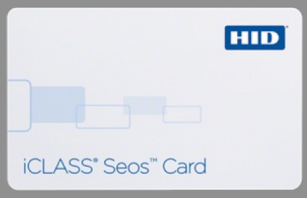
July 2014

iCLASS Seos

Introducing the HID Global iCLASS Seos Card

This whitepaper introduces the HID Global iCLASS Seos Card. It positions the card as the flagship Genuine HID Credential and articulates its capabilities and benefits with reference to other leading card technologies available on the market today.



Günther Lackner & Julian Lovelock
HID Global
July 2014

Table of Contents

Introduction

Access control cards have evolved through several generations, with each generation bringing new functionality and improved security.

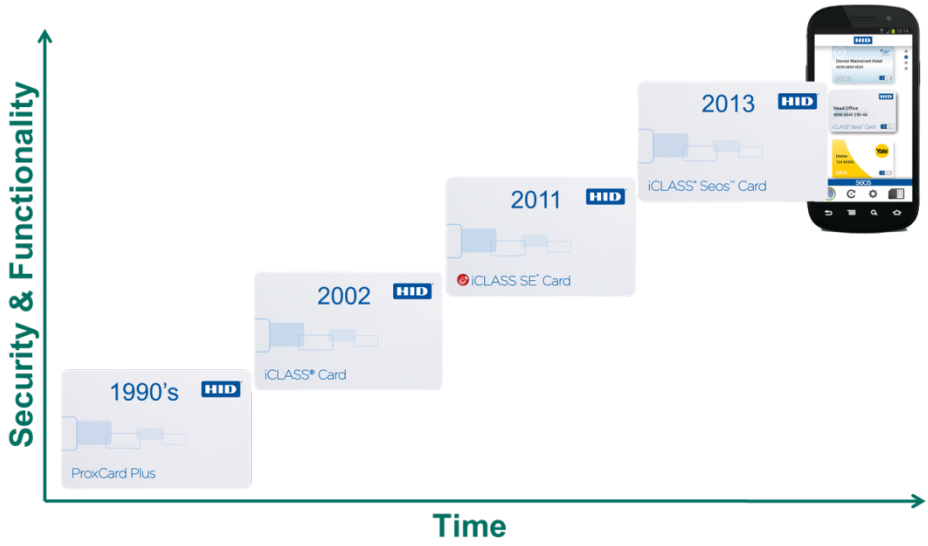


Figure 1 – Evolution of Access Control credentials

The first generation of access control credentials is often referred to as 'Prox'. Prox cards provide a simple ID that can be read by a contactless low frequency (125KHz) reader. The ID is static and can be read in the clear. Thus the cards are easy to copy or forge. These cards cannot be encoded with multiple IDs or other data attributes. Despite their significant limitations, prox cards remain widely deployed due to lack of awareness regarding the risks and inertia arising from the cost of infrastructure upgrades.

Second generation credentials such as standard iCLASS and MIFARE Classic are high frequency cards (13.56MHz) that address the two main limitations of prox cards. Firstly the ID is protected by a mutual authentication process that requires the card to trust the reader and vice versa. This prevents the card from being copied or forged, provided that the cryptographic keys on which this trust is based remain uncompromised. Secondly these 'smart' cards support read/write functional, enabling additional data to be written to the card. Second generation credentials are constructed from an Application Specific Integrated Circuit (ASIC). The ASIC has a unique ID which is leveraged as the trust anchor for these credentials.

Second generation cards provide a substantial increase in security and functionality. However the implementation of identity systems based on these credentials still relies on the ID of the ASIC as a proxy for the user's identity. This limitation is addressed with 3rd generation credentials such as the

iCLASS SE card. The user identity on an iCLASS SE card is encapsulated in a data packet known as a Secure Identity Object (SIO). In line with best practice security models, this data packet is encrypted and signed, thereby providing an additional layer of trust and protection that is independent of the underlying card technology. SIO technology enables multiple application identities to be encoded to the card at manufacturing or post-issuance. SIOs can be loaded onto other card types, such as MIFARE DESFire EV1 and EV2, enabling 3rd generation credentials to be delivered on card technology from HID, NXP and other suppliers.

