

Glossary of *iCLASS*TM Terms

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Appendix A – Glossary of Keys

2K/2 -- A 2kbit (256 Byte) memory credential with 2 Application Areas. The read/write area is from block 6 to 31. This credential offering does not allow for ISO 14443B communications or the updating of keys after the fuse is blown.

16K/2 -- A 16kbit (2K Byte) memory credential with 2 Application Areas. The read/write area is from block 6 to 255. This credential offering allows for multi-ISO communications in both 15693 and 14443B modes and the ability to update the keys on the cards as often as desired.

16K/16 -- A 16kbit (2K Byte) memory credential with up to 16 Application Areas. The read/write area is from block 6 to 31 per Page, with 8 Pages. This credential offering allows for multi-ISO communication in both 15693 and 14443B modes and the ability to update the keys on the credentials as often as desired.

AES -- Advanced Encryption Standard. A symmetric block cipher algorithm that can use key lengths of 128, 192, or 256 bits. AES replaced the DES standards for U.S. government applications as of July 2002 and is documented in NIST FIPS 197. Can be used in *iCLASS* to encrypt *iCLASS* Field Programmer generated keys before storing them in the database. (*Also see Encryption.*)

Algorithm -- A sequence of steps used to mathematically manipulate data. (*Also see Hash and Encryption.*)

Anti-counterfeiting -- Additions to the exterior physical makeup of the credential that protect it from being easily copied. Examples of anti-counterfeiting elements include holograms, ultraviolet fluorescing inks, optical variable devices (OVDs), and micro-printing.

Anti-Passback -- A configurable reader parameter that defines the delay duration between consecutive reads of the same credential.

APDU -- Application Protocol Data Unit, as defined in ISO 7816-4. A simple Command/Response communication protocol developed for the contact chip market. The use of this protocol in *iCLASS* will enable previously developed contact applications to easily port over to contactless smart card technology.

Application Areas -- A dynamic memory segment of readable/writable storage.

Application Limit -- A fixed length 8 bit field within the Configuration Block (Byte 7) that sets the last block of the first Application Area per page.

Application Issuer Area -- Block 5 on all *iCLASS* credentials. Proposed as a storage area for Application Identifier and Version information.

ASCII -- American Standard Code for Information Interchange.

Back Box -- Sometimes called a J-box or junction box, this is a standard wall switch electrical enclosure that readers can be mounted to. Back box sizes differ in various parts of the world.

Binary -- Base 2 numbering system, where the only valid units are 0 and 1. (*Also see Bit.*)

Biometrics -- The technology of using physical characteristics of the human body for verification of identity.

bit -- A single binary digit, either a one (1) or a zero (0). (*Also see Binary.*)

Blank -- Any credential that has not been Configured or Programmed.

- Brute Force Attack – An attack on keys that requires testing every possible key one at a time. This is uncommon; even if thousands of keys could be tested per minute, it would still take years to find the actual key.
- BWL -- Block Write Lock. A fixed length 8 bit field within the Configuration Block (Byte 6) that can be set to write protect blocks 6 to 12.
- Byte -- Eight bits.
- Card -- A credential manufactured out of PVC to conform to the ISO 7810 standard. Additional cards can either meet more stringent standards (*also see Embeddable*) or no standard at all. (*Also see iCLASS Wiegand*.)
- CE -- The CE mark is the official marking required by the European Community for all electric- and electronic equipment that will be sold, or put into service for the first time, anywhere in the European community.
- Challenge -- The result of the mutual authentication algorithm that the credential uses to authenticate the reader. (*Also see Mutual Authentication*)
- Chip Configuration -- A fixed length 8 bit field within the Configuration Block (Byte 3) that defines secure and non-secure credentials.
- CHK -- Checksum, used to validate data
- Cloning – The attempt to duplicate a credential in order to defeat a smart card system. (*Also see Replay Attack*.)
- Configuration Block -- Block one (1) of all **iCLASS** credentials.
- Configuration Card -- A special **iCLASS** credential that will reconfigure **iCLASS** reader parameters. Configuration cards will allow you to adjust such things as LED/Sounder operation, Wiegand pulse/spacing, hold line, and update keys.
- Configured Credentials -- Any credential that has been configured (i.e., the memory configuration has been set) and the fuse blown.
- Credential -- Any of the available form factors of **iCLASS** (Card, Tag, and Key).
- CSN -- Card Serial Number, also called the Unique Identifier (UID). Designed to be unique on every 13.56MHz contactless smart card worldwide. Used for anti-collision to select one card in the excite field at a time.
- Decryption -- Manipulation of encrypted data through an algorithm to return it to its original form.
- DES -- Data Encryption Standard. A symmetric block cipher algorithm using a single 56 bit key. The same key is used for encryption and decryption. DES is documented in NIST FIPS 46.
- Diversification -- A hash algorithm that “scrambles” the CSN with a specified key.
- DLL -- Dynamic Link Library. Allows software developers a high-level programming interface that helps reduce integration time and difficulty.
- Dual-LED Control -- A configurable parameter in the reader that allows hardware control of both the Red and Green LED.
- EAS -- Electronic Article Surveillance
- EEPROM -- Electronically Erasable Programmable Read Only Memory
- Elite -- A program developed by HID whereby we will generate, manage, and program site-specific High Security Keys into **iCLASS** credentials and readers before they are shipped to the customer. This provides a higher level of security than Standard Security Keys and alleviates the customer's key management responsibilities.
- Embeddable -- A card that is manufactured to the ISO 7816 standard to allow for the embedding of a contact smart chip.
- Encryption -- Manipulation of data through an algorithm to make it indecipherable.
- Written by: Nathan Cummings – Product Marketing Manager

