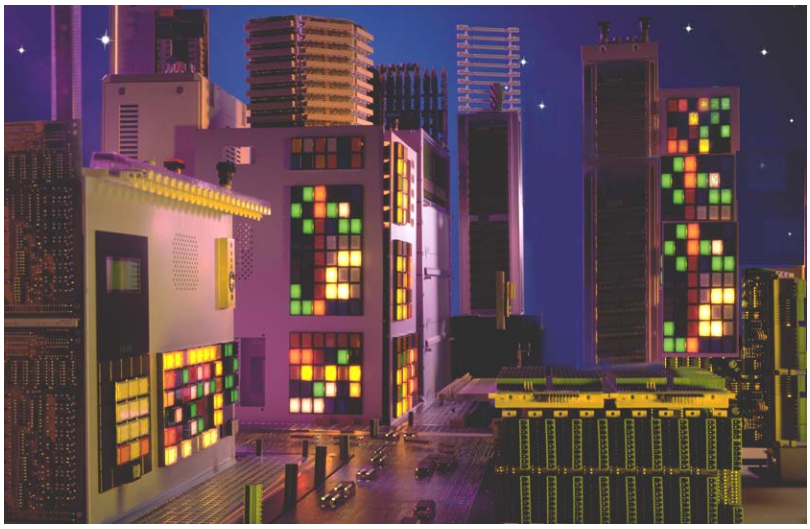
Application Notes Biometric Templates on Contactless Smart Cards



HP3000 / HKII – IOLAN XXW

Version 5.0

Contents

Versions

Release	Date	Status	Description
1.0	6/3/2002	Concept	Application notes on the integrated solution of the HP3000 / HKII with the IOLAN XXW MIFARE reader.
1.1	10/07/2002	First Release	Added Upload Keys From Project Card based on pincode
1.2	10/08/2002		Upload Keys From Project Card based on MIFARE keys
2	06/20/05		Added Notes on Card management
3	07/08/09	Special Release	Added Support for two card configurations, card type 1 uses Sector 2 and 3, card type 2 uses Sector 13 and 14
4	06/04/11	Special realease	Added Support for two card configurations, One type card uses sector 2&3, second type uses sector 11&12
5	02/27/12	Combined release	Merges different types of documentations into one, extra information on project cards

References

#	Title	Version	Authors	Date
1	RSI IOLAN ISI Hand Punch 4000	1.4	ISI	04/08/01
2	SmartEncoder Manual	8	ISI	06/01/10

Biometric Templates on Contactless Smartcards

Instead of storing user templates in centralized databases, the contactless smart card technology allows users to store templates directly on the user card, thus preventing complicated template management over several locations. This new approach allows a direct check on ownership of the card at the access points where the card is presented. Stolen cards will be left unusable to others.

Recognition Systems and Iolan Systems Inc. have developed a turn-key integrated solution of Smart card reader / writer and the RSI products. The combination of HandReader and smart card reader manages templates on the user card. No centralized storage of the templates is required. Performance and distribution problems are solved in this integrated solution. The contactless smart card reader is built into the unit, thus reaching an optimal integration and user friendliness level.

Integration HP3000 / HKII / XXW

User interface and networking aspects are handled by the HP3000 / HKII; the XXW reader is responsible for reading from and writing to the MIFARE Cards. This setting allows the HP3000 a uniform interface where no project specific items like keys and card location have to be programmed; the XXW reader is prepared for easy adaptation to these project specific settings and can be programmed to project specific needs.
Also, from a security point of view this setup is a good one; no MIFARE keys will be transported from the HP3000 to the XXW; thus allowing no interception of this type of information on the communication line.

Functionality

After enrolling users on their own user card, using a project specific procedure the operation of the system is very user friendly:

- The user card IS presented to the smart card reader
- ID information and template are read from the card
- The user places their hand on the HandReader
- The HandReader checks the actual hand image against the template on the card
- If the user is verified, the door open contact is activated or Wiegand output is created
- When necessary, an updated template is written back to the card

Since the smart card reader uses a dedicated port of the HandReader, the normal communication options stay intact, thus allowing easy upgrades of existing projects without changing the technical infra-structure.

Only 2 out of 16 sectors (1K card) are used to store the Template and ID information for this application and the rest of the card is freely available to other applications. The information on the card is securely stored behind project specific MIFARE keys so only cards created for a specific project can be read by the integrated combination.

