to calculate card-specific keys bound to application and role. Seos' key management model differs from other technologies that use a more simplistic method, which do not bind the card-specific key to anything but the card serial number.

Mutual Authentication: Seos uses standard-based mutual authentication schemes that provide best-in-class message integrity protection – the same standards as electronic passports. The purpose of the mutual authentication is not only to validate the authenticity of the card and reader to each other, but also to establish the seed for the session keys to be later used in secure messaging. This approach protects the integrity and confidentiality of the full Seos transaction.

Secure Messaging: Seos uses a secure messaging mechanism that protects the integrity of the session as a whole – the same as secure signature creation devices, EMV cards (Europay, MasterCard, Visa), and electronic passports. This secure messaging mechanism protects both commands and responses, regardless of their length. It also protects the integrity of the session as a whole, so that any message deletion, insertion, replay, or re-ordering is detected and rejected. This approach differs from competing technology, which introduces vulnerabilities by allowing a message to be replayed or reordered.

Standards-Based: Seos uses open standards that are reviewed, checked, and verified by authorities to offer the most transparent level of security possible. Standards-based security means proven security: these standards are regularly checked and verified by authorities, in contrast to proprietary systems which usually do not evolve unless the solution is compromised. With Seos, these standards cover contactless communication, authentication, and cryptography on both smart cards and mobile devices. For maximum interoperability, Seos has been developed on well-proven open global standards or reference specifications.

In addition to these stringent best practices, Seos offers extra privacy enhancements to boost security. For example, the Seos Core does not reveal any static unique identifier to an unauthorized application, nor does it reveal to an unauthorized application whether an ADF even exists.

This strict adherence to the highest standards of data and privacy protection helps Seos better protect organizations from today's threats and vulnerabilities more than any other solution in the market.

With Seos, these standards cover contactless communication, authentication, and cryptography on both smart cards and mobile devices.

Software-based to Provide Form Factor Flexibility

Seos is a software-based credential technology, meaning it is not tied to the underlying hardware chip. This independence creates a wealth of opportunities to extend this secure credential technology to a much wider variety of form factors and communication protocols, all so organizations can select the right mix for their unique needs.

Freedom of form factor

Modern credentials require an independence from the underlying hardware chip so that phones, cards, wearables, and other form factors can be used interchangeably as authentic, trusted credentials. Unlike competing technologies built by chip manufacturers, Seos is completely independent of the chip because the Seos Core is software that is written to be platform agnostic. This implementation means that Seos can be ported onto different microprocessor devices. It is this portability that enables a Seos credential to be delivered in multiple form factors.

This flexibility provides organizations the freedom to choose the right mix of form factors to meet their unique needs. For example, security teams can issue a mix of smart cards and mobile devices to meet employee preferences. To use a mobile device as a trusted credential, Seos powers the award-winning HID Mobile Access solution.

With HID Mobile Access®, employees can use their smartphone, tablet, or wearable to access doors, gates, networks, and more. This new option for access control greatly improves user convenience and operational efficiency, as well as boosts security. HID Mobile Access apps are easily downloaded on Google Play and Apple's App Store, and offers a modern, professional option for employees who prefer to use their mobile device as a replacement or supplement to traditional smart cards.

Wide range of supported devices

HID Mobile Access supports hundreds of the most popular mobile devices available today and is consistently updated to support a growing number of mobile device options across the globe. This capability enables organizations to allow their employees to use their mobile devices for access control, whether it is a personal device or company-issued.

A full list of compatible devices can be seen at hidglobal.com/mobile-access-supported-devices.

Choice of communication protocols

In addition to choosing the right mix of form factors, Seos provides organizations the flexibility to select their preferred communication protocol. This is possible because the media-independent nature of the Seos Core implementation enables it to reside on a wide variety of mobile devices and present a consistent interface to the access control reader, regardless of whether it is communicating over Bluetooth, NFC, or other future protocols.

