

iCLASS SE Next Generation Access Control

New HID Global iCLASS SE Platform Delivers Trust-Based Security, New Levels of User Empowerment, Improved Usability and Performance, and Enhanced Environmental Sustainability

Building on the success of its proven HID iCLASS® standard for 13.56 MHz contactless smart card technology, HID Global has now created a next-generation access control platform and open ecosystem based on its Trusted Identity Platform™ (TIP) architecture for a new era of advanced applications, mobility and heightened security threats. By enabling a new class of portable identity credentials that can be securely provisioned and safely embedded into both fixed and mobile devices, HID Global’s next-generation platform will provide advanced security and performance functionality while enabling the use of virtual credentials on mobile devices. They will also enable users to add levels of security, customize security protection, and extend system capabilities without having to overhaul the device infrastructure and applications.

HID Global’s new access control platform goes beyond the traditional smart card model to introduce a secure, standards-based, technology-independent and flexible identity data structure based on a new portable credential methodology called the Secure Identity Object™ (SIO). The first product to support interpretation and authentication of this data structure will be HID Global’s iCLASS SIO-Enabled (SE) reader and credential family, which is designed to raise the bar for overall system security while supporting key emerging technologies and delivering superior performance, enhanced usability, and increased environmental sustainability. iCLASS SE readers and credentials also will be the first access control products to operate under the company’s Trusted Identity Platform™ (TIP) framework, which creates a secure and trusted boundary within which all cryptographic keys governing system security can be delivered with end-to-end privacy and integrity.

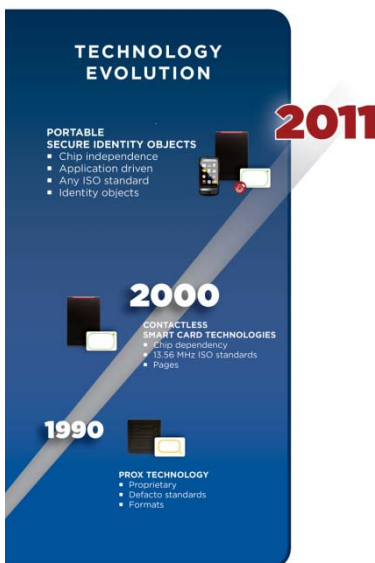
The Access Control Evolution

Prox Technology – Pre 1990 - 2000

Over the last 20 years, HID’s 125 kHz RFID proximity (or Prox) cards and readers have become a de facto standard in the industry. For security managers, dealers, integrators and OEMs, HID Prox cards and readers are recognized as the industry standard for physical access control. HID Prox products are robust, affordable, and seamlessly integrate with access control systems. Today, Prox technology still offers customers the optimum in cost and convenience. However, 125 kHz RFID card technology and card formats are not as secure as contactless smart cards.

Contactless Smart Card Technology – 2000 - 2010

HID Global introduced its first-generation iCLASS technology in 2002, extending the convenience, affordability and reliability of proximity technology to a more powerful and versatile platform that delivered enhanced security through data encryption and mutual authentication. Optimized to make physical access control more



powerful, iCLASS 13.56 MHz read/write contactless smart card technology and read/write fields provides versatile interoperability and supports multiple applications such as biometric authentication, cashless vending and PC log on security. The iCLASS platform has provided reliable service for nearly a decade and, along with HID Global's multi-technology multiCLASS solution, has become the standard for efficient, secure and effective access control.

Portable Secure Identity Objects within a Trusted Identity Platform – 2011 & Beyond

In 2010, HID Global took the first step toward a new generation of contactless smart card and reader technology with the introduction of its TIP framework, which improves security while enabling the migration of physical access control technology beyond cards and readers into a new world of configurable credentials and virtualized contactless solutions. TIP-enabled devices, otherwise referred to as TIP Nodes, provide interoperability and portability of secure identity within a trusted boundary.

