# seos

## La última generación en tecnologías de credenciales

Seguro, flexible y escalable

HID®


# La última generación en tecnología de credenciales

Las amenazas de seguridad han evolucionado a lo largo de los años y para contrarrestarlas, la tecnología ha ido madurando sobre la marcha. Sin embargo, en lo que respecta a la seguridad física, la mayoría de las organizaciones continúan utilizando tecnologías preexistentes de control de acceso que las dejan expuestas a vulnerabilidades innecesarias. Las organizaciones no solo deben cerrar rápidamente las brechas de seguridad, sino que además deben encontrar soluciones tecnológicas modernas que brinden flexibilidad y escalabilidad para satisfacer las demandas del dinámico mundo de hoy.

**Esta es la razón por la que HID Global creó Seos, la última generación en tecnologías de credenciales.**

Seos ofrece la combinación ideal de seguridad y flexibilidad a cualquier organización. Gracias a sus avanzadas técnicas de cifrado y a una infraestructura basada en software, Seos protege las identificaciones confiables en dispositivos de cualquier forma y tamaño, y puede expandirse a aplicaciones que van más allá del control de acceso físico.

Seos supera tanto a las tecnologías de credenciales existentes como a las preexistentes con los siguientes beneficios fundamentales:

- **Seguridad:** un cifrado óptimo ofrece una inigualable protección de los datos y la privacidad, generando así un entorno más seguro que otras tecnologías de credenciales.
- **Mobilidad:** Seos es una tecnología basada en software y no depende del chip de los equipos de base, lo cual permite mucha más flexibilidad en cuanto a los medios físicos utilizados como vehículos de la tecnología: dispositivos móviles, tarjetas inteligentes y, etiquetas, entre otros.
- **Applicaciones:** El uso de Seos se puede extender a aplicaciones distintas a las del control de acceso físico, entre otras, casos prácticos específicos del sector empresarial, educativo, gubernamental, hotelero y muchos más.

Estas avanzadas prestaciones brindan mayor protección a las organizaciones, a la vez que les of recen la flexibilidad de elegir la combinación adecuada de formas y tamaños de dispositivos y aplicaciones que mejor se ajuste a sus necesidades particulares.

seos

***Seos ofrece la combinación ideal de seguridad y flexibilidad a cualquier organización.***

# Inigualable protección de los datos y la privacidad

Seos ofrece la mayor seguridad, brindando un nivel de protección de los datos y la privacidad superior al que ofrecen las tecnologías de credenciales tradicionales y otras tecnologías del mercado. Esto se debe a que Seos usa un enfoque de seguridad por niveles y a que utiliza las mejores y más estrictas prácticas de protección de datos, entre otras, el uso de estándares abiertos que han sido objeto de exhaustivos estudios.

### Seguridad por niveles y Objeto de Identidad Segura

Seos y sus plataformas de lectores iCLASS SE y multiCLASS SE tienen un enfoque de seguridad por niveles, lo que significa que la tecnología combina varios controles de seguridad para proteger tanto los recursos como la información.

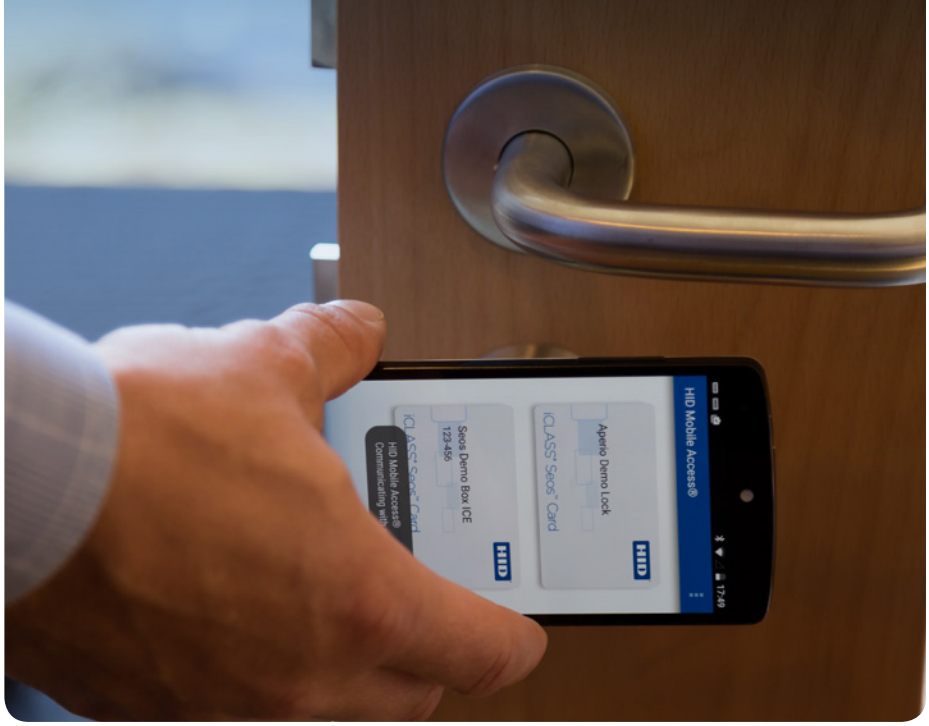
Uno de estos niveles de seguridad proviene del Objeto de Identidad Segura, o SIO, que es un modelo de datos protegido con cifrado para el almacenamiento de datos una identidad segura, como la identificación de un usuario.

