IrisAccess™
Advanced Identity Authentication

LG
The iris identity experts.™

LG IrisAccess™ Smart Card Integration

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by LG Electronics USA
Incorporated. LG Electronics USA Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this document.
Please remember that existing images or drawings that you may want to include in your document may be protected under copyright law. The unauthorized incorporation of such material into your work could be a violation of the rights of the copyright owner. Please be sure to obtain any permission required from the copyright owner.
LG, LG Iris, the LG logo, LG Iris logo and IrisAccess are either registered trademarks or trademarks of LG Electronics Incorporated in the United States and/or other countries.

LG Electronics USA Incorporated, Iris Technology Division. 7 Clarke Drive, Cranbury, New Jersey 08512, USA.
Created: November 1, 2006

www.lgiris.com

Table of Contents

1. Introduction

Using smart cards with the LG IrisAccess™ system provides greater flexibility by allowing the user to carry their iris biometric templates with them. Making the iris templates portable, allows iris verification to take place at remote locations where the standard IrisAccess DB or connecting infrastructure may not be available.

With the iris templates stored only on the smart card this can eliminate privacy concerns because the iris templates will not be stored in a central database.

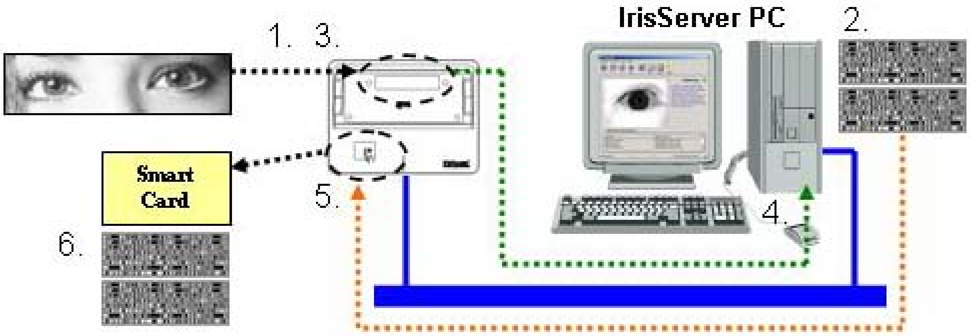
Smart card enrollment uses the IrisEnroll application, which is part of the EAC software. With a smart card reader/writer connected to the enrollment computer, or iCAM, and the system is configured for smart card operation, the enrollment operator can choose to store the users' iris template on a smart card, in the IrisAccess database, or both.

This document describes the hardware and software configuration used with the iCAM4000 / 4100 and LG 3000 series iris cameras in enrollment or verification modes using EAC v2.03 or higher software. The LG IrisAccess™ system supports HID iClass, Integrated Engineering Smart ID, MiFare, and DESFire smart cards.

Before adding smart cards, the LG IrisAccess™ system hardware and software should be installed and tested to be fully operational in identification mode. For instructions on how to install and setup the LG IrisAccess™ hardware and software for a base system using the ICU4300, please refer to the Hardware and Software manuals included on the EAC software CD. If using the older ICU3000 hardware for control of the ROU3000 iris cameras, refer to the "LG IrisAccess™ 3000 Smart Card Installation and Operation" document.

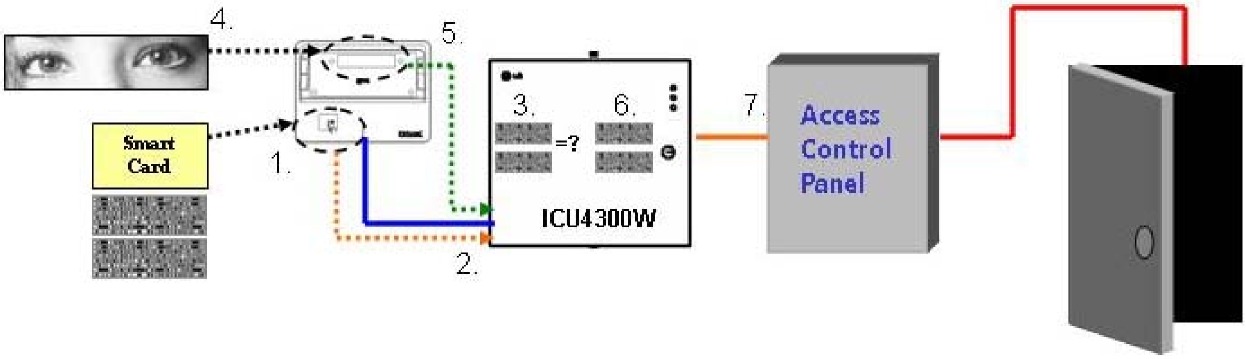
2. Operational Overview – Smart Cards

2.1 Enrollment



1. The enrollment operator puts the EAC software in enrollment mode; the user presents their iris(es) to the enrollment iris camera.
2. The iris images are transmitted to the enrollment software which selects the best images which are then converted to 512 byte IrisCodes®.
3. The user then presents their iris(es) again to verify a good enrollment.
4. Once the enrollment of the user has been verified, the operator enters the users' information into the system. The operator can choose to save the users enrollment (IrisCodes® and information, including Card ID) in the Iris Server database and/or a Smart Card.
5. If the operator selects to issue a smart card, the card is placed near the smart card reader for encoding. The smart card is written then verified, the user is asked one last time to present their iris(es) to the camera to verify the card was encoded properly.
6. The smart card now contains a copy of the users' IrisCodes® and Card ID.

2.2 Recognition



1. The user presents their smart card to the smart card reader.
2. IrisCode® data and Card ID is read from the smart card and communicated to the ICU.
3. The IrisCodes® and Card ID are temporarily stored in ICU memory.
4. The user is then prompted to present their iris(es) to the iris camera.
5. The newly captured iris images are transmitted to the ICU.
6. The software selects the best images to be converted to a set of 512 byte IrisCodes®. The system will then compare the IrisCodes® created from the image to the IrisCodes® from the smart card.
7. Upon a positive match the door relay (if the ICU is connected to a DCU) is activated which releases the door lock, and/or the users Card ID is sent via Wiegand to an external access control panel.

3. Required Equipment

3.1 Software

LG IrisAccess™ Entry Access Control (EAC) software v2.03 or higher

3.2 Hardware

The minimum system required for performing iris enrollments to smart cards is:

- **Computer** – required for controlling the iris camera used for enrollments and smart card encoding.

- **Iris Camera** – to capture iris images

- **Smart card reader/writer** – to encode and read the smart cards **- not required if using an iCAM iris camera with built in smart card reader.**

- **FGB3000** (PCI Frame Grabber Board) – captures video from the LG 3000 series iris camera – **Only required when using a LG 3000 series iris camera for enrollment.**

Additional equipment may be required for iris / smart card verifications and communications with other access control devices.

- **Additional Iris Camera** – can be installed at entry locations and controlled by ICU for verification only.

- **Additional Smart Card Readers** – either built-in the iCAM or external. One for each entry where smart card verification is required.

- **ICU4300** – controls iris cameras and provides input and output communications for card readers and access control panels. Supports up to 4 iCAMs or 2 LG 3000 series iris cameras with smart card per ICU.

- **DCU4000** – controlled by the ICU, the DCU provides additional input and output communication options including relays for door control. (not typically used with an access control panel)

Refer to the IrisAccess™ 3000 and 4000 Hardware Manuals for more detailed information on hardware and system requirements.

3.2.1 Computer

When used with an iCAM 4000/4100 iris camera with an integrated smart card reader.

Minimum Computer Requirement (iCAM with built-in smart card reader):
Pentium 4 compatible1.6Ghz
Microsoft Windows 2000 Pro, 2000 Server, XP Pro, or 2003 Server OS
256Mb RAM
10/100 Ethernet Port

When used with an iCAM 4000/4100 iris camera and an external smart card reader/writer, the computer will require a serial or USB port (depending on the smart card reader)

Minimum Computer Requirement (iCAM with external smart card reader):
Pentium 4 compatible1.6Ghz
Microsoft Windows 2000 Pro, 2000 Server, XP Pro, or 2003 Server OS
256Mb RAM
10/100 Ethernet Port
1 Serial or USB Port (as required by the card reader)

When a 3000 series iris camera will be used for enrollments along with an external smart card reader/writer, the computer will require a FGB3000 (Frame Grabber Board) installed and two available serial ports.

Minimum Computer Requirement (EOU3000 with external smart card reader):
Pentium 4 compatible1.6Ghz
Microsoft Windows 2000 Pro, 2000 Server, XP Pro, or 2003 Server OS
256Mb RAM
10/100 Ethernet Port
1 Open full height, half length PCI Card slot (for installation of FGB3000)
1 Serial Port for connection to EOU3000 (USB-to-Serial is not acceptable)
1 Serial or USB Port (as required by the card reader)

3.2.2 Iris Camera

iCAM 4000 / 4100
iCAMs are available with an integrated smart card reader. The following sub models of iCAM have the smart card reader built-in:

HID iClass smart card reader (iClass only)
iCAM 4110-H3 (includes display and HID iClass reader, no keypad)
iCAM 4111-H3 (includes display, keypad, and HID iClass reader)

Integrated Engineering Smart-ID smart card reader (MiFARE and DESFire)
iCAM 4010-E1 (small form factor camera with IE smart card reader)
iCAM 4110-E1 (includes display and IE smart card reader, no keypad)
iCAM 4111-E1 (includes display, keypad, and IE smart reader)

Note: iCAMs with a built-in smart card reader will have a card reader icon on the front cover of the unit.