By defining the user's Identity at the level of the SIO, these 3rd generation credentials take the first important step towards the implementation of Secure Identity ecosystems that are independent of the underlying physical form factor of the credential. However, in practice the implementation remains tethered to specific micro-processor chips and RFID based communication protocols. This is because the mechanisms used to store and read the SIO are hardwired into the underlying micro-processor chip. This hardware dependency represents a key limiting factor in today's secure identity ecosystems. Today's organizations are seeking the ability to manage user identities independent of the underlying hardware form factor (and micro-processor chip). These organizations want to be able to create and manage 'Secure identities', not just on cards but also on mobile phones, tablets, wearables and other credential form factors, connecting through NFC, Bluetooth and other communication protocols. They understand that this requires a credential management technology that is independent of the underlying hardware form factor and connection protocol. From a security standpoint they realize that no technology is ultimately unbreakable, but that best practice security is the adaptability to evolve to address new threats. They also understand the significant benefits in terms of cost savings, security and usability that come from a converged identity management strategy.

The iCLASS Seos card is a fourth generation credential that addresses the needs of these forward looking organizations. Seos adds a software layer executing on top of the underlying hardware chip that provides a secure vault for the storage and use of multiple Secure Identities, defined as SIOs or other formats. This architecture provides a unique set of capabilities and benefits that make the card the most powerful credential on the market today, at a price point comparable to 3rd generation credentials.

This whitepaper considers those capabilities and benefits in more detail and positions the iCLASS Seos card with respect to other credential technologies available on the market today, such as NXP MIFARE DESFire EV1. It also explores how Seos credentials fit within the SE Platform strategy and how the Seos technology powers HID Global solutions such as Integrated Access Control, Mobile Access and Smart Employee ID.

iCLASS SE Platform

In order to fully understand the benefits of 4th generation Seos credentials it is helpful to review the capabilities of the iCLASS SE Platform. 'SE' stands for SIO Enabled. Products across the iCLASS SE Platform enable the creation, management and use Secure Identities Objects (SIOs). The additional layer of trust provided by these Secure Identity Objects is underpinned by the four defining characteristics of an SIO.

Firstly the SIO contains a unique ID for the user. This ID is completely independent of the media on which the SIO is stored. Secondly the SIO contains a binding to the storage media. This ensures that the SIO cannot be copied from one credential form factor to another. In other words it prevents an attacker from making an unauthorized copy of the user's credential. Thirdly the SIO is signed at time of creation and this signature is validated each time the credential is used. This enables the relying system (e.g. PACS door reader) to validate that it is an authentic credential and prevents an attacker from creating a forged credential for a known User ID. Lastly the SIO is encrypted, which prevents an unauthorized party from reading the User ID embedded in the SIO.

The iCLASS SE Platform is comprised of a broad portfolio of products that leverage the SIO to create manage and use Secure Identities. The SE Encoder is able to create SIOs for the encoding of cards and other credential form factors. The iCLASS SE and MIFARE DESFire EV1 SE cards are able to securely store SIOs. The iCLASS SE Readers are able to read and validate SIOs.

A Layered Security Model

Layered security describes the practice of combining multiple mitigating security controls to protect resources and data. While any single defense mechanism will have individual points of compromise, a series of different layers of defense can be used to cover the gaps in any individual layer.

The iCLASS SE platform leverages the Secure Identity Object (SIO) as an additional layer of security.

The SIO is a cryptographically protected data format for the storage of secure identity data such as User ID, biometric templates, demographic or personal data. Based on industry standards, SIO credentials are designed to increase the level of security regardless of the underlying device security level. The SIO is a portable ID that can be programmed on a variety of physical credentials and can be leveraged by 3rd party applications and products. Beyond providing data confidentiality and authentication capabilities, the SIO also protects against data cloning by binding all those identities to a specific physical credential. The cryptographic algorithm used to protect an SIO is based on AES cryptography while the SIO data structure complies with the ASN.1 specification to provide a flexible data model notation.

