



# Quick Guide to HID Card Formats

**Do you use HID contactless cards to access the building each day?** If so, consider using your HID card to authenticate to Dell® Latitude™ and Precision™ laptops. Simply choose to order an optional embedded contactless smart card reader in your new laptop!

## Introduction

One of the ways that Dell simplifies IT is by removing cost and complexity associated with the prevention of unauthorized access to the laptop and associated data. By integrating the first multi-technology contactless smart card reader into select Latitude and Precision laptops, Dell can help customers to use one card for logical and physical access control.

There are two types of contactless cards typically used for physical access control:

- The 125 kHz proximity card is widely used for physical access control. It is a read only card and does not work with the embedded contactless smart card reader offered by Dell. If you are using this type of card for physical access control, HID and Dell can assist in the use of this card with peripheral readers. Or, we can help you to seamlessly upgrade to a multi-technology card. This card will allow users to leverage their existing investment in the physical access control system while upgrading to new applications.
- The 13.56 MHz contactless smart card is also used for physical access control and other applications such as cashless payment and transit. It is a read / write card and does work with the embedded contactless smart card reader offered as an option by Dell. iCLASS® by HID is the most commonly used contactless smart card for physical access control.



**HID iCLASS® cards can now be ordered through Dell.**

In the physical access control space, most contactless cards rely on a "format" for individual user identification. In order for the user community to take advantage of one card for logical and physical access control, cards must be provided with the correct format. This document is to provide an overview of "formats" and the associated security levels.

To learn more, use the Quick Guide to HID Card Formats on the back of this sheet.



USE A CONTACTLESS SMART CARD FOR AUTHENTICATION TO  
**THE NEW LATITUDE™**



### **Definition of a Format**

A "format" is simply a number encoded into a contactless card that identifies a specific person within an organization. The structure of the numbering scheme can be either very simplistic and widespread, or very specific to a facility or company.

### **Non-Secure Format Communications**

Every contactless smart card has a card serial number (CSN) in accordance with the respective contactless ISO standards. The CSN is designed to be used for anti-collision only (i.e., the ability to distinguish between multiple cards near the reader at the same time). The transmission of the CSN is completely in the clear (unencrypted), so it can be easily intercepted and replayed to the reader. Additionally, the CSN is a unique random number encoded during manufacturing and cannot be modified to be added or adapted to existing physical access control systems. For these reasons, the CSN should never be used for physical or logical access control.

### **Secure Format Communications**

HID Global primarily supplies personalized cards that have a specialized format encoded into a secure memory area of the contactless smart card. Secure formats are typically specific to a physical access control manufacturer or an end-user. The format is secured within the card using industry standard encryption, mutual authentication and diversified keys. The security mechanisms employed for secure reading of the format prevent known attacks such as replay and card cloning.

### **The Importance of Defining / Matching Formats**

When deploying replacement or new cards for logical access into existing physical access control installations, cards must be ordered and personalized to match the existing system. Or, in some cases, if ordering new cards, users may choose to upgrade their format. Many physical access control manufacturers have enabled their systems to accept multiple formats, but this feature can limit the total number of users available in the database. Identifying and providing the correct format into an existing installation will dramatically reduce the work necessary to provide a converged physical/logical solution.

For assistance in defining a card format, please contact HID Global at: [dellhotline@hidglobal.com](mailto:dellhotline@hidglobal.com)

### **It is Easy to Use One Card for Logical and Physical Access Control**

- Step 1:** Determine if you are using an HID card for physical access control. (The HID logo is typically on the back of the card.). Make note of the string of letters and numbers printed in the lower right-hand corner on the back of the card. This will help HID to identify the exact type of card you are using.
- Step 2:** If you are interested in using the same card for pre-boot authentication or secure two-factor authentication to the Windows® Operating System (XP® or newer), move to Step 3.
- Step 3:** For more information, technical assistance, or to discuss what options are available, contact HID at [dellhotline@hidglobal.com](mailto:dellhotline@hidglobal.com).

© 2010 HID Global. All rights reserved. HID, the HID logo, and iCLASS are trademarks or registered trademarks of HID Global in the U.S. and/or other countries. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

**Let HID show you how Dell simplifies IT by removing cost and complexity associated with the prevention of unauthorized access to the laptop and associated data.**