The iCAM has a built in “Smart Card Reader IF” serial port for the connection of an external smart card reader. This reader interface can supply 12VDC and uses serial communications. Note: Not all smart card readers are supported by the iCAM software. Refer to the www.lgiris.com support site for the latest list of supported smart card readers.

EOU/ROU 3000

The 3000 series of iris camera requires an external smart card reader. The 3000 will support three different smart card reader types: HID iClass, Indala DESFire, and BQT (Banquetec) MiFARE. Smart card readers used with the 3000 series for enrollment must be connected to the enrollment computer. Refer to the IrisAccess™ 3000 smart card document for connection details of the enrollment smart card reader, and if an ICU3000 will be used with the 3000 iris camera. This document will cover connection of the smart card readers to the ICU4300 only.

HID iClass:
HID RW400 iClass Smart Card Reader / Writer - RS232 serial and Wiegand output is required. One card reader/writer is required for each enrollment computer. One card reader is required for each 3000 to be used in smart card mode.

Indala DESFire:
Indala DESFire Smart Card Reader / Writer - RS232 serial output only. One card reader/writer is required for each enrollment computer. One card reader is required for each 3000 to be used in smart card mode.

BQT Solutions (Banquetec) MiFARE:
BQT BT-815 Smart Card Reader / Writer - RS232 serial output only. One card reader/writer is required for each enrollment computer. One card reader is required for each 3000 to be used in smart card mode.

Important Note: All of the supported smart card readers use RS232 serial communications to transfer the smart card data. RS232 has a maximum distance limitation of 50 feet (15 meters). To extend this distance will require converting the RS232 to a different serial communication method such as RS422.

A pair of RS422 converters may be required for each smart card reader channel. Contact the smart card reader or RS232 to RS422 converter manufactures for more information and specifications.

3.2.3 Smart Cards

HID iClass - iClass 200 base model Cards Either the 2001 (16k/2) or 2002 (16k/16) models are acceptable; must be pre-programmed.

Indala DESFire - Indala DESFire smart cards. Must be pre-programmed.

BQT MiFARE - BQT Solutions MiFARE smart cards. Must be pre-programmed.

IE MiFARE DESFire – 4K Cards

4. Hardware Connections

4.1 iCAM with Integrated Smart Card Reader

The iCAM 4000 / 4100 is available with an integrated smart card option. When a card reader has been installed at the factory, no additional wiring is required for the smart card reader. Refer to the Required Hardware section of this document for the list of iCAM sub-models which have a built-in smart card reader.

Note: An iCAM with a card reader icon on the front cover has a smart card reader installed in the unit.

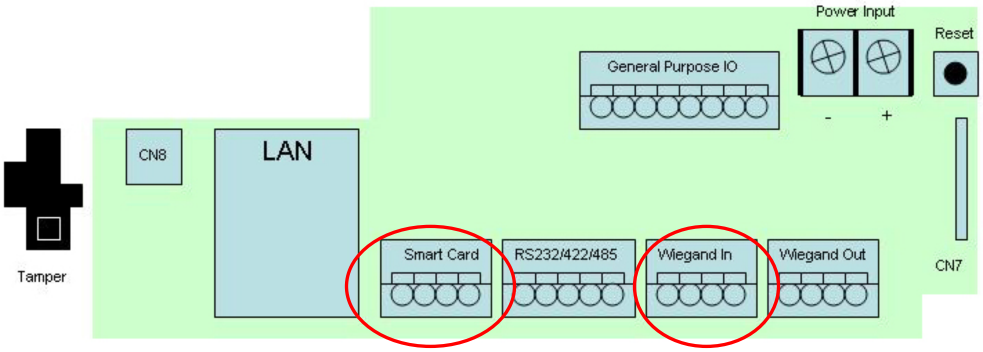
4.2 iCAM with External Smart Card Reader

If an external smart card reader is required, the iCAM has a built in “Smart Card Reader IF” serial port. This reader interface can supply 12VDC to power the card reader and uses RS-232 serial to communicate with the reader.

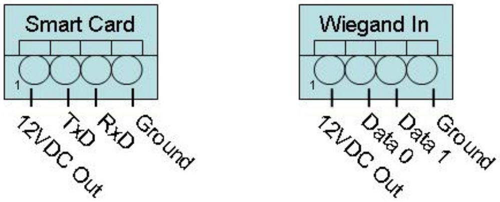
The iCAM also has a Wiegand input connection for the iClass smart card reader which uses Wiegand communications for the Card ID as well as serial for the smart card data.

Both the iCAM4000 and iCAM4100 have a Smart Card and Wiegand input interface built-in.

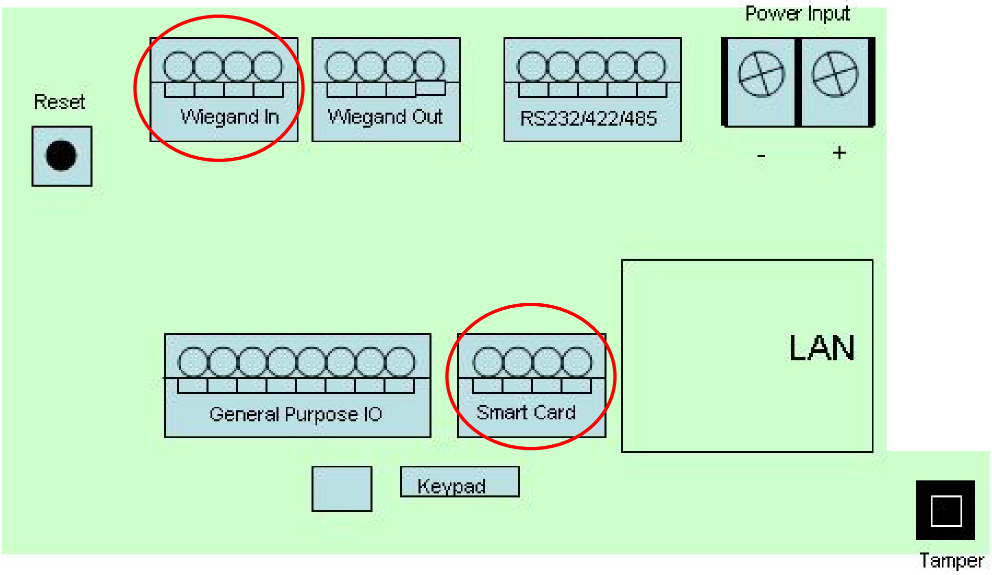
iCAM4000 Interface Connections



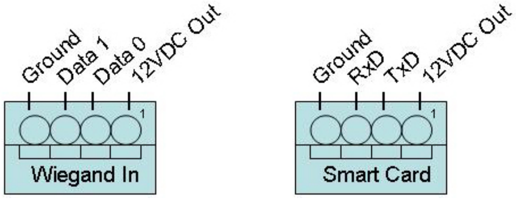
iCAM4000 Connection Details



iCAM4100 Interface Connections



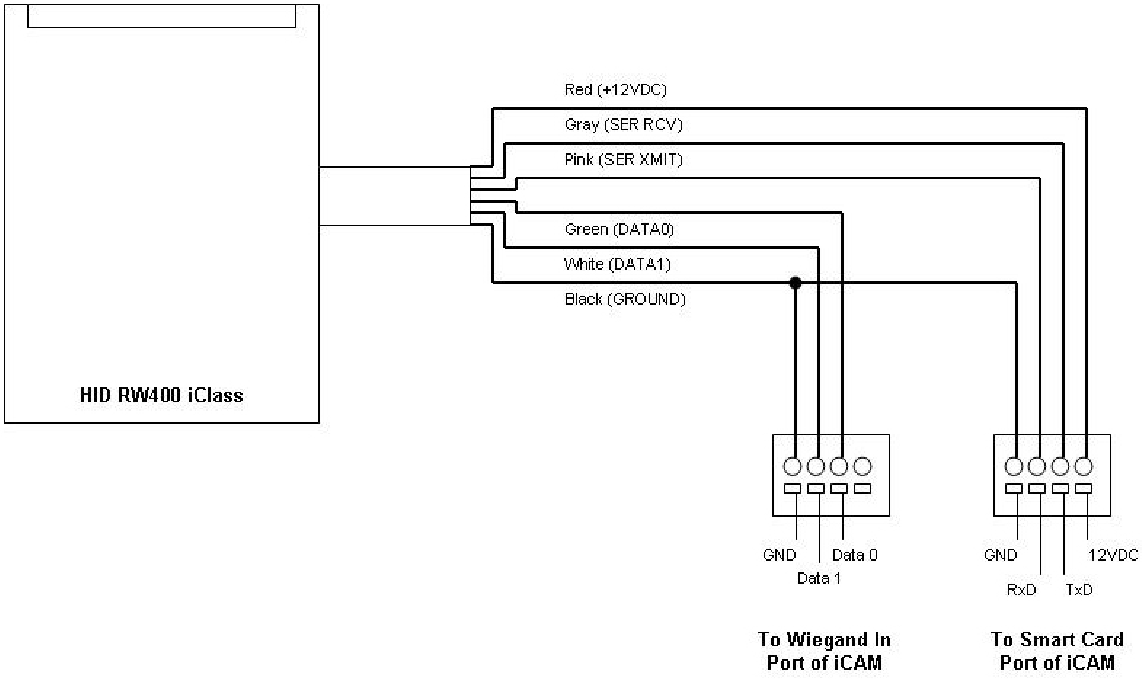
iCAM4000 Connection Details



Note: Although the connectors on the iCAM4000 and iCAM4100 are "flipped" from each other, the pin functions are the same. A connector wired for a 4000 will work in a 4100 with no modifications needed. The installed orientation is the only difference.

