

***iCLASS*[™] Levels of Security**

***iCLASS* is the most flexible 13.56 MHz smart card technology available today!**

Do you want the convenience of receiving preprogrammed cards that are ready for use?

No problem - trust HID to manage your keys!

Do you want your own keys or are you an HID Corporate 1000 user?

The *iCLASS* Elite Program provides preprogrammed keys that are specific to your organization and managed by HID!

Do you want to manage and change your keys on-site?

The *iCLASS* Field Programmer is a smart solution!

Do you want to write your own application to generate and manage keys?

HID provides powerful tools for advanced users.

Do you want to use your own badging software to personalize *iCLASS* cards?

Advanced development tools are available to select OEM customers.

Do you want a custom solution based on your security specifications?

Contact HID today!

***iCLASS*, the first contactless smartcard technology designed by and for the access control professional, is also flexible enough to bridge the gap to a multitude of applications. *iCLASS* for physical access, as well as embedded integration, is only limited by the imagination and expertise of HID customers and development partners worldwide.**

With assistance from the *iCLASS* support team, you too can choose and implement the level of *iCLASS* that best meets your requirements.

We begin with the definition a key:

The key is like a “password” that protects the contents of a specific application area on the contactless smart credential. There is always a diversified key (the key is hashed with the card serial number to create a unique key) on the credential, whether it is a secret key that no one knows or an insecure key that is known by many. When the credential is presented to a standard reader, mutual authentication will attempt to compare the selected key in the credential to the selected key loaded into the reader, and either permit or deny access. The key is 64 bits long, allowing for 2^{64} (or approximately 18.45×10^{18}) different combinations. The basis of key management is the way in which keys are generated, transferred, and securely stored.

The levels of iCLASS are defined by: (1) who is generating the key; (2) the algorithms at work during the key generation and authentication; and (3) who takes responsibility for the implementation and maintenance of the system.

Level 1 - Standard Security

Quick Reference			
Who generates the key?	Algorithms used?	How to order readers?	How to order cards?
HID	DES, H0	Standard Part Number	Standard Part Number

Standard Security is the first step for access control professionals who are upgrading from proximity or other legacy systems such as wiegand, magstripe, barium ferrite, and barcode to contactless smart cards. Level 1 incorporates the Standard Security features of *iCLASS* while maintaining the ease of installation and compatibility to existing access control panels. Any existing HID format can be stored securely on the credential and output in Wiegand.

To accomplish this, HID created a Standard Key that is stored in every reader and programmed into every Standard Security credential. Having this key match “out-of-the-box” allows all Standard Security credentials to “beep-n-blink” all Standard Security readers upon presentation. For a similar price, the *iCLASS* offering exhibits the same fit and function as proximity, with the added benefit of enhanced security.

Level 2 - High Security (iCLASS Elite)

Quick Reference			
Who generates the key?	Algorithms used?	How to order readers?	How to order cards?
HID	DES, H0,H1,H2	Custom Part Number	Custom Part Number

For those who want a boost in security, but not the added responsibility of key management, HID has designed the ***iCLASS*** Elite program. Utilizing two additional hash functions, HID will generate site-specific High Security Keys for the customer. Credentials and readers will be factory programmed with the site-specific High Security keys to match. Only those credentials programmed with site-specific High Security keys will communicate with site-specific High Security readers. HID assumes responsibility for unique key generation, key storage, and configuration cards.

Level 3 – High Security (iCLASS Field Programmer®)

Quick Reference			
Who generates the key?	Algorithms used?	How to order readers?	How to order cards?
Customer	DES,3-DES, H0,H1,H2	Standard Part Number	Blank

The highest possible security lies in the ability to generate your own keys and change them as often as you like. The ***iCLASS*** Field Programmer* (CP400) gives the customer the ability to completely control all aspects of key management and site maintenance, including key generation, reader configuration, and user data input and editing. The advanced capabilities require the greatest level of customer responsibility to maintain the system's integrity and ensure the future compatibility of credentials and readers.

With both the *iCLASS* Elite and Field Programmer levels, the keys can be updated with a configuration card at the readers. Credentials are updated during the next presentation to an updated reader.

Level 4 – Serial Protocol

Quick Reference			
Who generates the key?	Algorithms used?	How to order readers?	How to order cards?
Developer	DES, H0	Standard Part Number	Standard Part Number or Blank

Detailed documentation, sample source code, and knowledgeable technical support ensure that HID software developing partners have all of the necessary tools to interface between a host PC or microcontroller and the ***iCLASS*** reader/writer of choice. All default keys are freely distributed to developers who have attended ***iCLASS*** Level 2 Training, so that they may develop across any available application areas. Key generation and storage procedures allow the developer to implement their own key management scheme. The developer assumes all responsibility for the proper storage, retrieval, updating, and security of their own application.

Level 5 - OEM

Quick Reference			
Who generates the key?	Algorithms used?	How to order readers?	How to order cards?
OEM	DES, H0	Standard Part Number	Blank

With the use of advanced development tools, select OEMs will have the capability and flexibility to program credentials and configure readers, with either a custom key or the HID Standard Security key, utilizing their own software. In this level, the OEM assumes the responsibility for key management, programming of credentials, reader configuration, and configuration cards.

Level 6 – Custom

Quick Reference			
Who generates the key?	Algorithms used?	How to order readers?	How to order cards?
Customer Specified	Customer Specified	Custom Part Number	Blank

The advanced user will have the opportunity to submit a specification for custom reader firmware development by ASSA ABLOY Identification Technology Group (ITG) Research and Development Center. Custom features including alternate or no security algorithms will be considered.

*Consult Factory