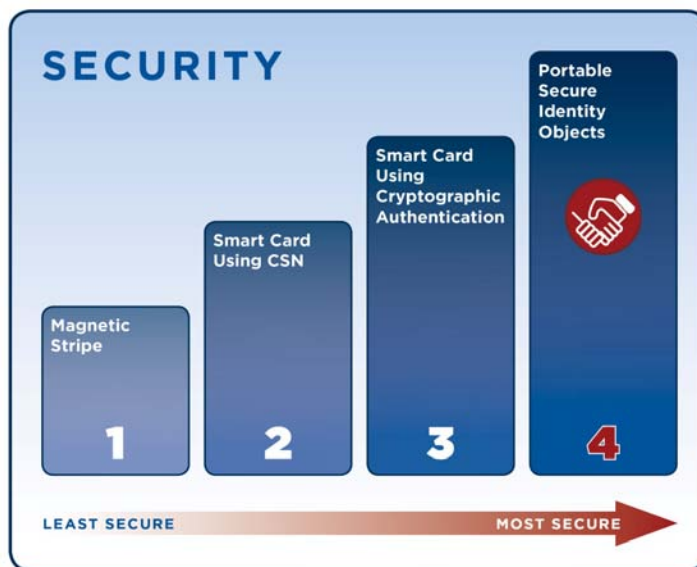


Fig. 1

TIP provides the framework and delivery infrastructure to extend the traditional card and reader model with a new secure, open and independent SIO data-structure on the credential side, and corresponding SIO interpreters on the reader side. SIOs and SIO interpreters perform similar functions to traditional cards and readers, only using a significantly more secure, flexible and extensible data structure.

From Cards to SIOs

An SIO is a standards-based, device-independent data object that can exist on any number of identity devices, including HID's iCLASS credentials. SIOs deliver three key benefits: portability, security and extensibility.

First, SIOs can live within any TIP Node, or where the SIO will be generated and interpreted by TIP Nodes. Thus, not only can SIOs live on HID's world-class iCLASS credentials, they also are portable and can reside on other memory cards containing other card technology, microprocessor-based cards like SmartMX, smartphones with NFC capabilities, USB tokens, computer disk drives, and many other formats. What does this portability bring?

Interoperability and Migration. SIO-based applications defined and encrypted by customers enable solutions that can operate on multiple device types with varying security capabilities. This enables the interoperability of the same object stored on one device to later port to another device with ease and without strict constraints. Research reported in an Avisian 2010 survey shows 90% of end users responding that adding new applications with minimal investment is important, with 53% of industry respondents stating they are not satisfied with the solutions to accomplish this in today’s market.



Second, device-independent SIOs provide an additional layer of **security** on top of device-specific security, acting as a data wrapper that provides additional key diversification, authentication and encryption, and guards against security penetration. Objects are bound to specific devices by utilizing device-unique properties, preventing card cloning.

Trust-Based Security. This security protects objects created and bound to one device from being copied to another device, thus protecting sites against cloned card attacks. 93% of end users expressed a requirement to have multiple layers of security on a card or credential, especially when other applications and private data are present. However, as many as 37% of the industry providers were not satisfied with solutions in the market today as noted in the Avisian 2010 survey.



Thirdly, SIOs are defined using open standards including Abstract Syntax Notification One (ASN.1, a joint ISO/IEC and ITU-T standard), a data definition that allows for an infinitely extensible object definition. This definition can support any piece of data, including data for access control, biometrics, vending, time-and-attendance, and many other applications. Unlike many other fixed-field structures used in today's access control card and reader systems, the SIO and associated interpreters continue to grow in security capabilities while traditional architectures are left behind, stagnant and stuck in a fixed definition. Additionally, this SIO's flexible data definition provides the aforementioned ability to deploy flexible security protection.