El SIO fue diseñado utilizando estándares que son referentes en la industria para aumentar el nivel de seguridad, independientemente del nivel de seguridad del dispositivo de base. Aún más, el SIO es una identificación portátil que se puede programar en varias credenciales físicas y puede ser empleado por aplicaciones y productos de terceros.

El SIO que se emplea con Seos es único ya que contiene cuatro características distintivas que brindan una mejor protección de la seguridad:

- El SIO contiene información de identidad digital que es exclusiva del usuario
- El SIO está ligado criptográficamente al dispositivo
- El SIO se firma en el momento de la creación y esta firma se valida cada vez que se usa la credencial, lo cual garantiza que el SIO proviene de una fuente de confianza
- El SIO está cifrado, lo que impide que una parte no autorizada lea la identificación del usuario incrustada en el SIO.

Estas funciones sientan las bases de un entorno de seguridad más sofisticado que el que se obtendría con las tecnologías preexistentes o con las demás tecnologías disponibles en el mercado.



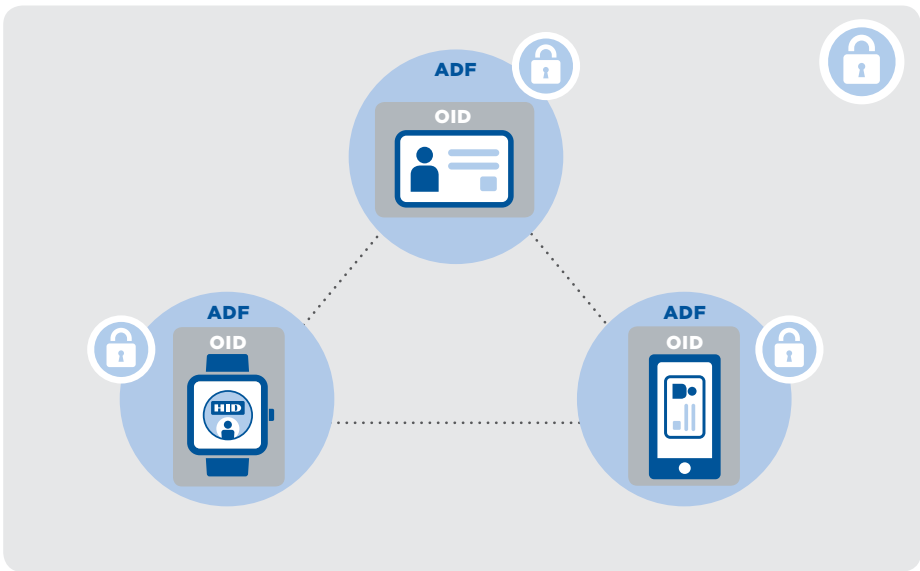

## El Seos® Core

*El Seos Core es una bóveda de seguridad que ofrece un modelo consistente para almacenar y usar credenciales digitales y que funciona en cualquier medio físico utilizado como vehículo de la tecnología, en cualquier hardware y en cualquier protocolo.*

Además de la seguridad que implica el uso del SIO, el núcleo de la tecnología de credenciales de Seos es el Seos Core. Seos Core es una bóveda de seguridad que ofrece un modelo consistente para almacenar y usar credenciales digitales y que funciona en cualquier medio físico utilizado como vehículo de la tecnología, en cualquier hardware (tarjeta inteligente, dispositivo móvil, dispositivo portátil, etc.) y en cualquier protocolo de comunicación.

Para entender mejor lo que es el Seos Core, piense en una bóveda segura que está dividida en varios contenedores. Cada contenedor se denomina archivo especializado de aplicación (ADF, por sus siglas en inglés), tiene un identificador único de objeto (OID, por sus siglas en inglés) y se usa para almacenar una credencial digital.