Specifics of the SIO:

- Each SIO can contain one or many data sets (e.g. a card format for access control)
- Each SIO has a cryptographic context that defines the cryptography used to authenticate and encrypt or decrypt data (e.g. AES encryption & authentication)
- A SIO can be secured by custom keys or by leveraging HID's key schemes such as Standard or Elite
- SIOs are supported in the "SE Elite" program that controls a series of key sets specifically assigned for the iCLASS platform.
- SIO cryptography is agnostic of the underlying chip cryptography and secure channel protocol

Customer Benefits

The SE Platform and the associated layered security model have three qualities essential to creating, managing and using Secure Identities.

- Security – The iCLASS SE Platform includes a variety of credential models appropriate for various risk environments. A core capability of iCLASS SE is media technology independence; achieved through a data model that adds layers of security beyond that provided by the media alone (iCLASS, MIFARE Classic, …). While credential media technologies are evolving, some have been identified by the academic community to contain vulnerabilities (including significant limitations such as insufficient privacy protection). The iCLASS SE layered security model protects against these vulnerabilities.

- End to end solution - The iCLASS SE Platform supports a wide variety of credential technologies available on the market. The platform also includes a full range of readers and encoders. Though the HID Embedded Solutions partner program, industry leaders in secure printing, parking access, healthcare terminals, elevator access, time and attendance and many others have integrated the SE technology into their solutions.

- Extensible – Components of the iCLASS SE Platform are upgradeable to allow for changes in technology and business environments. iCLASS SE also leverages standard-based technologies and practices wherever possible to increase interoperability moving forward.

Introducing Seos

As discussed in the previous section, the iCLASS SE Platform supports 3rd generation credentials such as the iCLASS SE and MIFARE DESFire EV1 SE cards by providing a portfolio of products for the creation, management and use of SIOs on these cards.

4th generation credentials require an independence from the underlying physical form factor, so that phones, cards, wristbands and other wearables can be used interchangeably as authentic trusted credentials. This independence is achieved through the Seos credential vault.

The Seos credential vault

For the purpose of access control, a credential can be considered to be a physical device that is presented by a user for the purpose of proving a claimed identity. As credentialing technology evolves it becomes increasingly important to draw a distinction between the physical credential, such as a plastic card with an embedded RFID chip, and the digital credential, which is the ID data loaded onto that chip. It is the digital credential that provides the proof of ID. The purpose of the physical credential is simply to carry that digital credential and protect it from being copied or manipulated.

As discussed in the introduction, physical credentials increasingly come in many different shapes and sizes. These are sometimes referred to as different form factors. The credential is no longer only an ID card. It may be a phone, a keyfob, a wristband or a watch. Likewise the credential won't always communicate over RFID. It may communicate to the reader over Bluetooth, WiFi or some other communication protocol that has yet to be invented.

The Seos vault provides a consistent model for storing and using digital credentials, regardless of the underlying form factor and communication protocol. Seos uses the cryptographic capabilities of the underlying micro-processor chip to ensure that digital credentials are protected when stored within the vault. Likewise it establishes a secure channel with the reader that is layered on top of the underlying transport protocol. This means that credentials can be securely read from the vault over lightweight protocols such as Bluetooth Smart.

While the implementation of the Seos vault may vary, depending on the underlying processor chip, in all cases the vault presents a consistent edge. Hence the process of reading a digital credential is identical, regardless of whether the vault is instantiated on a card, a phone or a wearable.

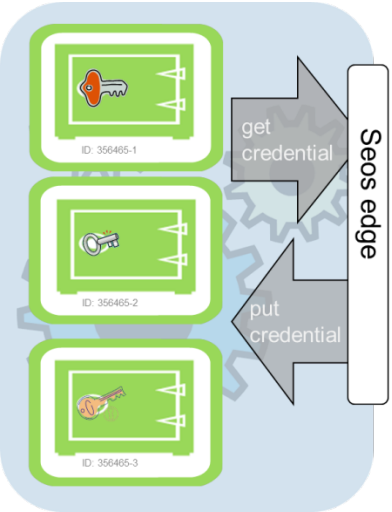


Figure 2 – Physical credential with Seos vault

Figure 2 shows a graphical representation of the Seos vault, instantiated on a physical credential. The vault can be thought of as being compartmentalized into multiple containers.