4.2.1 External HID iClass RW400 to iCAM wiring. Serial, Wiegand, and Power

Below is the wiring for an HID RW400 iClass smart card reader for connection to the iCAM.



HID iClass RW400 wired for connection to the iCAM

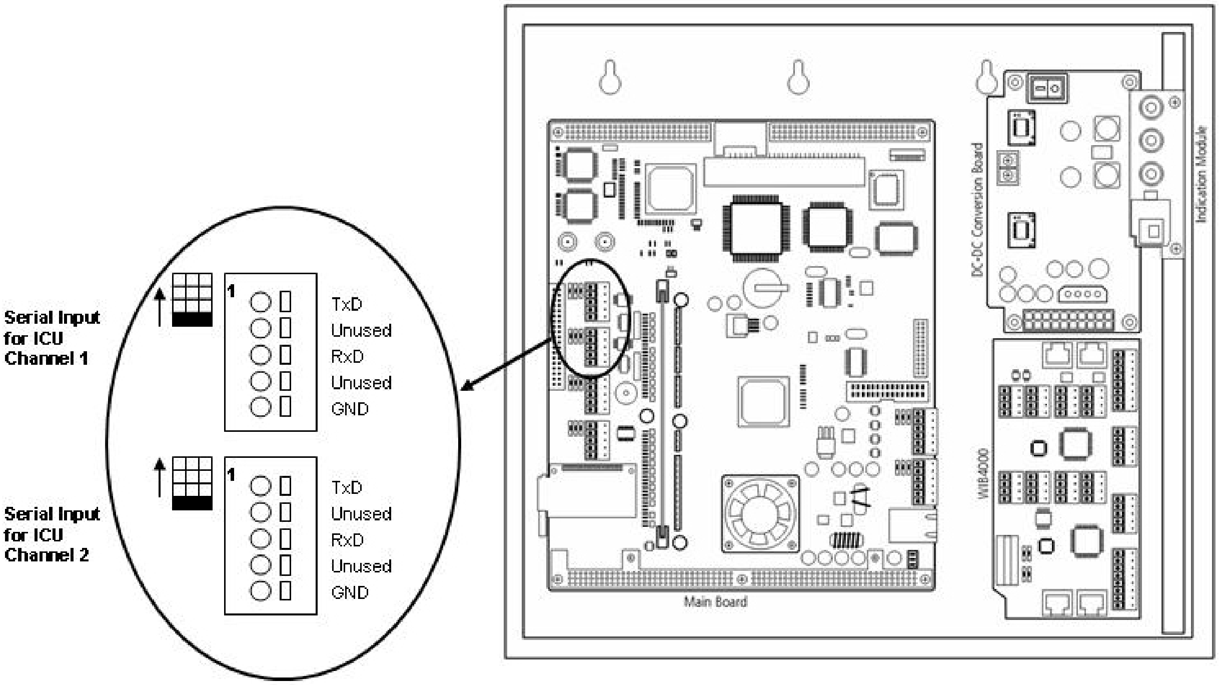
4.3 ROU3000 with External Smart Card Reader to ICU4300

When using ROU3000 iris cameras, all smart card connections are made at the ICU4300. If using the ICU3000 please refer to the “IrisAccess™ 3000 Smart Card Installation and Operation Manual”

Important Note: All of the supported smart card readers use RS232 serial communications to transfer the smart card data. RS232 has a maximum distance limitation of 50 feet (15 meters). This distance can be extended by converting the RS232 serial to a different serial communication method such as RS422.

A pair of RS422 converters may be required for each smart card reader channel. Contact the smart card reader or a RS232 to RS422 converter manufacturer for more information and specifications.

Smart Card Serial Ports in the ICU4300

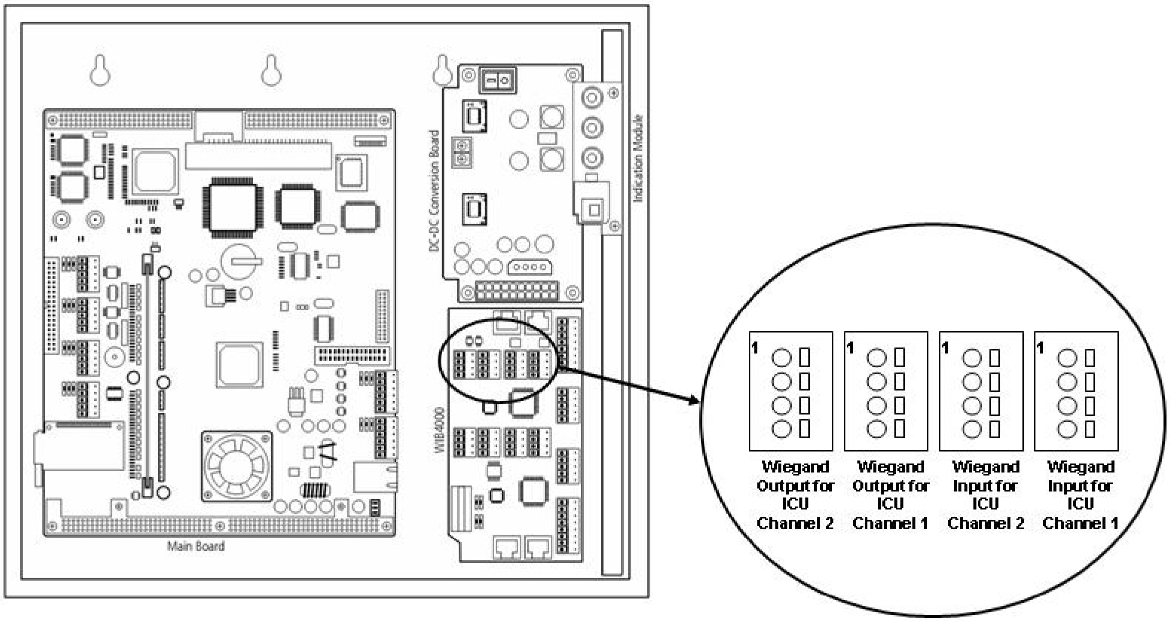


Note: All DIP switches must be in the up position for RS232 communications.

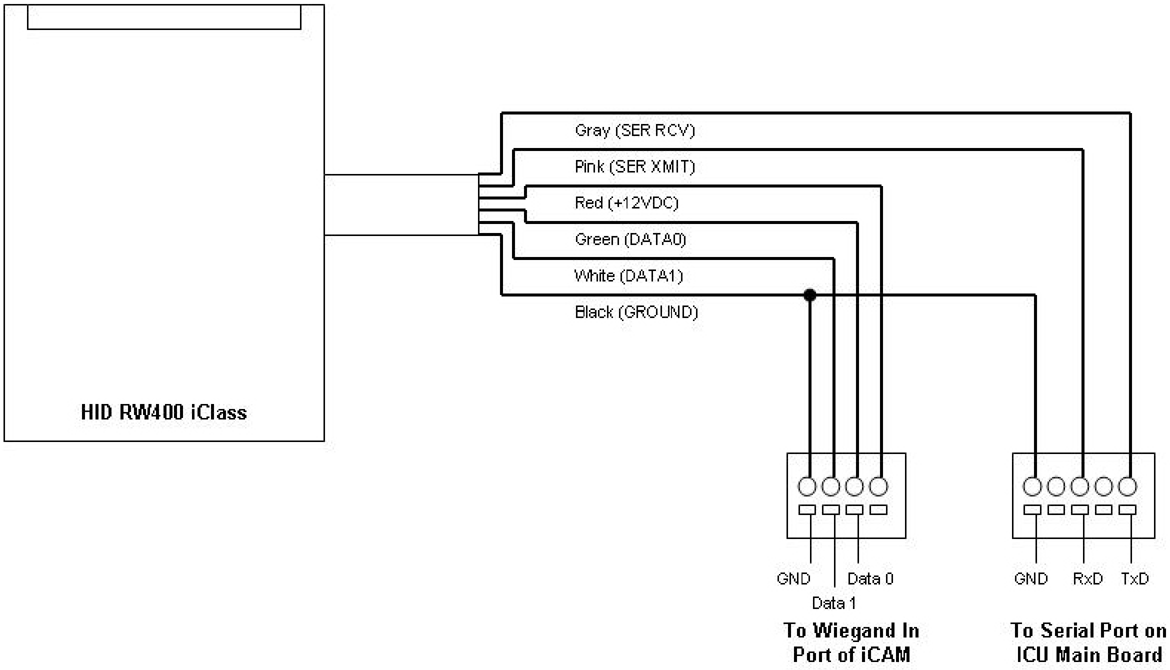
ICU4300s equipped with a WIB4000 board (ICU4300-2W or ICU4300-4W), can supply 12VDC power to the card reader(s). The WIB also provides Wiegand input connection for card readers such as the HID iClass RW400.