FCC -- Federal Communications Commission

Field Programmer -- An HID **iCLASS** product that will allow the customer to program **iCLASS** credentials with either Standard Security or High Security keys. The field programmer will also enable the customer to encrypt the HID Application, store and update PIN numbers and passwords, store and update the user-defined fields, and generate High Security keys on site.

FIPS -- Federal Information Processing Standards (which are NIST's published standards documents).

Firmware -- An executable application that resides within a microcontroller. With **iCLASS** the firmware resides in a Microchip PIC18F and defines the start-up, default settings, and operation/functionality of the reader/writer.

Fuse -- A fixed length 8 bit field within the Configuration Block (Byte 0) that when updated will eliminate the possibility of future changes to the Configuration Block.

Handspring -- A PDA (like a PalmPilot) that has a larger expansion port able to accommodate an **iCLASS** read/write module. (*Also see Springboard*.)

Hash Algorithms -- An algorithm that when provided with a variable length unique input will always provide a fixed length unique output. This is a one-way algorithm such that given the output, it is nearly impossible to re-generate the input. NIST supports hash algorithms with SHA-1 covered in FIPS 180.

Hex -- Hexadecimal, Base 16 numbering system, where valid units are 0 – F.

HID Access Control Application (HID Application) -- Always resides in Application Area 1 of programmed **iCLASS** credentials. HID has reserved 13 blocks (6 – 18) for the HID Application to contain the HID Directory, HID card format, PIN, Password, and 4 user defined fields.

Hold Line -- A hardware line with a configurable EEPROM parameter in all **iCLASS** readers. Allows for either buffering a single card read or completely disabling the RF excite field when active.

Host -- The host is either a PC or a microcontroller that controls the communications of an **iCLASS** reader/writer (slave), usually in Pass-thru mode.

iCLASS/Wiegand -- A multi-technology card that incorporates both the **iCLASS** and Wiegand load technologies. This card is thicker than most and thus does not meet the ISO standards.

Interoperability -- The ability for products from multiple manufacturers to recognize and operate with one another.

ISO -- International Standards Organization

ISO 10373 -- Standard that covers testing methods for identification cards.

ISO 10536 -- Standard that covers Contactless Integrated Circuit Cards – Close-Coupled. Not widely used.

ISO 14443 -- Standard that covers Contactless Integrated Circuit Cards – Proximity. Includes the Type A (primarily MIFARE®) and Type B versions.

ISO 15693 -- Standard that covers Contactless Integrated Circuit Cards – Vicinity. This is the primary standard used in **iCLASS**.

ISO 7810 -- Standard that covers the physical characteristics of identification cards.

ISO 7811 -- Standard that covers the specifications of recording techniques such as embossing and magnetic stripes.

ISO 7816 -- Standard that covers the placement and communications of contact smart chips.

Keyfob -- A credential made of hard plastic and designed to be either placed on a key ring or suspended from a standard badge clip or lanyard.

Key Management -- The way in which keys are generated, transferred, and securely stored.

LED -- Light Emitting Diode. HID has implemented a LED array and light bar to produce a better visual indicator at the reader.

Logical Access -- (*See Secure Logon*)

LSB -- Least Significant Byte

mA -- Milliamp

MHz -- MegaHertz

Microcontroller -- A board level component that controls the operations and communications of a specific device based on its firmware. A microcontroller can also act as a host when embedding *iCLASS* OEM Modules into other equipment.