Each container is referred to as an ADF. Each ADF has a unique OID and is used to store a digital credential, (such as but not limited to an SIO). The vault construct does not constrain the format of that credential.

Each ADF is protected by a distinct access key. The reader must know the access key for the desired ADF in order to read the digital credential from that ADF.

This segregation ensures that the reader only gets visibility to the ADFs that it is authorized to read from. It is an integral part of the privacy model of the Seos vault that the reader is not even aware of the existence, let alone the contents, of ADFs that it is not authorized to access.

Figure 2 represents the Seos vault with three ADFs. In practice the number of ADFs is limited only by the available memory space on the underlying processor chip. Seos enables ADFs within the vault to be created and destroyed as needed even after the credential has been issued in the field.

This fourth generation credential architecture based on the Seos vault provides an important set of benefits.

- The Seos vault can be instantiated on any computing platform. This enables any smart device to function as a credential. Of course, the security of the vault is dependent on the underlying runtime environment. Hence a Seos vault instantiated in a Java Card chip will be more secure than one that is running natively on a mobile phone's operating system. Nonetheless, this portability offers immense potential for a broad range of credentials with varying degrees of risk appropriate security. The benefits of **Media / Device Independence** are explored further on in this section

- The Seos vault is implemented as a software layer independent of the underlying micro-processor chip. This enables the implementation of the vault to evolve more rapidly to address new security threats. Seos supports changes to the ADF structure that is not achievable with 3rd generation credentials. This **Upgradeability** is explored subsequently in this section.

- Digital credentials can be read from and written to the Seos vault over any communication channel, including NFC, Bluetooth and WiFi. This greatly extends the range of use cases for both provisioning and use of a digital credential. The most immediate benefit of this capability is evident in solutions that leverage a Mobile phone as a physical credential. **Mobile readiness** is also explored in this section.

- The vault 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. Nor does it reveal any information on the types of digital credential stored in the vault, to an unauthorized reader. **Privacy support** is explored in more detail at the end of this section.

Media/ Device Independence

The iCLASS Seos vault can be ported onto different microprocessor devices. It is this portability that enables Seos credential to be delivered as multiple different form factors including Java Cards, key fobs, wearables and mobile phones.

The Seos edge (see figure 2) is consistent independently of the underlying form factor. In other words, SIO's or other data objects can be read from the Seos vault using a consistent command set, regardless of the device is a card, a phone or a wristband.

Media / Device Independence brings a number of important benefits

- A consistent model for lifecycle management of credentials, regardless of the underlying form factor.
- Different credential form factors can be used interchangeably with a common reader infrastructure without needing to program readers to understand different communication protocols or credential formats.

Upgradeability

The upgradeability of a Seos credential can be considered at two levels.

The first level is the ability to create or destroy ADFs within the vault after the credential has been issued. The structure of ADFs within the vault 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. As with file folders on a PC, the number of folders is constrained only by the available memory space. Likewise, the folders themselves are ambivalent to the format of the data files stored within them.

Benefit:

- iCLASS Seos vault executes as a software application on the microprocessor chip on the card. Therefore it is able to create and destroy ADFs in order to optimize use of the available memory over the lifetime of a card.

The second level is the ability to upgrade the functionality of the Seos vault after the device has been programmed and issued and not to lose the existing data while performing this update. This enables new features for the management and use of digital credentials, as well as the ability to apply security patches These specific requirements will be addressed according to the capabilities and usual management processes for the underlying devices (such as TSM for SIM cards or secure elements, mobile application stores, card management systems, updater stations for off-line access control systems etc.).

Mobile Readiness

The demand for mobile access solutions continues to grow, driven by a variety of factors including user convenience, the immediacy of provisioning & de-provisioning and the more intangible 'coolness-factor'.

The access control market will continue to rely primarily on cards and key fobs for many years. A lot of organizations require their employees to carry badges bearing card holder's photo. Security policies can be simpler to apply if the credential is a physical device, such as a card, issued by the organization. Nonetheless secure mobile access credentials provisioned to NFC/Bluetooth devices (smart phone, tablets, and handhelds) can complement access cards. Organizations are planning ahead to support both types of credentials for access control and beginning to run pilots and POCs to better understand how they can gain benefits from these emerging technologies. The best approach is to use a standards-based card technology that is portable onto those emerging smart devices, and to enable multiple types of physical credentials to co-exist within an integrated access control solution.

