Secure, Flexible and Scalable

HID®

The Next Generation of Credential Technology

Security threats have evolved over the years, with technology maturing along the way to counter growing risks. When it comes to physical security, however, most organizations continue to use legacy access control technologies that leave them open to unnecessary vulnerabilities. Organizations must also find modern technology solutions that 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 better protects organizations from today's threats and vulnerabilities more than any other solution in the market today.

Unrivaled Security

Seos offers 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.

Secure Identity Object

Seos and the HID Signo™, iCLASS SE® and multiCLASS® SE reader platforms 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 a portable ID that can be programmed on a number of physical credentials and can be leveraged by third-party applications and products. The Seos SIO is unique, as it contains four defining characteristics that provide enhanced security protections:

- Assigned unique digital identity information for the user
- Bound to the device cryptographically
- Signed at the time of creation and validated each time the credential is used, ensuring a trusted source
- Encrypted to prevent an unauthorized party from reading the embedded User ID

Credential Storing Model: The Seos Core

Seos credential technology is centered on the Seos Core, 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.

The Seos Core utilizes containers, referred to as Application Dedicated Files (ADF). Within each ADF is a unique Object Identifier (OID) that stores a digital credential. Each ADF is privacy protected.

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

Assured Protection With Third Party Validation

What good is the promise of security without evidence to support the claim? Aggressive and potentially misleading marketing from security vendors can make it very difficult for procurement departments to make good buying decisions.

Investing in a solution that has been independently validated by a qualified and unbiased third party is one of the most effective methods of mitigating this risk.

HID strives to achieve this level of assurance for all customers with Seos. In July 2020 the Seos technology achieved a SEAL-5 rating – the highest level attainable – during an independent security evaluation conducted by TÜV.

This means that Seos offers the first and only physical access control card to ever have been certified by an independent security laboratory.

Who is TÜV?

The TÜV brand has represented security, reliability and neutrality worldwide for over 150 years. TÜV Informationstechnik (TÜViT), a division of the TÜV NORD Group, is one of the leading testing service providers for IT security and is completely focused on security in information technology.

The TÜV NORD Group is one of the biggest technical service providers in Germany, with more than 10,000 employees and business activities in 70 countries worldwide.

You can learn more about TÜViT here.

What is SEAL-5?

TÜViT evaluates information technology solutions and ranks them with a Security Assurance Level (SEAL). SEAL-5 is the highest level attainable through this certification.

To learn more about the evaluation criteria for different security assurance levels, please refer to TÜViT's trusted product security guide.

Data and Privacy Protection

Seos adheres to best practices for data protection and widely reviewed open standards. In fact, it utilizes the same standards as electronic passports, secure signature creation devices and Europay, Mastercard and Visa cards. These include:

Key Management: Goes beyond simplistic methods to calculate card-specific keys which are bound only to application and role.

Mutual Authentication: Provides best-in-class message integrity protection, validating the authenticity of the card and reader to each other and establishing the seed for the session keys used later.

Secure Messaging: Reduces vulnerabilities and protects the integrity of the session as a whole, regardless of its length. Message deletion, insertion, replay or re-ordering is detected and rejected.

Standards-based: Seos proactively uses open, global standards that are regularly reviewed, checked, and verified by authorities to offer the most transparent level of security possible. This is in contrast to proprietary systems which usually do not evolve unless the solution is compromised. 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.

seos

Seos has been developed on proven open global standards.

TIME AND ATTENDANCE

More Applications for More Use Cases

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

SECURE PRINTING

CASHLESS VENDING

PARKING MANAGEMENT

NETWORK LOGIN

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. Seos powers such digital identities across multiple applications, far beyond traditional physical access control, for use in a wide array of industries.

Comprehensive Framework

Seos creates a secure framework that protects access to those digital credentials using cryptographically strong authentication. This is the foundation for a true multi-application card where only authorized systems are able to read those credentials.

Dynamic ADFs

Digital credentials are stored in ADFs and each is protected through selection and authentication, which uses the highest security and privacy levels with multiple keys. ADFs can be created and destroyed dynamically, optimizing use of the available memory over the lifetime of a credential.

Memory Options

Store applications with either 8KB or 16KB memory options. For Java card-based platforms, Seos can be loaded in the secure memory area and available memory is up to 144KB to support custom application development.

One-Time Passwords

Store static passwords and generate One-Time Passwords based on the Oath HOTP standard, a credible alternative to one-time password tokens for secure remote access to computer networks and applications.

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.

Software-based to Provide Form Factor Flexibility

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.

Seos is a software-based credential technology, so 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.

Portable Capabilities - Seos can be ported onto different microprocessor devices for the ability to be delivered in multiple form factors.

Customizable Solutions - Security teams can issue a mix of smart cards and mobile devices to meet employee preferences. Seos powers the award-winning HID Mobile Access® solution.

Selectable Protocol - The Seos Core provides the flexibility to select communication protocols and present a consistent interface to the access control reader, regardless of the communication method.

Additional Convenience and Efficiency - With HID Mobile Access, employees can use smart devices to access doors, gates, networks, and more.

Deployable Remotely - Software patches can also be deployed over the air if needed, as opposed to having to fully reissue chip-based credentials.

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

Discover Seos at hidglobal.com/seos

seos

SMART CARD

MOBILE DEVICE

WEARABLE

HID®

HID Global has helped thousands of organizations around the world to seamlessly introduce Seos. To begin your upgrade to Seos, contact us at **getHID@hidglobal.com** to schedule your consultation today.

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 9171 1108

2021-02-11-hid-pacs-seos-br-en PLT-03689

Part of ASSA ABLOY

hidglobal.com