Cada ADF garantiza la protección de la privacidad de los datos, lo cual pone de relieve la manera en que Seos Core respeta los principios de confidencialidad: no revela ningún identificador específico que permita que la persona que porta una credencial Seos sea rastreada por alguna parte o individuo no autorizado. Tampoco revela ninguna información sobre los tipos de credenciales digitales almacenadas en el Seos Core a un lector no autorizado.



# Prácticas recomendadas para la protección de los datos y la privacidad

Lo que realmente diferencia a Seos de otras tecnologías de credenciales es su estricto cumplimiento de las prácticas recomendadas para la protección de datos y el uso de estándares abiertos ampliamente documentados. Entre dichas prácticas recomendadas, se encuentra la gestión de claves, la autenticación mutua, la mensajería segura y un modelo de diseño fundamentado en estándares.

**Gestión de claves:** Seos utiliza un modelo de gestión de claves para definir claves específicas para cada tarjeta vinculada a la aplicación y al rol. El modelo de gestión de claves de Seos es diferente al de otras tecnologías que usan un método más simplista, por medio del cual solamente vinculan la clave específica de la tarjeta a su número de serie.

**Autenticación mutua:** Seos utiliza esquemas de autenticación mutua basados en estándares que brindan una óptima protección de la integridad de los mensajes: los mismos estándares de los pasaportes electrónicos. El objetivo de la autenticación mutua no es solo que la tarjeta y el lector validen entre sí su autenticidad, sino también sentar las bases para que las claves de la sesión se utilicen posteriormente en mensajes seguros. Este enfoque protege la integridad y la confidencialidad de la transacción de Seos en su totalidad.

**Mensajería segura:** Seos utiliza un mecanismo seguro de mensajería que protege la integridad de la sesión como un todo, como lo hacen los dispositivos de creación de firmas seguras, las tarjetas EMV (Europay, MasterCard, Visa) y los pasaportes electrónicos. Este mecanismo seguro de mensajería protege tanto los comandos como las respuestas, independientemente de su extensión. También protege la integridad de toda la sesión, de tal manera que cualquier eliminación, inserción, repetición o reordenamiento del mensaje es detectado y rechazado. Este enfoque difiere del de las otras tecnologías disponibles en el mercado, las cuales introducen vulnerabilidades al permitir que un mensaje sea repetido o reordenado.

*Con Seos, estos estándares cubren la comunicación sin contacto, la autenticación y el cifrado tanto en tarjetas inteligentes como en dispositivos móviles.*

**Basado en estándares:** Seos usa estándares abiertos que son revisados, comprobados y verificados por las autoridades correspondientes, a fin de brindar el nivel de seguridad más transparente posible. Tener una seguridad basada en estándares significa tener una seguridad de demostrada eficacia: estas normas son revisadas y verificadas de forma regular por las autoridades, a diferencia de los sistemas patentados que, por lo general, no evolucionan a menos que la solución se vea comprometida. Con Seos, estos estándares cubren la comunicación sin contacto, la autenticación y el cifrado tanto en tarjetas inteligentes como en dispositivos móviles. Para lograr la máxima interoperabilidad, Seos ha sido desarrollada con base en reconocidos estándares globales abiertos o especificaciones de referencia.

Además de estas estrictas prácticas, Seos ofrece mejoras adicionales a la privacidad para fortalecer la seguridad. Por ejemplo, el Seos Core no revela ningún identificador único estático a ninguna aplicación no autorizada, ni revela a ninguna aplicación no autorizada siquiera si existe un ADF.

Este estricto cumplimiento de los más altos estándares de protección de datos y privacidad ayuda a Seos a proteger mejor que cualquier otra solución del mercado a las organizaciones frente a las amenazas y vulnerabilidades actuales.

# Solución basada en software que permite el uso de cualquier dispositivo

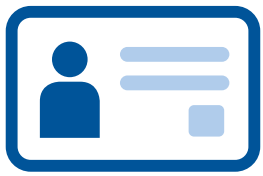
Seos es una tecnología de credenciales basada en software, lo que significa que no está atada al chip del hardware de base. Esta independencia permite muchísimas oportunidades de extender esta tecnología de credenciales seguras a un rango mucho más amplio de dispositivos y protocolos de comunicación, todo para que las organizaciones puedan seleccionar la combinación que mejor se ajuste a sus necesidades particulares.