Note: Smart Card readers can be powered by the WIB Wiegand input ports Pin 1 and 4 or from an external power source.

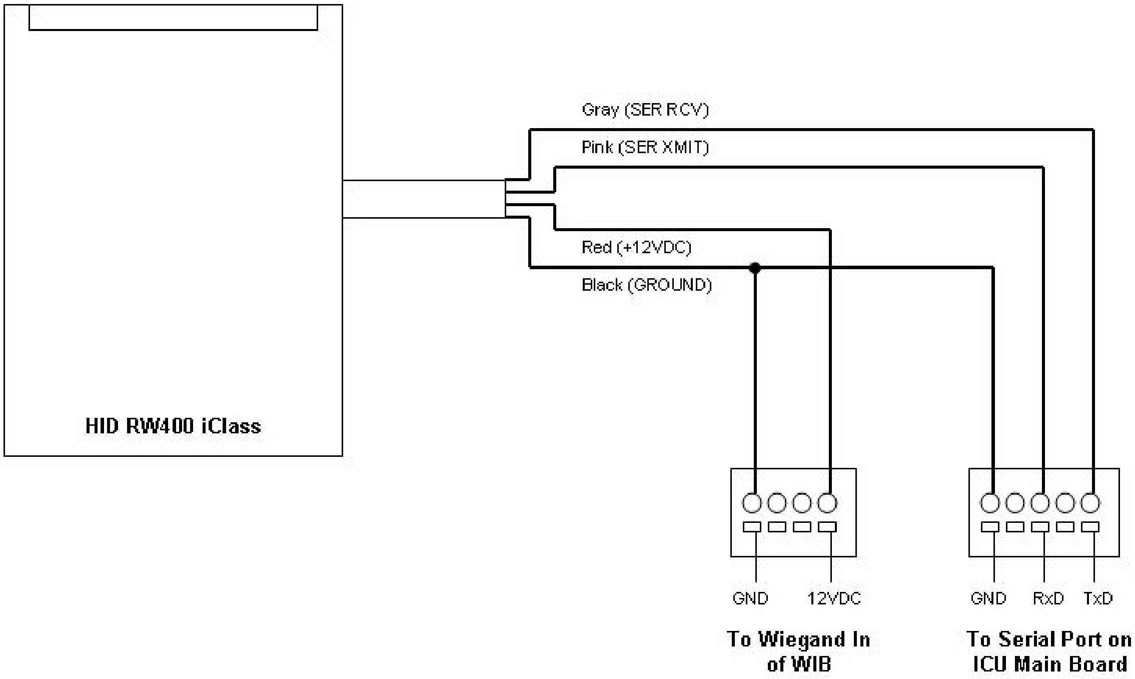
Wiegand Input Connections of WIB4000


Main Board
DC-DC Conversion Board
WIB4000
Indication Module
1
1
1
1
Wiegand Output for ICU Channel 2
Wiegand Output for ICU Channel 1
Wiegand Input for ICU Channel 2
Wiegand Input for ICU Channel 1

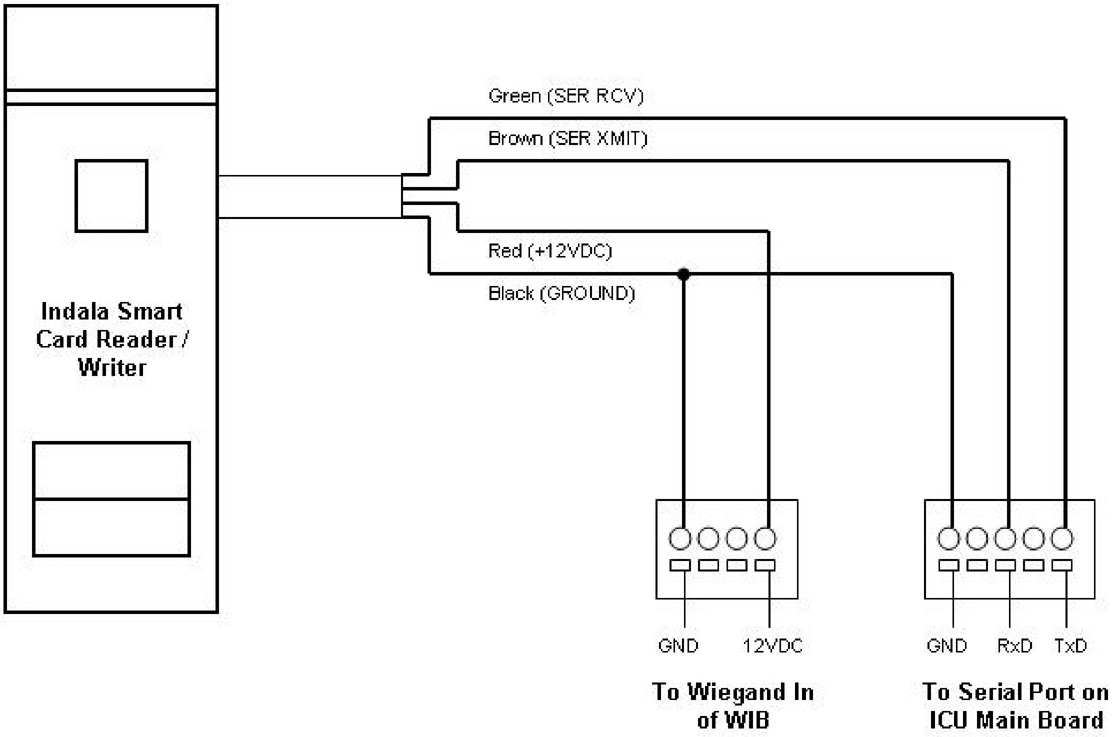
4.3.1 HID iClass RW400 to ICU4300 with Wiegand, Serial, and Power



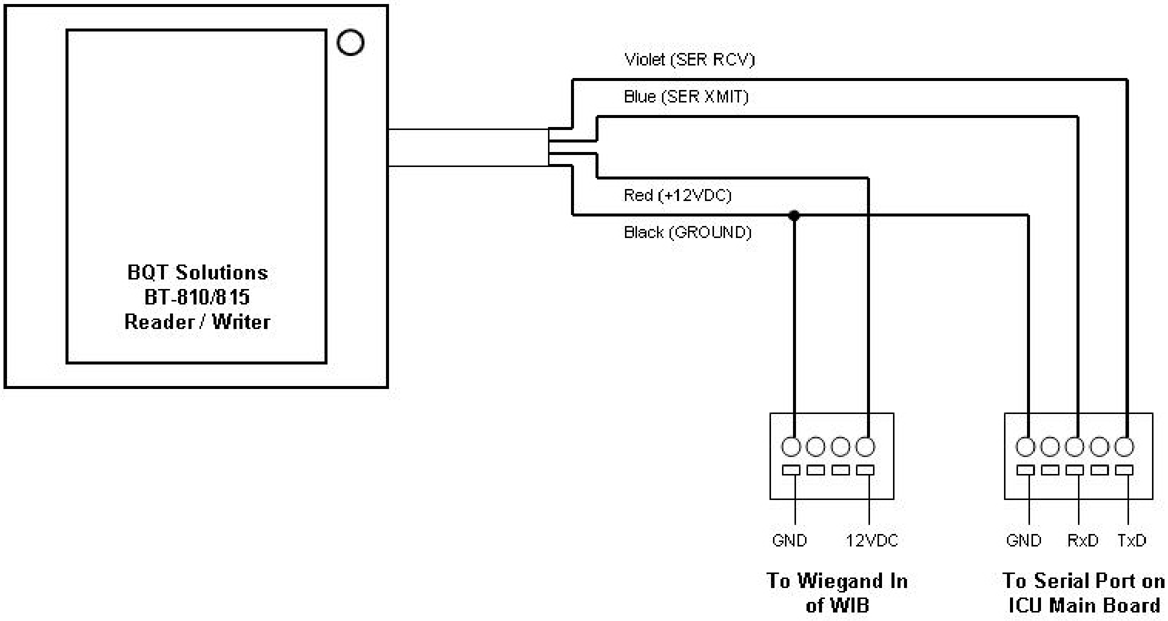
4.3.2 HID iClass RW400 to ICU4300 Serial and Power Only



4.3.3 Indala DESFire Reader to ICU4300 Serial and Power Only



4.3.4 BQT BT-815 Reader to ICU4300 Serial and Power Only



5. Software Configuration for Smart Cards

5.1 Creating an Iris Template Encyption Key Set

For greater security it is recommended that the iris template stored on the smart card is encrypted. The IrisAccess software includes an encryption key generator which can be used to create a key set. The encryption key set can then be applied to the iris enrollment stations and the ICUs for encoding and decoding the iris template encryption on the smart card.