Project Cards

The function of the project card that is shipped with every reader is to upload the MIFARE keys to the HandReader. This allows companies to bring the MIFARE keys that they use to secure sector 2 and 3 of the badges (user cards) they have in use to the HandReader reader. For any MIFARE reader to work with user cards, there will need to be a match between MIFARE keys in the card and reader. When you receive the HandReader from the factory, the public keys set A0A1A2A3A4A5, B0B1B2B3B4B5 are pre-loaded in the project card and already brought to the HandReader for test purposes.

There are two kinds of projects: Demo projects that come with a demo project card and Production projects. Production Projects are installations that are used for secure access control.

Demo projects

HandReaders belonging to a demo project are used in demo situations like on site sales demo, test situations and for readers used in shows. Basically these readers use the same type of project card; any demo project card will work with any demo reader. Security is not an issue here so it is convenient that any project card will work with all the readers on site.

Production projects

Every production project has its own project card, and it is important that a project card created for company A does not work on the site of company B. Otherwise, it would be possible that company A could change reader keys in company B readers. The combination of reader / project card is embedded in the reader software and can only be changed by reprogramming the reader.

Uploading user card keys to the HandReader

The user cards that are used by the employees to get access to a building are protected by secret MIFARE keys. When default MIFARE cards are purchased, they are unprotected and block 3 for all sectors will contain a public keyset, depending on the chip manufacturer either A0A1A2A3A4A5, B0B1B2B3B4B5 or FFFFFFFFFFFF, FFFFFFFFFFFF.

Before going into production the public keys need to be replaced by a new set of secret keys, and this can be done with the SmartEncoder software.

The next step is to get the HandReaders to work with the new secret keys. The project card will take care of transporting the secret MIFARE keysets to the HandReader.

Uploading MIFARE keys to project card

There are a couple of options to get the company specific secret MIFARE keys in the project card:

1.) ISI can upload the keys and send them with the readers. For this to work we will need the secret keys in Austin under a NDA

Companies can use the SmartEncoder software and upload the secret keys on site.

User cards

MIFARE is a remote coupling smart card system for multi-applications. It was tailored especially for automatic fare collection (AFC) and similar applications. A plastic card the size of a credit card is passed over a reader target within a distance of up to 10 centimeters, or 4 inches. Reading information from the card and writing information back to the card takes only a few milliseconds. Thus, for example, passengers boarding a bus or subway train can simply walk through gates while the transaction takes place.

When moving the card over the reader target, passengers can leave the card in their wallet, even if it contains coins. The world largest installation of contactless smartcards services the 12 million inhabitants of Seoul, where MIFARE cards are used for payment in the public transport system, and related applications. This project has proven the maturity and reliability of MIFARE.

The MIFARE Cards can handle multiple applications. Every sector can carry information for a different application. On the 1K MIFARE cards each sector is divided into 4 blocks of information; each block can contain 16 bytes of data; block 3 of each sector is used for key storage and access conditions for that particular sector.

0	Block 0 16 bytes	Block 1 16 bytes	Block 2 16 bytes	Sector Keys and AC
1	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
2	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
3	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
4	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
5	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
6	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
7	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
8	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
9	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
10	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
11	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
12	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
13	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
14	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
15	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC

More information on MIFARE cards can be found at: www.MIFARE.net

User Cards: Application Sectors

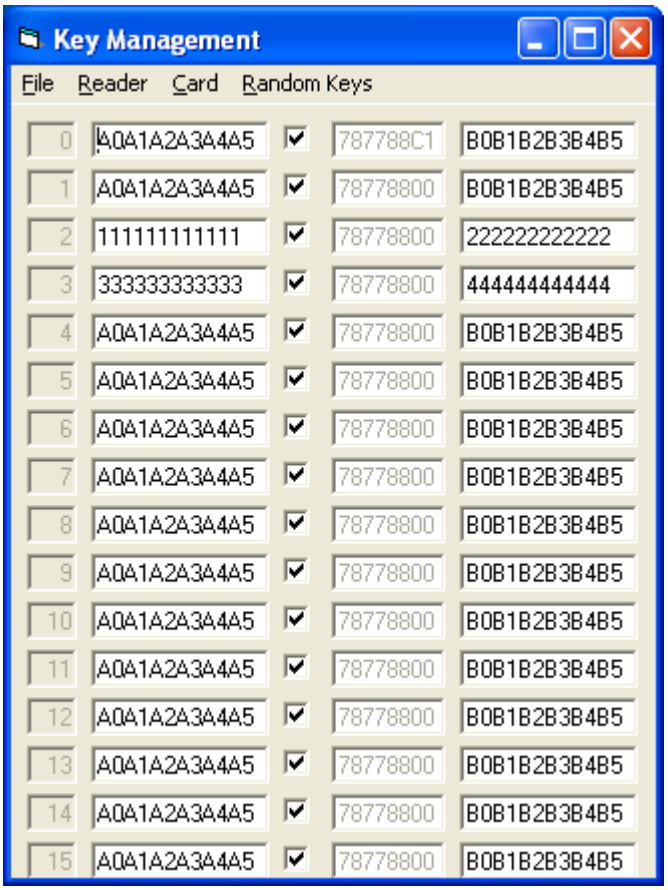
For the HP3000, application sector 2 and 3 are used to store the information. It is possible to use different sector pairs if 2 and 3 are already in use in your project. When a different set of sectors needs to be used we need to have this information when ordering the readers.