The media independent nature of the Seos vault enables it to reside on a wide variety of mobile devices and present a consistent interface (or edge) to the reader, regardless of whether it is communicating over Bluetooth or NFC.

Benefits:

- Users can now deploy an access control solution that starts with cards and then subsequently adds mobile phones as an additional credential type, with the same readers.

- The media independence provided by the Seos vault enables “any” mobile device to be provisioned with an SIO and used with an SE reader. This is critical for organizations with a Bring Your Own Device (BYOD) policy because it enables support for many different types of phone.
- The Seos TSM provides support for Over-The-Air (OTA) management (delivering and revoking digital keys) of devices and credentials.

Privacy Support

Definition: “Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.” (Source: http://en.wikipedia.org/wiki/Privacy

In the context of PACS/LACS solution, privacy protection requires that personal identifiable information or global unique identifiers (such as UID or CSN) are not accessible or traceable, by unauthorized parties.

How to get effective privacy protection on RFID cards:

- Mutual Authentication with diversified keys (to ensure that cards only present information to authorized readers)
- Secure Data Storage (data is only accessible by entities with proper access rights or security parameters (ex: keys are obfuscated/scrambled in the device memory)
- Secure Communications through secure messaging which ensures that intercepted data is not readable by unauthorized entities.
- Resistance to smart bomb attacks (*) - the card does not disclose even under active probing any information about the context in which the card would work or not.

(*) A smart bomb attack imagines an explosive device which is set to trigger when it detects the presence of an RFID card used for access to a high profile building such as an embassy. Defense against a smart bomb attack requires not just that the digital credential itself is protected but that the card reveals no information about the types of credentials that it carries.

The iCLASS Seos card

The iCLASS Seos card is the reference solution for organizations deploying fourth generation credentials in a card form factor. The same card can be used for cafeteria payment, parking, secure-printing and as a logical access control solution (LACS) credential for computers, VPNs, applications or mobile devices without any additional cost on the credentials side

Ideal for organizations with stringent security requirements, iCLASS Seos cards provide superior data integrity and privacy protection by leveraging the latest standardized cryptographic algorithms.

For migration purposes, Seos credentials are also available as multi-technology cards combining 125 kHz Proximity and a 13.56 MHz high frequency Seos contactless microprocessor. Further multi-technology cards will follow in due time opening further migration paths towards Seos (e.g. from MIFARE Classis and iCLASS)

The iCLASS Seos Card is built around an NFC compliant RFID enabled micro-processor chip, executing the Seos vault application. This implements open protocols based on standards to provide long-term security of customer's investments.

The iCLASS Seos card is a multi-application credential providing state of the art layered security, privacy and a simplified customer experience.

Leveraging Open Standards

iCLASS Seos card is fully based on open standards, that are well proven and state-of-the-art in the industry. These standards cover contact and contactless communication, authentication, cryptography on smart cards as well as on mobile devices. Supported applications reach from access control to payment, transportation and many others. All Seos credentials will carry out of the box support for PACS credentials as well as LACS supporting applications such as VPN access or device login.

For maximum interoperability, Seos has been developed on well-proven open global standards or reference specifications

Benefit:

- Standards based security means proven security: Standards in general are more often reviewed and result from the collective work of several companies, the academic community as well as government entities. Those standards are regularly checked and verified by authorities (including government standardization bodies), in contrast to proprietary systems which usually do not evolve unless the solution is compromised or under strong scrutiny from attackers. For this reason, open standard-based solutions are more generally secure.
- Open standards enable customers to invest into future-proof access control infrastructures as well as easy 3rd party product integration with iCLASS SE platform through Developer Tool Kits (to be available in the future). As of the platform ecosystem of products, iCLASS Seos cards can be provisioned through HID Global's iCLASS SE Encoder.
- Mutual authentication using AES-128 keys.
- Access control to data objects using access lists
- Key diversification ensuring each card has unique keys for each credential (ADF: Application Data File. This is where each Application resides).