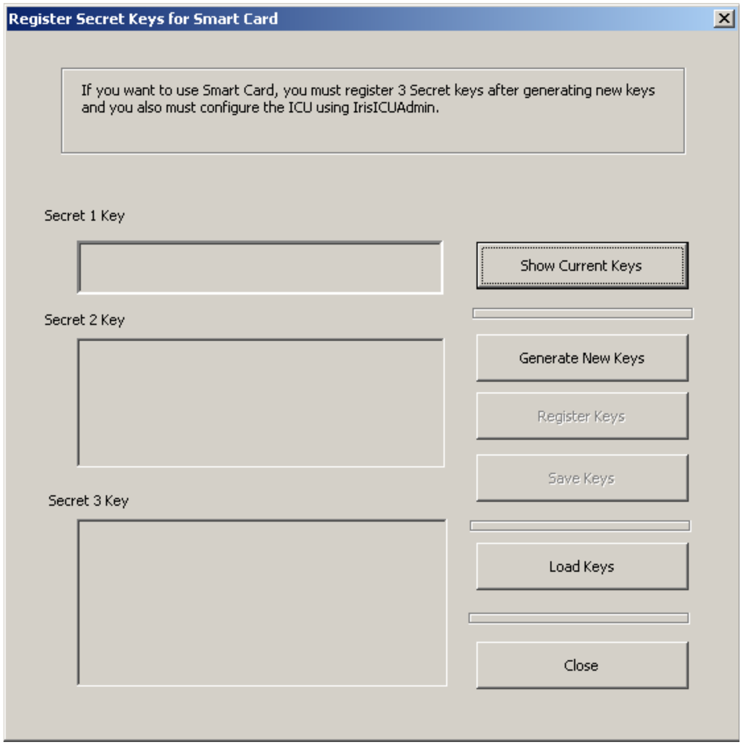
Note: If the format of the smart card will be in GCS-IS with no encryption, DO NOT create or register encryption keys.

Encryption key generation

To create and register the encryption key set:

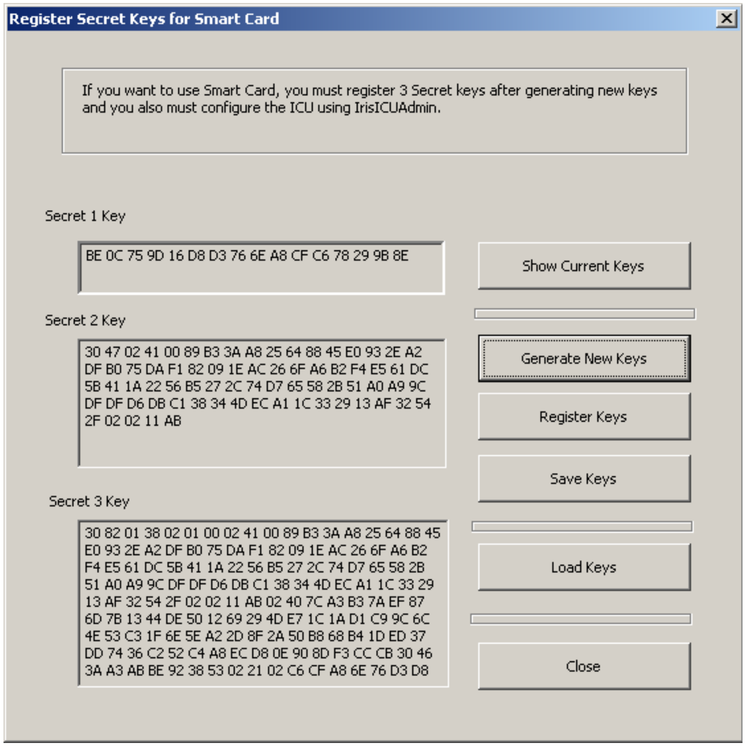
1. Open IrisServer.
2. Enter ID and Password (Default ID = administrator, password = iris3000)
3. Select **Option > Set Smart Card** item in the menu bar of the IrisServer,

The Register Secret Keys for Smart Card window will appear**.**



If you want to use Smart Card, you must register 3 Secret keys after generating new keys and you also must configure the ICU using IrisICUAdmin.

4. Click the **Generate New Keys** button to create new keys.



Register Secret Keys for Smart Card

If you want to use Smart Card, you must register 3 Secret keys after generating new keys and you also must configure the ICU using IrisICUAdmin.

Secret 1 Key

```
BE 0C 75 9D 16 D8 D3 76 6E A8 CF C6 78 29 9B 8E
```

Secret 2 Key

```
30 47 02 41 00 89 B3 3A A8 25 64 88 45 E0 93 2E A2
DF B0 75 DA F1 82 09 1E AC 26 6F A6 B2 F4 E5 61 DC
5B 41 1A 22 56 B5 27 2C 74 D7 65 58 2B 51 A0 A9 9C
DF DF D6 DB C1 38 34 4D EC A1 1C 33 29 13 AF 32 54
2F 02 02 11 AB
```

Secret 3 Key

```
30 82 01 38 02 01 00 02 41 00 89 B3 3A A8 25 64 88 45
E0 93 2E A2 DF B0 75 DA F1 82 09 1E AC 26 6F A6 B2
F4 E5 61 DC 5B 41 1A 22 56 B5 27 2C 74 D7 65 58 2B
51 A0 A9 9C DF DF D6 DB C1 38 34 4D EC A1 1C 33 29
13 AF 32 54 2F 02 02 11 AB 02 40 7C A3 B3 7A EF 87
6D 7B 13 44 DE 50 12 69 29 4D E7 1C 1A D1 C9 9C 6C
4E 53 C3 1F 6E 5E A2 2D 8F 2A 50 B8 68 B4 1D ED 37
DD 74 36 C2 52 C4 A8 EC D8 0E 90 8D F3 CC CB 30 46
3A A3 AB BE 92 38 53 02 21 02 C6 CF A8 6E 76 D3 D8
```

5. Once the keys are created, click the **Register Keys** button.
   - **Keys must be registered before using IrisEnroll**

6. Click the **Save Keys** button to save the keys in a .dat file. This file will be needed during the configuration of the ICUs.

Note: The encryption key generated and registered here is used to encrypt the iris data on the smart card. This key must be registered in the IrisAccess DB by clicking on **Register Keys**. The keys must also be registered in each ICU that will be required to recognize the smart cards generated by this IrisAccess system. If a different key is later registered, all previous smart cards created with the old key will not longer be able to be read by the system.

5.2 Configuring the IrisAccess™ Software for use with iCAMs

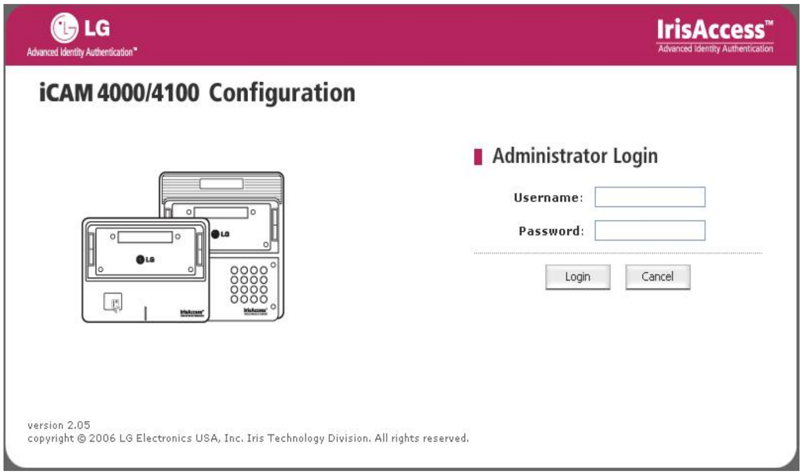
5.2.1 Configuring the iCAM for Smart Cards

When used with a smart card reader the iCAM Smart Card Port must be enabled and configured. Each iCAM that has a smart card reader installed must be configured.

To configure the iCAM for smart cards:

Using Internet Explorer, log into the iCAM web interface by entering in the IP Address for the iCAM in the web browser address bar. (ex. http://192.168.5.100)

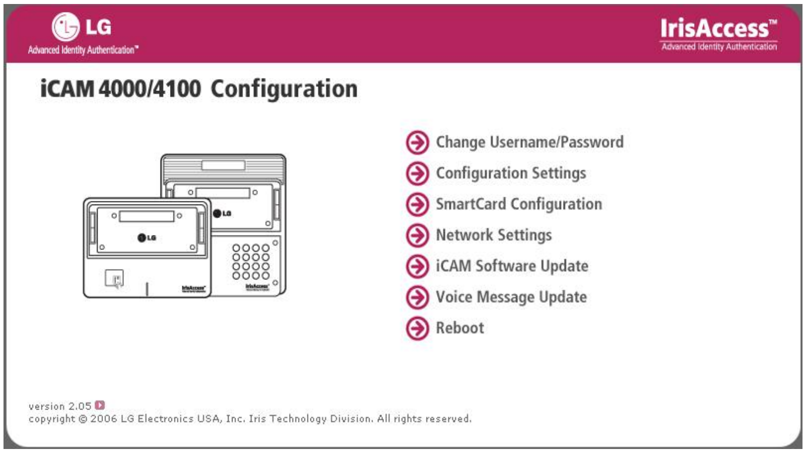
The iCAM web configuration interface logon screen will appear.