MSB -- Most Significant Byte

Multi-Technology Credential -- A credential that incorporates more than one technology into a single card (i.e., *iCLASS* Prox or *iCLASS* Wiegand).

Mutual Authentication -- A means by which two entities can authenticate each other before transferring data. With *iCLASS*, mutual authentication is accomplished using a Challenge and Response generated from a secret algorithm that resides in both the readers and the credentials. The keys are never transferred during mutual authentication.

NIST -- National Institute of Standards and Technology, Founded in 1901, NIST is a non-regulatory federal agency within the U.S. [Commerce Department's Technology Administration](#). NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

OEM -- Original Equipment Manufacturer

OEM Module -- A reader/writer that is distributed in PCB form to be embedded into third-party products. Usually operates in slave mode.

Ones Complement -- A permutation of binary data where every 1 becomes a 0 and every 0 becomes a 1.

Open Collector Output -- This solid-state switch provides a means of controlling any device or logic input that can be operated by a switch closure, and is useful for non-access control applications, where a relay may not be available at the reader location. Available only on the Reader/Writers.

OTP -- One-time Programmable. A fixed length 16 bit field within the Configuration Block (Bytes 5 and 6) that can not be updated. Default setting is "FFFF". Each bit can be changed from a one (1) to a zero (0) only once.

Page -- A 2kbit (256 byte) separation of the 16K/16 credential, thus eight pages are available. Each page has up to 2 Application Areas protected by their own 64 bit diversified key. Each page has a maximum 208 bytes of read/write data storage.

Pass-thru Mode -- A state of the reader/writer that responds to serial communication commands. (*Also see Slave.*)

Password -- A 64 bit field reserved within the HID Application (Block 10) for PC password storage. (*Also see Secure Logon and Logical Access.*)

PC -- Personal Computer. A desktop, or laptop, that can be used to interface with any *iCLASS* reader/writer. (*Also see Host.*)

PCB -- Printed Circuit Board

PDA -- Personal Data Assistant. A mobile data processor normally used to store calendar events, addresses, and to-do lists. With the addition of an *iCLASS* Springboard Module, the PDA becomes a mobile reader/writer. (*Also see Handspring.*)

Permute -- To change the order or arrangement.

- PIN -- Personal Identification Number, used as an alternate form of verification with a keypad reader. A 48 bit field reserved within the HID Application (Block 9) for PIN storage.
- Programmed Credentials -- Any credential that has been Configured and Application Area 1 has been programmed for access control with any existing HID format.
- Reader -- An **iCLASS** reader that is used for access control applications in Security Mode. The readers do not have serial communication capabilities.
- Reader/Writer -- An **iCLASS** reader/writer has all the capabilities of an **iCLASS** reader with the added functionality of serial communications.
- ReadIT -- A generic database demonstration application developed for the Handspring.
- Read Range -- The maximum distance between the credential and the reader whereby proper communications can take place. Read range can be affected by the credential form factor, reader size, and installation environment.
- Replay Attack -- A way of compromising security by recording the communications between the credential and the reader and replaying it back to the reader at a later date. (*Also see Sniffer and Cloning.*)
- RES -- A temporary storage string used during the checksum calculation in the key generation process.
- Response -- The result of the mutual authentication algorithm that the reader uses to authenticate the credential. (*Also see Mutual Authentication.*)
- RFU -- Reserved for Future Use.
- RND -- Random Number. A 64 bit random number generated by the reader/writer and used in the key generation process.
- RS-232 -- A common serial communication protocol that allows up to 150 feet cable distance.
- RS-485 -- A common serial communication protocol that allows up to 4000 feet cable distance.
- SDK -- Software Developers Kit. A complete package of tools that will allow software developers to easily integrate **iCLASS** into their application. Usually consists of a reader/writer, power supply, serial interface cable, and CD-ROM that contains sample application, source code and documentation.
- Secure Logon -- An application that allows you to securely log on to your PC. Usually incorporates something more than a password, such as a token or biometric.
- Security Mode -- A state of the reader/writer that will search **iCLASS** credentials for the HID Application card format information and output the data in Wiegand and/or RS-232. (*Also see HID Application.*)
- Serial Protocol -- A list of commands used by software developers to communicate with **iCLASS** reader/writers and credentials. The serial protocol can be implemented using low-level APDU messaging or high-level DLL calls. (*Also see DLL and Character Protocol.*)
- Site-specific -- Only credentials programmed for a specific site will operate with readers configured for the same site. (*Also see Elite.*)
- Slave -- A state of the reader/writer when it is completely controlled by a host. (*Also see Pass-Thru Mode.*)
- Sniffer -- A piece of equipment that is used to analyze, record, and replay radio frequency communications. Companies such as IFR manufacture spectrum analyzer equipment that can monitor frequencies from 9kHz to 26.5Ghz. (*Also see Cloning and Replay Attack.*)
- Source Code -- Software developer generated text files that can be compiled into executable applications. Source code is usually generated using programming languages such as Visual Basic (VB) or C++. (*Also see SDK.*)
- Speaker -- A sounding device used in place of a beeper in **iCLASS** readers to emit variable frequency and duration sounds.
- Springboard -- The expansion port of a Handspring PDA.
- Stored Value Area -- Block 2 on all pages of all **iCLASS** credentials. Requires access to both Key 1 (Debit) and Key 2 (Credit). Not available on 2 Application Area credentials. Maximum value is 65535.