### Libertad para elegir dispositivos de cualquier forma y tamaño

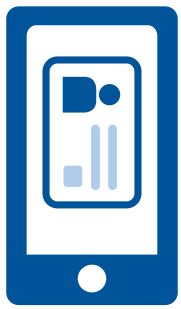
Las credenciales modernas requieren independencia del chip del hardware de base para que los teléfonos, las tarjetas, los accesorios electrónicos y otros dispositivos se puedan usar indistintamente como credenciales auténticas y confiables. A diferencia de las tecnologías de la competencia, diseñadas por los fabricantes de chips, Seos es completamente independiente del chip porque Seos Core es un software que fue desarrollado para funcionar en todas las plataformas. Esto significa que Seos puede ser portado en diferentes dispositivos con microprocesador. Es esta portabilidad la que permite llevar una credencial Seos en dispositivos de múltiples formas y tamaños.

Gracias a esta flexibilidad las organizaciones tienen la libertad de elegir la combinación ideal de medios físicos que mejor se ajuste a sus necesidades concretas. Por ejemplo, los equipos de seguridad pueden emitir una combinación de tarjetas inteligentes y dispositivos móviles para satisfacer las preferencias de los empleados. Para usar un dispositivo móvil como una credencial confiable, Seos ofrece la galardonada solución HID Mobile Access.

Con HID Mobile Access®, los empleados pueden usar sus teléfonos inteligentes, tabletas o prendas electrónicas para acceder a puertas, portones, redes y más. Esta nueva opción de control de acceso mejora enormemente la comodidad del usuario y la eficiencia operativa, además de aumentar la seguridad. Las aplicaciones de HID Mobile Access se descargan fácilmente en Google Play y App Store de Apple, y constituyen una opción moderna y profesional para los empleados que prefieren usar su dispositivo móvil como sustituto o complemento de las tarjetas inteligentes tradicionales.



TARJETA INTELIGENTE



DISPOSITIVO MÓVIL


PRENDA ELECTRÓNICA

### Amplia gama de dispositivos compatibles

HID Mobile Access es compatible con cientos de los dispositivos móviles más populares del mercado actual y se actualiza constantemente para ampliar la compatibilidad a un número cada vez mayor de dispositivos móviles en todo el mundo. Gracias a esta característica, las organizaciones pueden permitir a sus empleados emplear sus dispositivos móviles para el control de acceso, ya sea su dispositivo personal o uno suministrado por la compañía.

En el siguiente enlace podrá consular la lista completa de dispositivos compatibles: hidglobal.com/mobile-access-supported-devices.

### Amplia variedad de protocolos de comunicación

Además de poder elegir la combinación ideal de medios físicos que portará la tecnología, Seos permite a las organizaciones la posibilidad de seleccionar el protocolo de comunicación deseado. Esto es posible dado que la implementación del Seos Core no depende de los medios y, por lo tanto, puede llevarse en una amplia variedad de dispositivos móviles y tiene una interfaz consistente para el lector de control de acceso, independientemente de si se está comunicando a través de Bluetooth, NFC (comunicación de campo cercano) u otros protocolos futuros.

Debido a que Seos está basado en software y no está ligado al chip del hardware de base, funciona en todos los dispositivos, lo cual le permite ofrecer una nueva ola de flexibilidad y escalabilidad para todo tipo de organizaciones. Seos no solo brinda mayor flexibilidad, sino que además aumenta la seguridad ya que los parches de software se pueden instalar de forma inalámbrica si fuese necesario, sin necesidad de tener que volver a emitir por completo las credenciales con chips, como puede suceder con las tecnologías de la competencia.

TIEMPO Y ASISTENCIA

# Más aplicaciones en más casos prácticos

Otro pilar distintivo de las prestaciones de Seos es la posibilidad de usar esta tecnología en aplicaciones distintas a la del control de acceso físico tradicional. Estas aplicaciones pueden abarcar una amplia gama de casos prácticos en diversos sectores, entre otros, el empresarial, el educativo, el gubernamental, el hotelero, el financiero y el de salud. Seos no solo permite la posibilidad de más aplicaciones, sino que su diseño permite que dichas aplicaciones sean más seguras, gracias a su infraestructura y a los ADF seguros y dinámicos.

### Infraestructura segura

Las organizaciones deben estar en capacidad de gestionar las credenciales digitales que se usan en diferentes aplicaciones independientes. Como parte de dicha gestión, deben estar en capacidad de configurar diferentes dominios de confianza. Por ejemplo, no permitir que el sistema de acceso al estacionamiento pueda leer la contraseña de Windows de un usuario de la misma tarjeta. Una tarjeta que tenga aplicaciones múltiples puede almacenar varias credenciales digitales, por consiguiente, implementar una política de control de acceso segregado garantizará que solo los sistemas autorizados puedan leer esas credenciales.