LG
Advanced Identity Authentication™
IrisAccess™
Advanced Identity Authentication
iCAM 4000/4100 Configuration
Administrator Login
Username:
Password:
Login
Cancel

version 2.05
copyright © 2006 LG Electronics USA, Inc. Iris Technology Division. All rights reserved.

Enter the iCAM web interface login username and password.
Default Username = iCAM4000
Default Password = iris4000

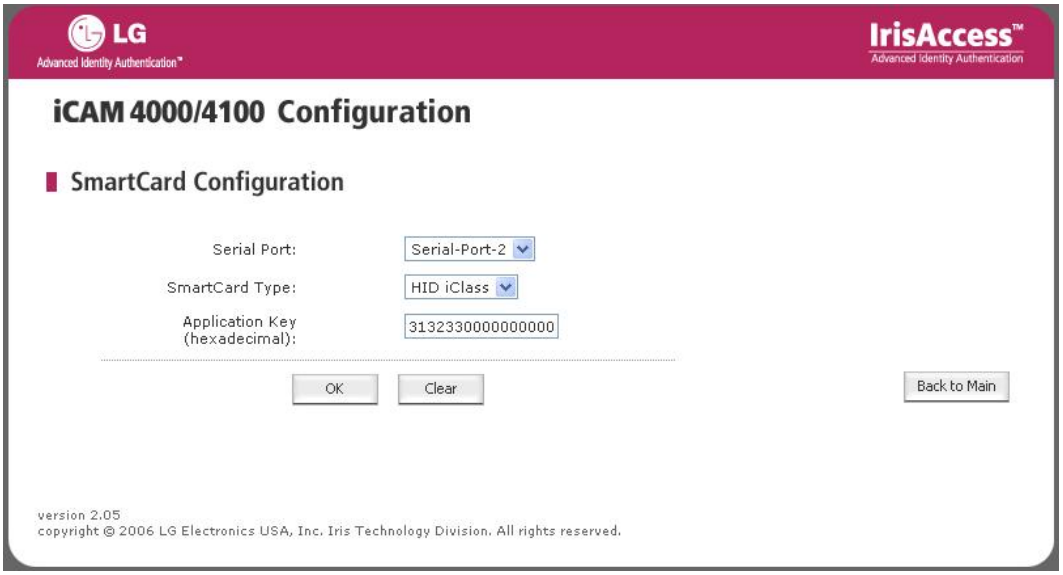
The iCAM main menu will display:



version 2.05
copyright © 2006 LG Electronics USA, Inc. Iris Technology Division. All rights reserved.

From the iCAM Main Configuration Menu, select SmartCard Configuration.

The SmartCard Configuration will display:


LG
Advanced Identity Authentication™
IrisAccess™
Advanced Identity Authentication
OK
Clear
Back to Main

iCAM 4000/4100 Configuration

SmartCard Configuration

Serial Port: Serial-Port-2

SmartCard Type: HID iClass

Application Key (hexadecimal): 3132330000000000

version 2.05
copyright © 2006 LG Electronics USA, Inc. Iris Technology Division. All rights reserved.

Three parameters are selectable:

Serial Port – The serial port of the iCAM where the smart card reader is connected.

- None (serial ports disabled)
- Serial-Port-1 (not currently supported)
- **Serial-Port-2 ("Smart Card Reader IF" port)**

Select Serial-Port-2

SmartCard Type – The type of smart card reader connected to the iCAM.

- HID iClass – Installed iClass module or external RW400 (use with iClass cards)
- MIFARE – Installed IE Module or external MiFARE reader (use with MIFARE cards)
- SMART ID – Installed IE Module or external IE Smart-ID reader (use with DESFire cards)

Select the type of smart card reader connected to the iCAM.

Application Key – **For HID iClass Card Readers Only –** The application key used to unlock the iClass card. **All iClass readers in the system must have identical application keys**.

Enter the application key used for the iClass cards.

Click OK to enter changes and exit the SmartCard configuration.

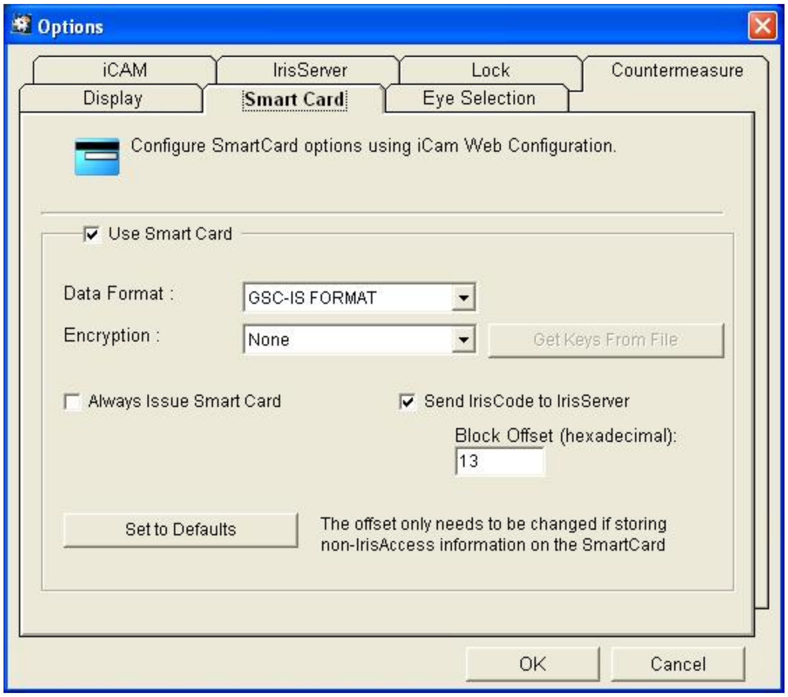
The configuration must be repeated for each iCAM with a smart card reader.

5.2.2 Configuring IrisEnroll4000 for Smart Cards with iCAM

IrisEnroll4000 is used to control the iCAM for iris enrollment and smart card generation. IrisEnroll4000 must be configured for smart card operation.

1. Open IrisEnroll4000
2. Enter ID and Password (Default ID = administrator, password = iris3000)
3. Enter the IP Address of the iCAM used for enrollment, click Connect
4. After the iCAM has connected select **Options**
5. Select the **Smart Card** tab

The Options Smart Card window will appear.



Configure SmartCard options using iCam Web Configuration.

☑ Use Smart Card

Data Format : GSC-IS FORMAT

Encryption : None

□ Always Issue Smart Card

☑ Send IrisCode to IrisServer

Block Offset (hexadecimal): 13

The offset only needs to be changed if storing non-IrisAccess information on the SmartCard

6. Select the check box for **Use Smart Card.**
7. Select the **Data Format**:

- **IA EAC Format** = IrisAccess EAC smart card format (AES Encryption only), **iClass only**.
- **GSC-IS Format** = Government Smart Card Interoperability Standard format.

8. Select **Encryption** (GSC-IS format only):

- **None =** The iris data will not be encrypted
- **AES** = Advanced Encryption Standard
- **DES** = Data Encryption Standard (**iClass Only**)
- **DES3 =** Triple Data Encryption Standard (**iClass Only**)

Note: The encryption key set (.dat file) created must be loaded if encryption is selected. This same key file must used for each ICU channel and ICU in the system.

9. Always Issue Smart Card – check this box if all enrollments at this station are to be issued a smart card. With this box checked, the Card will automatically be selected, as Smart Card and the smart card writing process will start immediately after enrollment. If this box is unchecked, you will have the option of selecting the type of card (smart, prox, or no card) that will issued for the user. The default of this box is unchecked.

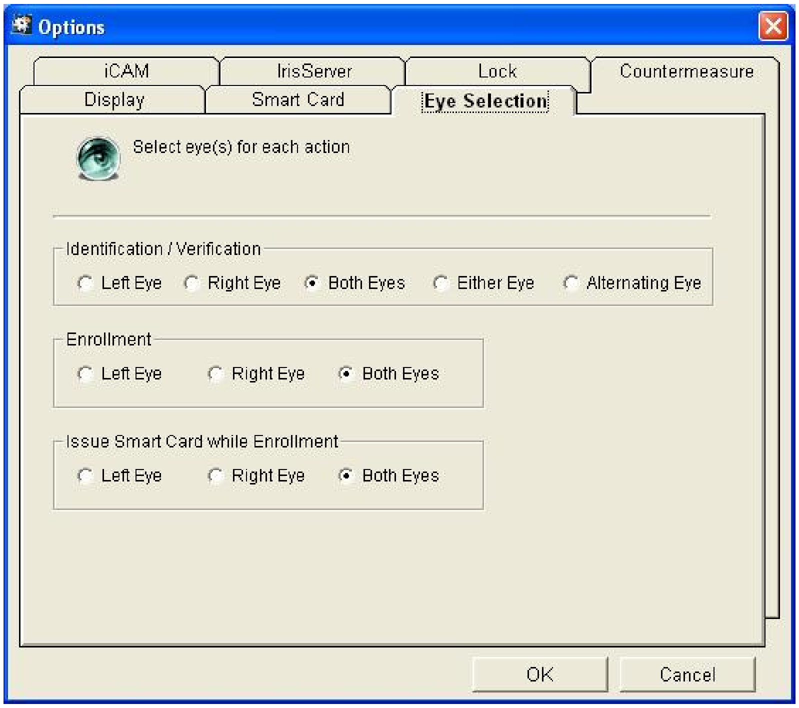
10. Send IrisCode to IrisServer – check this box if copies of the enrolled iris template(s) are to be stored in the IrisAccess DB as well as on the smart card. It is recommended to have enabled so that replacement cards can be issued without requiring re-enrollment of the user. The default is with this box checked.