Tag -- An adhesive backed credential that can be placed on any non-metallic device to *iCLASS*- enable the device. (*Also see Credential.*)

Tamper Magnet -- HID provides a magnet embedded in the potting of the reader to be used with a reed switch (not provided) mounted in a back box. This is only available on the R30, R40, RW300, RW400, RK40, and RWK400. (This is not available on the R10.)

Template -- The mathematical representation of a physical characteristic used in biometric storage and verification. (*Also see Biometric.*)

Triple-DES -- A symmetric block cipher algorithm that uses two 56 bit keys. The same keys are used for encryption and decryption. DES is documented in NIST FIPS 46.

TTL – Transistor/Transistor Logic. A binary serial communications where logic high (>2V) = 1 and logic low (<0.8V) = 0.

UL – Underwriters Laboratory. An independent, non-profit product safety testing and certification organization.

VDC -- Volts Direct Current

Wiegand -- A standard access control output protocol where two conductors, white and green, are used to send binary data, ones and zeros respectively. The normal state of a Wiegand conductor is +5VDC. When the voltage drops below +1.7VDC, it signifies a single bit. When the voltage returns above +2.8VDC, the bit is complete and the conductor returns to its normal state. (*Also see Wiegand Pulse and Wiegand Spacing.*)

Wiegand Pulse -- A configurable reader parameter that defines the duration of a single wiegand bit pulse.

Wiegand Spacing -- A configurable reader parameter that defines the duration between two wiegand bit pulses.

XOR -- Truth table.

Input		Output
0	0	0
0	1	1
1	0	1
1	1	0

Appendix A – Glossary of Keys

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 on the credential whether it is a secret key no one knows or an insecure key that is known by many.

Keys that are stored in the card:

Key 1 -- A diversified key that resides in Block 3 of the credential and protects the first Application Area on any particular page.

Debit Key -- Same as Key 1 that is required to decrease the amount currently loaded into the Stored Value Area (Block 2).

Key 2 -- A diversified key that resides in Block 4 of the credential and protects the first Application Area on any particular page.

Credit Key -- Same as Key 2 that is required to increase the amount currently loaded into the Stored Value Area (Block 2).

Diversified key -- All keys that are stored on the credential are diversified with the card serial number to ensure that every key on every credential is unique.

Keys that are stored in the reader:

Default Keys -- Key locations 1 and 2 are pre-loaded with default keys during the manufacturing of the reader. The pre-loaded keys match Key 1 and Key 2 in blank credentials. (Default Key 1 = F0E1D2C3B4A59687 and Default Key 2 = 7665544332211000).

HID Default Keys -- HID generated “public” keys that protect Application Areas 2 – 16 on all Configured or Programmed *iCLASS* credentials. These keys will be made available to our software development partners in the Key Distribution document.

Standard Security Key -- A key developed by HID and stored in all *iCLASS* readers and reader-writers. The Standard Key allows for instant compatibility between Standard Security readers and Standard Security credentials.

High Security Current Key -- High Security Mode key that protects the HID Application. Can be updated using a special configuration card that moves the Current Key to the Previous Key location and Updates the Current Key to the one stored in the card. Only available on 16K credentials.

High Security Previous Key -- High Security Mode key that protects the HID Application. Used for mutual authentication if the Current Key fails. If the Previous Key passes authentication the Current Key will be updated on the credential. Only available on 16K credentials.

Encryption Keys -- Two keys securely stored in the reader used for DES and Triple-DES encryption of data within the HID Application.

Key locations 0 – 11 -- Twelve key locations in the reader that store keys used in Pass-thru Mode. These are the only keys that are accessible via the serial port. (At the current time, only key locations 0 through 7 are accessible.)

Exchange Key -- Knowledge of this key is required in order to load alternate keys into the reader. This key is stored in key location 0.