Open and Flexible. This extensibility brings significant value to the developer community that utilizes the technology. Since the interpreter takes care of mapping data to supported devices, all the developer has to focus on is generating and transacting (reading/writing) secure objects. The days of the vending-machine developer having to learn about intricate credential-technology sector terminology and key rules is over.

iCLASS SE Platform Overview

The first endpoints to be based on the Secure Identity Object platform will be HID Global's iCLASS SIO-Enabled (SE) family of readers and credentials. The family includes:

- iCLASS SE credentials
- iCLASS SE and multiCLASS SE readers
- iCLASS SE Reader Programming Cards (for field configuration and upgrade options)

SIO-Enabled Platform

Features and Benefits

Based on HID Global's flagship smart card and reader technology, HID Global's iCLASS SIO-Enabled platform features deliver trusted security, new levels of user empowerment, improved performance and usability, and a higher level of environmental sustainability.



Trusted and Secure

- **Multi-Layered Security.** Ensures data authenticity and privacy through the multi-layered security of HID's SIO.
- **Out-of-Box SIO Compatibility.** Ensures highest level of protection.
- **Trusted Identity Platform™ (TIP) Node.** Provides trusted identity within a secure ecosystem of interoperable products.
- **EAL5+ Certified Secure Element Hardware.** Provides tamper-proof protection of keys and cryptographic operations.
- **SIO Data Binding.** Inhibits data cloning by binding an object to a specific credential.
- **Expanded iCLASS Elite™ Program.** Extends private security by protecting uniquely keyed credentials, SIOs, and programming update keys.
- **Velocity Checking.** Provides breach resistance against electronic attacks.
- **Active Tamper.** Protects against physical tampering of the reader.

Sustainable

- **Software Defined Radio (SDR) Technology.** Enables reading multiple types of Prox (125 kHz), including HID and Indala simultaneously enabling SKU reduction.
- **Intelligent Power Management (IPM).** Reduces reader power consumption by as much as 75% compared to standard operating mode.
- **Recycled Content.** Contributes toward building LEED credits.
- **iCLASS SE Credential Compatibility with Standard iCLASS Readers.** Increases perimeter security while reducing reader rip-and-replace.
- **Wiegand-Cmpatible Interface.** Provides connection to existing panels without the need to swap out back-end systems.

Usability / Performance

- **SIO media mapping.** Simplifies deployment of third-part objects to multiple types of credentials.
- **Multi-mode Frequency Prioritization.** Increases transaction performance and improves card management.
- **Combined Bi-directional Host Communication and 125 kHz Support.** Simplifies the reader portfolio offering and expands the use of Prox and higher security connections.
- **New Models.** RP10 and RP30 provide multiCLASS functionality in new form factors, creating more flexible installation options.
- **Flexible Hardware Connection.** Pigtail or terminal strip connections are included on all reader models.
- **Field Programmable Readers.** Provide secure upgrades for migration and extended lifecycle.
- **RGB LEDs.** Delivers increasing capability to notify users and troubleshooters regarding system state.
- **Reader/Card Anti-Passback User Notification.** Provides clear feedback to the user while assisting troubleshooters.

- **Read Progress Notification using LEDs.** Provides clear feedback to the user about new credentials entering the market that require more lead time (e.g. FIPS 201-compatible credentials).

Open

- **Near Field Communication (NFC) Card Emulation.** Enables migration to HID access control on mobile devices.
- **SIO Portability.** Provides technology independence and portability to other smart card technologies.
- **Licensable SIO Generators and Interpreters.** Provide an expansive ecosystem through SDKs and embedded products.
- **Upgradeable Hardware Connection.** Allows all Wiegand-based communication readers to later expand communication capabilities to OSDP, Hi-O and other bi-directional communication protocols.

Conclusion

HID Global's next-generation access control card-and-reader platform provides a generational step function in security, usability and performance, and environmental sustainability. The platform introduces a new portable credential methodology based on a standards-based, technology-independent and highly flexible SIO identity data structure. Products like HID Global's iCLASS SE reader family will use this identity data structure to significantly improve overall system security while creating a more easily extensible access control system infrastructure that can also support a new era of more convenient, virtual credentials that can be embedded into phones and other portable devices.

###