- Secure channel protocol using session keys for all data transfers.
- Isolated credential domains. No compromising relationships (e.g. shared keys) if multiple credentials are used.

Multi-application

A multi-application card can be used as a single credential across multiple different applications. For example, the same card is used to access the parking garage, enter the building, login to a computer system, purchase a coffee and collect a print job.

In some instances this can be achieved by configuring all these different applications to recognize a single ID (digital credential) stored on the card. However this approach has substantial limitations:

Firstly, a single digital credential format does not work for all applications. For example, the digital credential used to access a computer system would need to be a password or a One Time Password (OTP), which is a fundamentally different type of digital credential to that which is required for physical access

Secondly, organizations need to be able to manage the digital credentials used for different applications independently. They need to be able to set up different domains of trust. It would not be acceptable for the parking access system to be able to read a user's windows password from the card. Nor would it be acceptable for the closed loop payment system in the staff canteen, operated by an external catering company, to be able to read from the employee's card the SIO that gains access to the data center.

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 such as iCLASS, MIFARE DESFire, MIFARE Classic, or PIV cards are capable of storing multiple digital credentials for use across multiple applications, but iCLASS Seos goes further, providing a comprehensive framework that protects access to those digital credentials using cryptographically strong authentication. (this is not always the case with other technologies where some credentials may communicate via their contactless interface without proper authentication).

Digital credentials are stored in ADFs. Each ADF is protected with the Seos Authentication Key Set, which must be known to the application in order for the application to read the digital credential. The Key Set comprises an encryption key and MAC key which collectively establish a Secure Channel, using the ISO 7816-4 Secure Messaging protocol.

The default profile for the iCLASS Seos card includes an SIO for secure access to Physical Access Control Systems (PACS). It also includes an One Time Password (OTP) seed for secure access to computer systems as well as allocated containers for static passwords. Seos doesn't support PKI-based services

(neither do MIFARE Classic and MIFARE DESFire). For such deployments, an HID Crescendo or pivCLASS smart card is needed.

Benefits of the Seos card:

- Provides a dynamic model for allocating space for digital credentials for new applications
- Enforces strong segregation across digital credentials for different applications, preventing credential leakage

Converged Logical and Physical Access

Many organizations follow best practice and require the use of two factor authentication (2FA) for access to IT resources such as Virtual Private Networks (VPNs) and web based applications. Employees who need access to these IT systems are issued with an authentication device which secures the login process. In most cases these authentication devices take the form of a One Time Password (OTP) token. The token generates and displays an OTP, which the user enters when logging in. These tokens provide a substantial improvement in security when compared to a static password. However there are a number of issues with OTP tokens. The tokens can be expensive to issue and manage. These costs are not limited to the cost of the token itself but also include the cost of issuing the devices as well as helpdesk costs for replacing lost devices. The tokens are battery powered and hence they expire after a few years and need to be replaced. The tokens are unpopular with users as they represent an additional device that needs to be carried around. They are particularly unpopular for use with touchscreen mobile devices.

The Seos card, in addition to being able to store static passwords, is also capable of generating One Time Passwords (based on the Oath HOTP standard) and hence provides a credible alternative to OTP tokens for secure remote access to computer networks and applications.

Benefits of the Seos card:

- Seos card can be used as a Tap-IN credential to a growing number of NFC enabled laptops, notebooks, tablets and phones.
- Organizations are able to reduce costs by no longer needing to issue and manage OTP tokens and instead can leverage the card that is already issued for physical access control
- iCLASS Seos card does not require batteries and hence unlike an OTP token it does not expire
- Removes the need for end-users to carry an additional device
- Provides a simpler and more convenient end-user experience by removing the need to type passwords into touch screen devices such as tablets

Total Cost of Ownership (TCO)

Investment protection and improved TCO with the ICLASS SE platform:

Future proof solution, ready for all “next generation” use cases: Ideal for securing the NFC interface for smart phones and tablets (delivered as “Virtual Credentials” for simplified migration to NFC-enabled phones).