It is even possible to use a mix of sectors on user cards. For example, one set of cards uses sector 2 and 3 and another set of cards uses sector 12 and 13. This can be necessary after mergers of companies where one set of user cards already uses sector 2 and 3 for other applications.

User Cards: Initialization

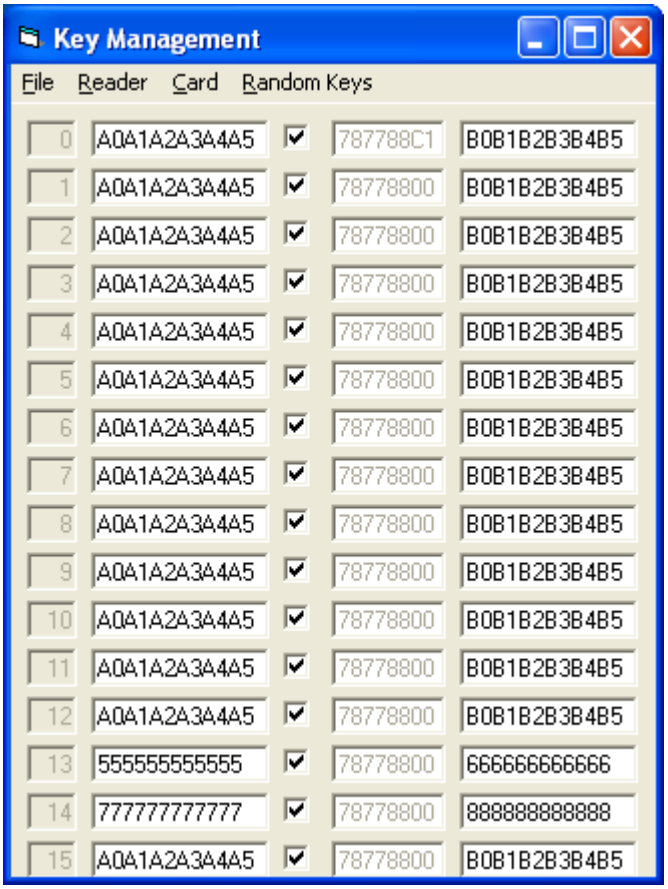
Preparing the MIFARE cards for operation in a project requires the following aspects:

- Defining a card layout (where on the card will the applications store and retrieve their data?)
- Defining key sets for the user cards
- Initializing the cards (put the keys on the card trailers). Take note, that sector 2 and 3 have read access with Key A and write access with key B.
- Initializing the cards for the different applications (put startup information on the card)



Keyset for type 1 cards, public keys need to be replaced by keys relevant to your project. (right)

Keyset for type 2 cards, public keys need to be replaced by keys relevant to your project. (right)



User Cards: Existing projects

When user cards are already in use in your project, they are probably already initialized. However, it should be checked that sector 2 and 3 are secured with for this project unique MIFARE keys. Also, check if there is read access with Key A and write access with key B.

User Cards: New Projects

When user cards are being bought off the factory, they need to be initialized. From the factory, the cards are unprotected and they have public keys that are known to everyone that works with MIFARE cards. Before handing out the cards to the users, all sectors will need to be protected with secret project keys. This initialization process can be done with the SmartEncoder software and reader or any other software from different manufacturers. More information on how to initialize cards can be found in the SmartEncoder manual.

Optional SmartEncoder Software

Software

Defining key sets and writing them to project cards can be done on site, through the use of the software package: “Smart Encoder”. In the software, MIFARE keys will have to be defined to be used for the sectors **2** and **3.** The Standard Key management screen can be used to define keys A and B for sectors 2 and 3 the key set has to be saved to the Project Card, presenting the card to the smartcard readers in the project will upload the new user card keys to the reader.