Las soluciones RFID (identificación por radiofrecuencia) actuales pueden almacenar múltiples credenciales digitales que se pueden usar en diversas aplicaciones, pero Seos va más allá, pues ofrece una infraestructura integral que protege el acceso a esas credenciales digitales utilizando una autenticación con cifrado robusto.

### ADF seguros y dinámicos

Con Seos, las credenciales digitales se almacenan en archivos especializados de aplicaciones, o ADF por sus siglas en inglés. Cada ADF es protegido a través de un proceso de selección y autenticación de última generación, en el que se utilizan los más altos niveles de seguridad y privacidad con varias claves, entre otras, claves de privacidad, MAC y de autenticación.

***Otro pilar distintivo de las prestaciones de Seos es la posibilidad de usar esta tecnología en aplicaciones distintas a la del control de acceso físico tradicional.***

IMPRESIÓN SEGURA

VENTA SIN EFECTO

ADMINISTRACIÓN DE ESTACIONAMIENTOS

INICIO DE SESIÓN EN LA RED


*Además de poder almacenar contraseñas estáticas, Seos también puede generar contraseñas de uso único (basadas en el estándar Oath HOTP).*

Además, la estructura que tienen los ADF dentro del Seos Core no es fija. Cualquier sistema que tenga los permisos correspondientes, puede crear nuevos ADF y destruir los ADF antiguos. Conceptualmente, es similar a la manera en que es posible crear o destruir dinámicamente carpetas de archivos en un sistema operativo de PC. Esto permite optimizar el uso de la memoria disponible a lo largo de la vida útil de una credencial.

### Distintas opciones de memoria

Las credenciales de Seos vienen con una amplia gama de opciones de memoria, incluyendo 8KB y 16KB, lo cual permite tener suficiente memoria para almacenar varias aplicaciones. En el caso de plataformas Java con tarjeta, Seos se puede cargar en el área de memoria protegida. En esas plataformas, la memoria disponible es de hasta 144 KB para brindar soporte al desarrollo de aplicaciones personalizadas. La aplicación Seos puede estar junto con otras aplicaciones en el chip.

### Contraseñas de uso único

Además de poder almacenar contraseñas estáticas, Seos también puede generar contraseñas de uso único (basadas en el estándar Oath HOTP) que permiten brindar una alternativa confiable a los tokens de contraseña de uso único para proteger el acceso remoto a redes informáticas y aplicaciones.

**Seos permite a las organizaciones ir un paso más lejos con su control de acceso físico gracias a estas funciones seguras y flexibles para varias aplicaciones. Desde la impresión segura hasta el control de asistencia y tiempo de trabajo, pasando por las máquinas automáticas que funcionan sin efectivo, Seos permite una ruta clara para crear una credencial de mayor valor y más convergente.**

# La última generación en tecnología de credenciales

La tecnología de credenciales de hace décadas se ha quedado corta para satisfacer las necesidades de las organizaciones actuales y su crecimiento en el futuro. Una tecnología de credenciales no solo debe garantizar que el control de acceso físico no sea el eslabón más débil de la cadena de seguridad, sino que además debe brindar un nuevo nivel de comodidad a los empleados y administradores que usan la tecnología diariamente.

El nivel de seguridad óptimo, la flexibilidad en cuanto a la forma y tamaño de los dispositivos portadores de la tecnología y las funciones para aplicaciones avanzadas hacen de Seos la elección ideal en tecnología de credenciales para hoy, mañana y siempre.

Para comenzar su actualización a Seos, comuníquese con nuestros expertos en HID Global. Ya hemos ayudado a miles de organizaciones de todo el mundo a incorporar sin problemas Seos a sus equipos.

Comuníquese con nosotros en **insidesales@hidglobal.com** y programe hoy mismo una asesoría.


***Comuníquese con nosotros en insidesales@hidglobal.com y programe hoy mismo una asesoría.***

seos

América del Norte: +1 512 776 9000 • Línea gratuita: 1 800 237 7769
Europa, Medio Oriente, África: +44 1440 714 850
Asia Pacífico: +852 3160 9800 • América Latina: +52 55 5081 1650



2018-11-27-hid-pacs-seos-br-es PLT-04187

An ASSA ABLOY Group brand

ASSA ABLOY

hidglobal.com