

Application Note #9 – XACTT™

XceedID
Automated
Credential
Transition
Technology



Overview

XceedID's patent pending XACTT™ technology provides automatic upgrading from industry standard HID® proximity cards to state of the art 13.56 MHz secure contactless cards.

One of the typical requirements for migrating to a new card technology is enrollment of the new credentials into the security system software and panels. This task can be time consuming, inconvenient and subject to input errors by the user. Fortunately XceedID XACTT provides a convenient, cost effective and seamless migration path from virtually all HID proximity cards to secure contactless smart cards.

Using XACTT technology eliminates the requirement of a dedicated card programming station and also eliminates the typical enrollment requirement of the new contactless smart card at the head end security workstation.

Simple 3 Step XACTT Upgrade

Once a decision has been made to migrate from proximity to secure contactless smart cards, using XACTT is simple. Each individual employee or cardholder has an existing proximity card that provides access. Security

personnel distribute new secure 13.56 MHz ISO-X contactless smart cards (Future compatibility with secure MIFARE® or secure DESFIRE®) to all individuals that possess existing proximity cards. Each User then visits an XACTT Upgrade Reader (reader configured in XACTT mode) in their facility for a simple 3 step automated upgrade process which requires less than one minute per user.

First, the user presents the new contactless smart card (picture 1). The ISO-X reader beeps once and begins flashing a green LED.



Picture 1 – present new contactless card

XceedID(TM), XACTT(TM) and ISO-X(TM) are trademarks of XceedID Corporation. GE®, CASI® and ProxLite® are registered trademarks of General Electric Corporation. MIFARE®, I-Code® and DESFire® are registered trademarks of Philips Electronics, Inc. HID® and iCLASS® are registered trademarks of HID Corporation. my-d® and Infineon® are registered trademarks of Infineon. Other product names mentioned herein may be trademarks and / or registered trademarks of other companies.

The user then presents the old HID proximity card (picture 2). The reader beeps twice and the green led stays on.



Picture 2 – present old proximity card

The new contactless smart card is presented once again and is now programmed (picture 3). The reader beeps three times to indicate successful programming. The new card now provides access through all prior authorized points of entry.



Picture 3 – present new contactless card again

During this three step process the ISO-X reader actually performs a secure write of data - identical to the original proximity cards data string - into the new contactless smart card. This allows the contactless smart card to output data identical to the data from the proximity card. The data is stored in the secure access control application area of the card. This is what eliminates the enrollment requirement at the head end security workstation. The user is then required to return the old HID proximity card to the security department for disposal (picture 4).



Picture 4 – disposal of old card

XACTT Implementation Example

From a logistics standpoint, each individual company will want to craft specific policies for how to administer secure credentials using XACTT. One example would be to require all individuals to pick up their new card from the security office and to perform the upgrade at the closest reader. They would then be instructed to immediately return the old proximity card for disposal. This could all be performed under the supervision of the security department. Another example of XACTT would be to perform the upgrades at a particular access point in a facility. A security guard could stand at the reader and watch users perform the upgrade. The guard would then simply collect the old cards from employees immediately upon upgrade (picture 5).



Picture 5 – return of old proximity card

Additional XACTT Features

After using XACTT to upgrade all personnel to contactless smart cards, some customers may want to eliminate any future access by proximity credentials. This is possible by presentation of a secure command card to the respective ISO~~X~~ readers. After all readers have been re-configured by command card, the reader will no longer allow access to any proximity cards. However, even though the reader will not allow access to the proximity card, it will continue to allow upgrading of proximity cards to contactless smart cards.

In practice, this feature may be desirable after a complete XACTT upgrade. Perhaps some personnel were on business travel during the upgrade or perhaps there were some proximity cards unaccounted for. This disabling of all proximity cards provides security and peace of mind that proximity cards will no longer provide access yet the flexibility of the XACTT technology combined with ISO~~X~~ readers allows continued upgrades.