Note: The following step is applicable only when using HID iClass smart cards storing additional non-iris data on the smart card (example: face or fingerprint data).

11. Block Offset – Location on the smart card where the iris data block starts. Default block offset is 13.

Configuring which iris template will be written to the smart card.

1. Within the IrisEnroll4000 Options, click on the **Eye Selection** tab.
2. Select which eye(s) – iris template will be written to the smart card during enrollment.



Select eye(s) for each action

Identification / Verification
○ Left Eye ○ Right Eye ● Both Eyes ○ Either Eye ○ Alternating Eye

Enrollment
○ Left Eye ○ Right Eye ● Both Eyes

Issue Smart Card while Enrollment
○ Left Eye ○ Right Eye ● Both Eyes

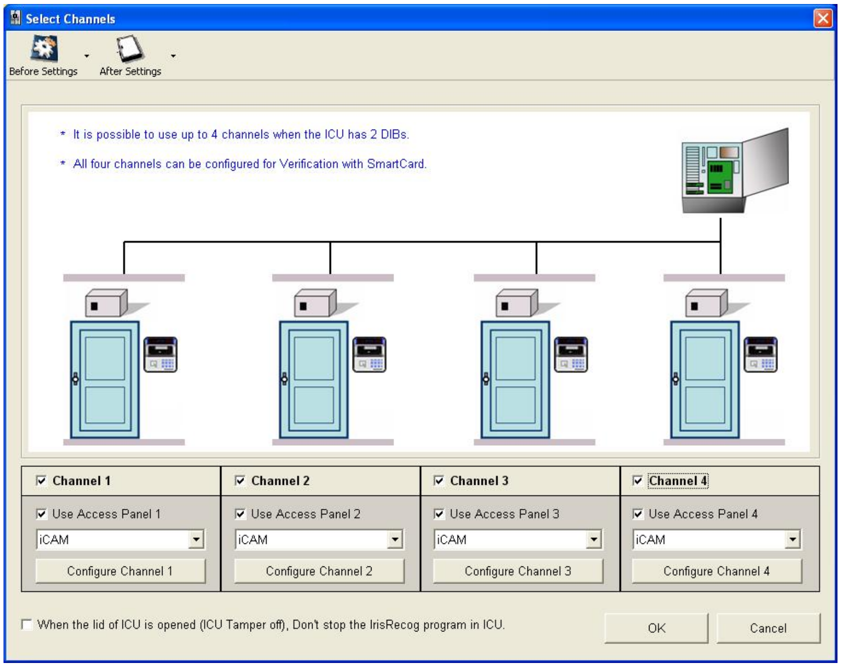
3. Click OK to exit the IrisEnroll4000 Options.

5.2.3 Configuring IrisICUAdmin4000 for Smart Cards with iCAMs

The configuration for smart card operation must be performed on each ICU and each channel that will utilize smart cards. This procedure assumes that the iCAMs are connected and have been tested to be operational in identification mode.

1. Open the **IrisICUAdmin4000** application.
2. Select **Configuration**.
3. At the main ICU configuration screen click on the arrow next to **Before Settings** and choose **Get the settings from an ICU.**
4. Select if you want to save the current configuration displayed on the configuration screen. Typically select No.
5. Enter the IP Address and password (default password = iris4000) for the ICU that is being configured. Click **OK**. The current settings of the ICU will load into IrisICUAdmin4000.

The IrisICUAdmin4000 configuration screen will display with the ICU current configuration.



* It is possible to use up to 4 channels when the ICU has 2 DIBs.

* All four channels can be configured for Verification with SmartCard.

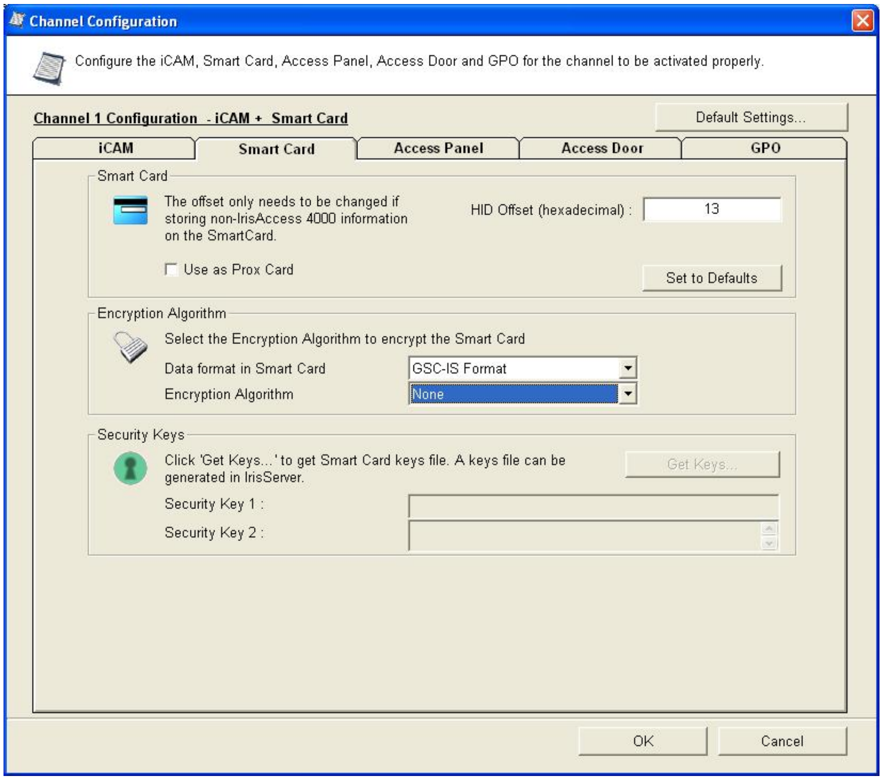
☑ Channel 1	☑ Channel 2	☑ Channel 3	☑ Channel 4
☑ Use Access Panel 1	☑ Use Access Panel 2	☑ Use Access Panel 3	☑ Use Access Panel 4
iCAM	iCAM	iCAM	iCAM

□ When the lid of ICU is opened (ICU Tamper off), Don't stop the IrisRecog program in ICU.

6. For the channel being configured for smart card support, change the drop down box to **iCAM + Smart Card**.
7. Click on **Configure Channel #**. (# = the channel number to configure)
8. Click on the iCAM tab
9. Verification Time Out – The number of seconds allowed between a smart card read and an iris read before the system will time out. Default is 5 seconds.
10. Use Network - When the box is checked for “with IrisServer of EAC S/W”, the ICU will communicate with the IrisAccess DB to check for user

permissions and report back to IrisMonitor the system and user activity that takes place on the ICU. Without this box checked the ICU will act in “stand-alone” mode, allowing all valid smart cards access and not reporting activity back at the server. Permissions in this mode are handled by an external access control system.

9. Click on the **Smart Card** tab to go to the Smart Card options screen.



Channel Configuration

Configure the iCAM, Smart Card, Access Panel, Access Door and GPO for the channel to be activated properly.

Channel 1 Configuration - iCAM + Smart Card

Smart Card

The offset only needs to be changed if storing non-IrisAccess 4000 information on the SmartCard.

HID Offset (hexadecimal) : 13

□ Use as Prox Card

Encryption Algorithm

Select the Encryption Algorithm to encrypt the Smart Card

Data format in Smart Card: GSC-IS Format

Encryption Algorithm: None

Security Keys

Click 'Get Keys...' to get Smart Card keys file. A keys file can be generated in IrisServer.

Security Key 1 :

Security Key 2 :

10. Block Offset – **HID iClass Only -** Location on the smart card where the iris data block starts. Default block offset is 13.

Note: The Block Offset is applicable only when using HID iClass smart cards storing additional non-iris data on the smart card (example: face or fingerprint data). The offset entered must match that set in IrisEnroll.

11. Use as Prox Card – **HID iClass Only** – When checked, the prox card portion of the iClass card will pass the Wiegand Card ID into the system for output. Requires Wiegand wiring of HID iClass smart card reader.

12. Data Format in Smart Card – The selection here must match the setting in IrisEnroll to be able to read the encoded cards.

- **IA EAC Format** = IrisAccess EAC smart card format (AES Encryption only), **iClass Only**.
- **GSC-IS Format** = Government Smart Card Interoperability Standard format.