Step I

To start, you need to have a working combination of Smart Encoder 8 software on a PC with the desktop MIFARE reader powered up and connected to the RS232 port.

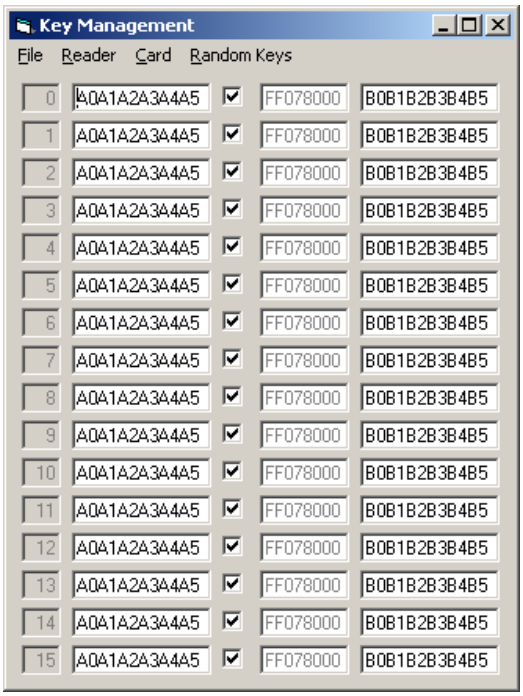
At start-up of the software, the message “Detected ISI Reader” should be shown in the startup screen of the software. When the reader is detected by the software, the green LED will light up.

Step II

The first step is to define keys A and B for the sectors 2 and 3 (these are the sectors the HandReader uses for storing and retrieving information).

Choose **File**, **Key Management** from the main menu, the next screen on the right should show:

Standard the public key set I is shown in this screen. With File open other key sets can be edited and saved.

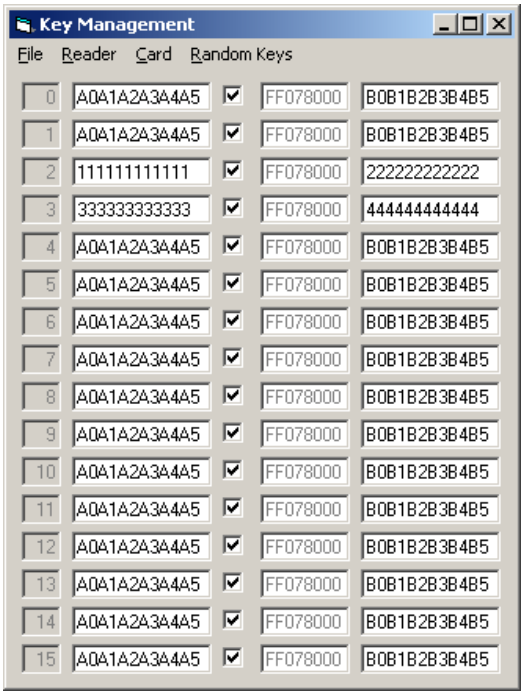


The relevant keys should be typed in HEX format (0 – 9, A – F) on position 2 and 3. The first key is the “A” key for reading information the second the “B” key for writing information to the card. The field in the middle is the access conditions for the sector. For our purpose: Key Upload they are not relevant.

As an example the keys “111111111111” are typed as key A for sector 2 and “222222222222” as key B for sector 2.

“333333333333” key A to sector 3 and “444444444444” as key B for sector 3.

When the keys are defined, the new key set can be stored on a floppy disk with **File**, **Save As**. Store the keys in a secure place!



Step III

The Key Set with the relevant keys for sector 2 and 3 need to be transported to the HandReader, this is done by means of the project specific Project Card. Put the Project Card on the IOLAN Desktop Reader. and choose option **Card**, **Save To Card** the key background will light up green and the key set is stored.

Step IV

Present the Project Card to the powered up HandReader, the card will be recognized by the IOLAN reader and the keys will be uploaded to the MIFARE module. A beep and Yellow LED can be heard and seen after a successful upload.

The key upload process can be repeated indefinitely with different keys.

Step V

The user cards for the project should have the right keys for this project on sectors 2 and 3. The access conditions for sector 2 and 3 should allow **read with key A** and **write with key B**. See the Smart Encoder manual for instructions. For example the settings “78778800” will work with this application.