Because Seos is software-based and not tied to the underlying hardware chip, it is truly form factor agnostic, presenting a new wave of flexibility and scalability for all types of organizations. Not only does Seos provide more flexibility, it also increases security in that software patches can be deployed over the air if needed, as opposed to having to fully reissue chip-based credentials as may be required with competing technologies.

More Applications for More Use Cases

Another distinct pillar of Seos' capabilities includes its capacity to power applications beyond traditional physical access control.

Another distinct pillar of Seos' capabilities includes its capacity to power applications beyond traditional physical access control. These applications can span a wide array of use cases for various industries, including Enterprise, Education, Government, Hospitality, Finance, Healthcare, and more. Not only does Seos enable the possibility of more applications, its engineering allows for more secure applications thanks to its framework and secure, dynamic ADFs.

Secure Framework

Organizations need to be able to manage the digital credentials used for different applications independently, including the ability to set up different domains of trust. For example, it is not acceptable for the parking access system to be able to read a user's Windows password from the same card. A true multi-application card can store multiple digital credentials and apply a segregated access control policy that ensures that only authorized systems are able to read those credentials.

Existing RFID solutions are capable of storing multiple digital credentials for use across multiple applications, but Seos goes further, providing a comprehensive framework that protects access to those digital credentials using cryptographically strong authentication.

Secure, Dynamic ADFs

With Seos, digital credentials are stored in Application Dedicated Files, or ADFs. Each ADF is protected through a state-of-the art selection and authentication process, which uses the highest security and privacy levels with multiple keys. These include Privacy, MAC, and Authentication keys.

Furthermore, the structure of ADFs within the Seos Core is not fixed. New ADFs can be created and old ADFs can be destroyed dynamically by any system with the requisite permissions. This is conceptually similar to the way that file folders can be dynamically created or destroyed on a PC operating system. This enables the ability to optimize use of the available memory over the lifetime of a credential.

Various Memory Options

Seos credentials come with a range of memory options, including 8KB and 16KB, which allows sufficient memory for storing multiple applications. For Java Card-based platforms, Seos can be loaded in the secure memory area. On those platforms, available memory is up to 144KB to support custom application development. The Seos application can reside side by side with other applications in the chip.

One Time Passwords

In addition to being able to store static passwords, Seos is also capable of generating One Time Passwords (based on the Oath HOTP standard) to provide a credible alternative to one time password tokens for secure remote access to computer networks and applications.

Seos allows organizations to take their physical access control to the next level and beyond thanks to these secure and flexible multi-application capabilities. From secure print to time and attendance, cashless vending, and more, Seos enables a clear path to creating a more converged, higher value credential.

In addition to being able to store static passwords, Seos is also capable of generating One Time Passwords (based on the Oath HOTP standard).

The Next Generation of Credential Technology

Decades-old credential technology is no longer enough to meet the needs of today's organizations and their future growth. Not only should a credential technology ensure that physical access control is not the weakest link in the security chain, it should also provide a new level of user convenience to everyday employees and administrators.

With its best-in-class security, form factor flexibility, and capabilities for cutting-edge applications, Seos is the right choice in credential technology for today, tomorrow, and beyond.

To begin your upgrade to Seos, contact our experts at HID Global. We have helped thousands of organizations around the world seamlessly introduce Seos to their teams.

Contact us at **sales@integratedid.com** to schedule your consultation today.

Contact sales@integratedid.com to schedule your consultation today.

seos

North America: +1 512 776 9000 • Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 • Latin America: +52 55 5081 1650

2018-02-20-hid-pacs-seos-br-en PLT-03689

An ASSA ABLOY Group brand

ASSA ABLOY

INTEGRATED SYSTEMS, INC.®

1150-E Crews Road
Matthews, NC 28105

(800) 729-3722
info@integratedid.com
integratedid.com

ADVANTAGE HID Platinum Partner