Readiness for post issuance updates: iCLASS Seos is using a microprocessor chip loaded with a software application. Therefore, it is possible to update the applications during the lifetime of a card.

iCLASS Seos cards are always shipped with long-life composite card body.

Capacity options

Memory options:

- iCLASS Card available in 2k bits / 16kb / 32 kb*
- On native cards: iCLASS Seos available in 8K-Bytes and 16K-Bytes*

Seos has ”32 times” the memory than iCLASS 2k / 2k+Prox for same price

For Java Card-based platforms, Seos can be loaded in the secure memory area. On those platforms, available memory is usually up to 144 KB. The Seos application can reside side by side with other application in the chip.

Summary

The Seos card is a true fourth generation credential, providing capabilities that are unparalleled on the market today. It is a multi-application, NFC compliant smart card that combines the layered security model of the SE platform with the standards based interface of the Seos vault.

It is the first credential with the potential to truly deliver on the promise of converged access control and offers the perfect choice for any organization seeking to issue an open standards credential that can be co-deployed with a mobile access solution.

Glossary of Terms

Term	Meaning
Physical Credential	A physical device that is presented by the user as proof of a claimed identity. Physical credentials can take many forms including cards, key fobs and mobile phones.
Digital Credential	The data attributes and keys stored on the physical credential that prove the claimed identity. A digital credential is sometimes referred to as a Virtual Credential.
Mobile ID	A Digital Credential stored on a mobile phone.
A Secure Identity Object (SIO)	An instance of a digital credential that is compliant with a specific HID defined format. The format provides mechanisms to encrypt the ID, sign the digital credential and bind it to a physical credential.
SIO Signing key	The key that is used to sign an SIO. The key is symmetric, hence the same key is used to verify the signature on an SIO
SIO Encryption key	The key that is used to encrypt an SIO. The key is symmetric hence the same key is used to decrypt the SIO.
SE Platform	A portfolio of Genuine HID products enabling the creation, management and use of secure identities encapsulated within SIOs
Seos Vault	A software application executing on a physical credential that takes responsibility for the secure storage and use of digital credentials.
Seos Edge	The interface exposed by the Seos vault that enables an authorized system to write to and read from an instance of the Seos vault instantiated on a physical credential
Seos Credential	A Physical Credential that exposes the Seos Edge
Seos Reader	A processing unit able to read digital credentials from the Seos vault. The read may occur over NFC, Bluetooth or another communication protocol. The Seos Reader may also validate the digital credential, as with the iCLASS SE Reader. Or validation may occur outside of the reader, as in the case of a One Time Password.
Application Dedicated File (ADF)	An individual container within the Seos Vault that is used to store one or more digital credentials. Access rules for the Seos vault are defined at the level of the ADF
Seos Integrator key	A key that enables the creation and destruction of ADFs within the Seos Vault. The Seos Vault Profile would define support for a finite number of Integrator keys.
ADF Name	A unique name (e.g. HID OTP ADF) for the ADF, which is used by the Seos reader to select it.
ADF Selection	The process of selecting the ADF from which the Seos reader wishes to read a digital credential. ADF selection can identify the full ADF Name or by a wild card search.
Seos Vault Profile	A pre-defined layout for a set of ADFs and associated access rules which determines the default structure of an instance of the Seos vault on a given class of physical credentials
Seos Authentication Key Set	The key Set required to read the digital credential from an ADF. The Key Set comprises an encryption key and MAC key which collectively establish the Secure Channel.
Secure Channel	A secure connection between the Seos Reader and the Seos vault, established using the ISO 7816-4 Secure Messaging protocol. The Secure Channel protects the Digital Credential from an unauthorized read, while in transit from the Seos Vault to the Seos reader.
ADF Diversifier	A seed that is read from the Seos vault and then used by the reader to derive the Seos Authentication Key Set for the ADF. The diversifier should be random but is not necessarily

	globally unique.
Seos Privacy Key	The key required for the ADF Selection and to read the ADF Diversifier.
SIO Interpreter	A component able to validate the authenticity of an SIO. To do this the SIO Interpreter needs access to the SIO Signing key and SIO Encryption key. The SIO interpreter may be an integral part of a Seos reader, such as the iCLASS SE Readers.