

CP400 Security

Q: What is the difference between Standard Security and High Security iCLASS systems?

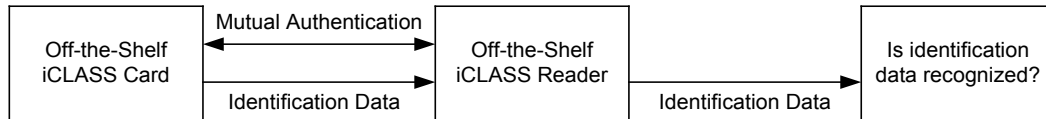
A: In a Standard Security system, the HID standard security algorithm is used by the reader to compute the key inside an iCLASS card. In a High Security system a system-specific algorithm is used for this purpose. An individual High Security system is thus isolated from all other iCLASS systems (both Standard and other High Security systems).

Q: How does a Standard Security or a High Security System affect the reader behavior?

A: A reader in a Standard Security system will successfully authenticate (reader will beep and blink its LED) all Standard Security iCLASS cards and will send the identification data on the card to the upstream system, for example, an access control panel. The upstream system is responsible for determining if the card is part of the local system or not. A High Security reader will only successfully authenticate iCLASS cards that are part of its own system so the only time the High Security reader sends data upstream is when it is from a card of its own system.

Q: If my Standard Security iCLASS card is authenticated by any Standard Security iCLASS reader, does this mean I can access other facilities?

A: No. The upstream system will differentiate between cards of its own system and cards from other systems. It will reject cards from other systems.



Q: What is involved in authenticating iCLASS cards and readers?

A: In all HID Global iCLASS systems, the iCLASS card and the iCLASS reader execute a mutual authentication protocol. Successful execution of this protocol convinces that reader that it is in communication with a valid iCLASS card and convinces the card that it is in communication with a valid iCLASS reader. In other words, the card and the reader authenticate each other; they mutually authenticate.

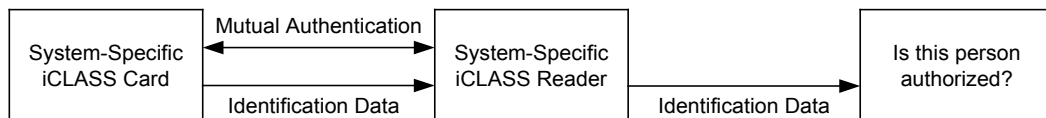
Q: Does Standard Security offer protection?

A: Yes. Standard Security and High Security systems use the same mutual authentication protocol between the card and reader. The only thing different is how the reader computes the key contained in the card.



Q: Are there any downsides to using a High Security system?

A: Some additional overhead may occur when introducing new cards into the system since each card has to be configured with a system-specific key. High Security readers can be configured to perform this task. Alternatively, HID can provide iCLASS cards configured for a specific High Security system as part of its Elite program.



Q: What else is involved when working with High Security Systems?

A: With more flexibility come more decisions to be made. For example, the keys in a High Security system can be changed whenever the manager of the system wishes. Such a change can be made temporary or permanent. Because High Security systems require the customer to be responsible for key management duties they may generate administration costs over and above those associated with Standard Security systems.

Q: Is there a way of getting the system isolation benefit of High Security without this management overhead?

A: Yes. The HID Elite program can supply High Security cards and readers pre-configured for a specific High Security system.

Q: What are the commonalities between High Security and Elite systems?

A: In operation they are identical. In both cases the readers use a system-specific version of the algorithm that computes the key in the card and the key on the card is specific to this algorithm.

Q: What is the difference between High Security and Elite systems?

A: Keys in High Security systems are managed by the customer or somebody the customer designates. Keys in Elite systems are managed by HID.

Q: What is the CSN?

A: CSN is an acronym for Card Serial Number. The CSN is an 8-byte number that is specific to a particular iCLASS card. The CSN is how the card is uniquely identified within the population of all iCLASS cards.

Q: Should I use the CSN for an access control solution?

A: The iCLASS card CSN is transferred from the card to the reader in the clear – that is, unencrypted – during the time that the card and the reader are establishing communication. As a result, the CSN could be seen by an unauthorized party and used to build a card that emitted this CSN. This duplicate card would fail iCLASS mutual authentication of course but if you based your access control decisions on just the CSN it might fool you. That said using just the CSN for access control or logging into internal spaces where the card has already successfully participated in the iCLASS mutual authentication protocol at an external boundary could be useful.

Q: Can a High Security or Elite reader also read a MIFARE CSN?

A: No. Only the secure iCLASS application can be read on High Security or Elite readers.