- **Lenel Format =** Special format for Lenel On-Guard, Refer to Lenel documentation for details

13. Encryption Algorithm - The selection here must match the setting in IrisEnroll to be able to read the encoded cards.

    - **None =** The iris data will not be encrypted
    - **AES** = Advanced Encryption Standard
    - **DES** = Data Encryption Standard (**iClass Only**)
    - **DES3 =** Triple Data Encryption Standard (**iClass Only**)

14. Security Keys must be entered when using encryption. Click the **Get Keys** button to open the Load Encryption Keys screen.

    - Click the **Load** button for the Open dialog and point to the .dat file created in IrisServer. (My Documents is the default location where the .dat file is saved)

    - Click **OK** to "**Succeed to loading data file for Smart Card Keys**" dialog.

    - Click **OK** to go back to the Smart Card configuration screen.

15. Click **OK** to go back to the main ICU configuration screen.

At this point the channel has been configured for smart card support. Repeat the steps starting at number 6 to configure the other channels of the ICU as required.

16. At the main ICU configuration screen click on the arrow next to **After Settings** and choose **Send to an ICU.**

17. Enter the IP Address and password (default password = iris4000) for the ICU that is being configured. Click **OK**

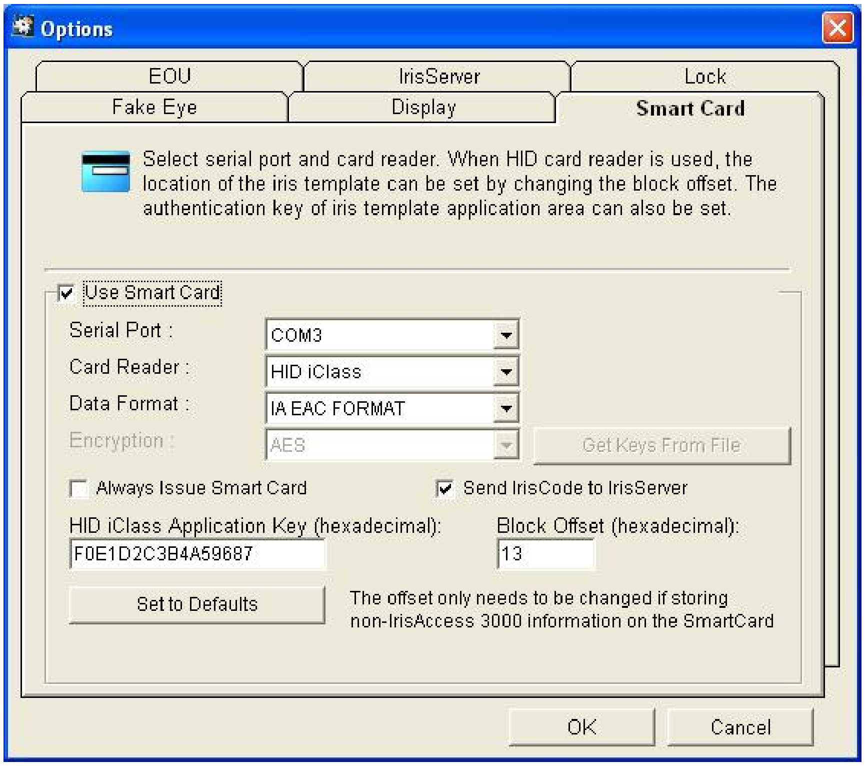
18. Click **Yes** to restart the ICU and **OK** to the dialog.

5.3 Configuring the IrisAccess™ Software for 3000 Series Cameras

5.3.1 Configuring IrisEnroll3000 for Smart Cards

IrisEnroll card configuration needs to be performed at each enrollment station on which a smart card reader will be connected.

1. Open IrisEnroll3000
2. Enter ID and Password (Default ID = administrator, password = iris3000)
3. Select **Options > Smart Card: the following window will appear.**



Select serial port and card reader. When HID card reader is used, the location of the iris template can be set by changing the block offset. The authentication key of iris template application area can also be set.

☑ Use Smart Card

Serial Port : COM3

Card Reader : HID iClass

Data Format : IA EAC FORMAT

Encryption : AES

☐ Always Issue Smart Card ☑ Send IrisCode to IrisServer

HID iClass Application Key (hexadecimal): F0E1D2C3B4A59687

Block Offset (hexadecimal): 13

The offset only needs to be changed if storing non-IrisAccess 3000 information on the SmartCard

4. Select the check box for **Use Smart Card.**
5. Select the **Serial Port** of the enrollment computer to which the smart card reader is connected. This must not conflict with the serial port assigned to the EOU.

   Note: Although the EOU3000 will not operate through a USB to RS232 Serial adapter or other devices that creates a virtual RS232 serial port, all of the supported smart card readers will operate properly through such an adapter.

6. Select the **Card Reader** type:

   a. **BQT BT-815** = BQT Solutions MiFARE smart card reader / writer
   b. **HID iClass** = HID iClass smart card reader / writer
   c. **Indala DESFire =** Indala DESFire smart card reader / writer

7. Select the **Data Format**:

   - **IA EAC Format** = IrisAccess EAC smart card format (AES Encryption only)
   - **GSC-IS Format** = Government Smart Card Interoperability Standard format.

8. Select **Encryption** (GSC-IS format only):

   - **None =** The iris data will not be encrypted
   - **AES** = Advanced Encryption Standard
   - **DES** = Data Encryption Standard
   - **DES3 =** Triple Data Encryption Standard

   Note: The encryption key set (.dat file) created must be loaded if encryption is selected. This same key file must used for each ICU channel and ICU in the system.

9. Always Issue Smart Card – check this box if all enrollments at this station are to be issued a smart card. With this box checked, the Card will automatically be selected, as Smart Card and the smart card writing process will start immediately after enrollment. If this box is unchecked, you will have the option of selecting the type of card (smart, prox, or no card) that will issued for the user. The default of this box is unchecked.

10. Send IrisCode to IrisServer – check this box if copies of the enrolled iris template(s) are to be stored in the IrisAccess DB as well as on the smart card. It is recommended to have enabled so that replacement cards can be issued without requiring re-enrollment of the user. The default is with this box checked.

11. Application Key – **For HID iClass Card Readers Only –** The application key used to unlock the iClass card. **All iClass readers in the system must have identical application keys**.

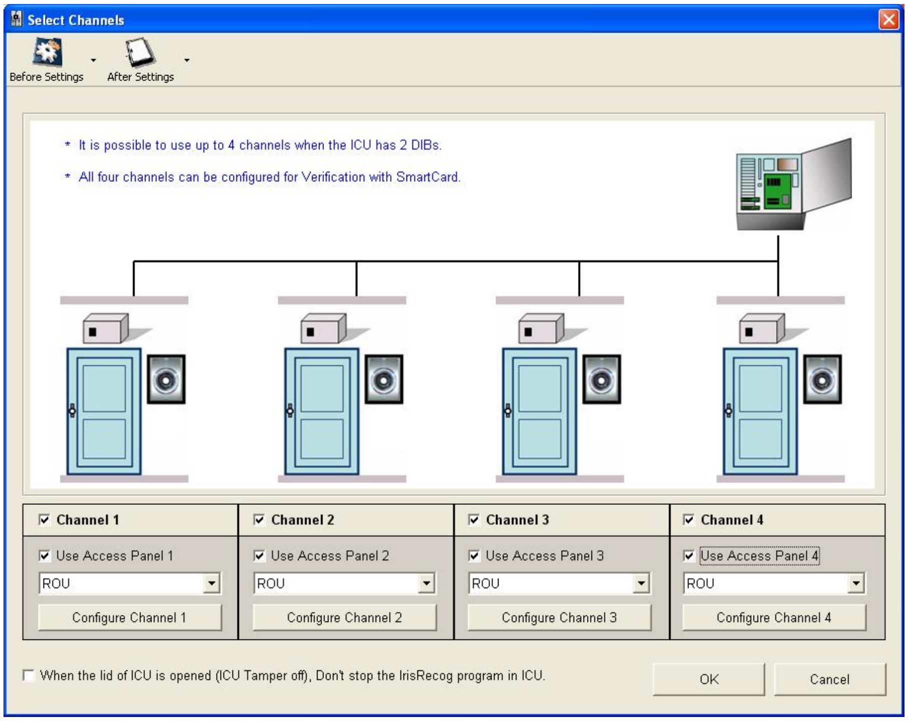
Note: The following step is applicable only when using HID iClass smart cards storing additional non-iris data on the smart card (example: face or fingerprint data).

12. Block Offset **–** Location on the smart card where the iris data block starts. Default block offset is 13.

5.3.2 Configuring IrisICUAdmin3000 for Smart Cards with ROU3000s

The configuration for smart card operation must be performed on each ICU and each channel that will utilize smart cards. This procedure assumes that the ICUs/ROUs are connected and tested to be operational in identification mode.

1. Open the **IrisICUAdmin3000** application.
2. Select **Configuration**.
3. Select the type of ICU being configured.
    - ICU3000 Hardware = ICU3000 (Large Dark Grey ICU)
    - ICU4000 Hardware = ICU4300 (Small Beige ICU)



* It is possible to use up to 4 channels when the ICU has 2 DIBs.

* All four channels can be configured for Verification with SmartCard.

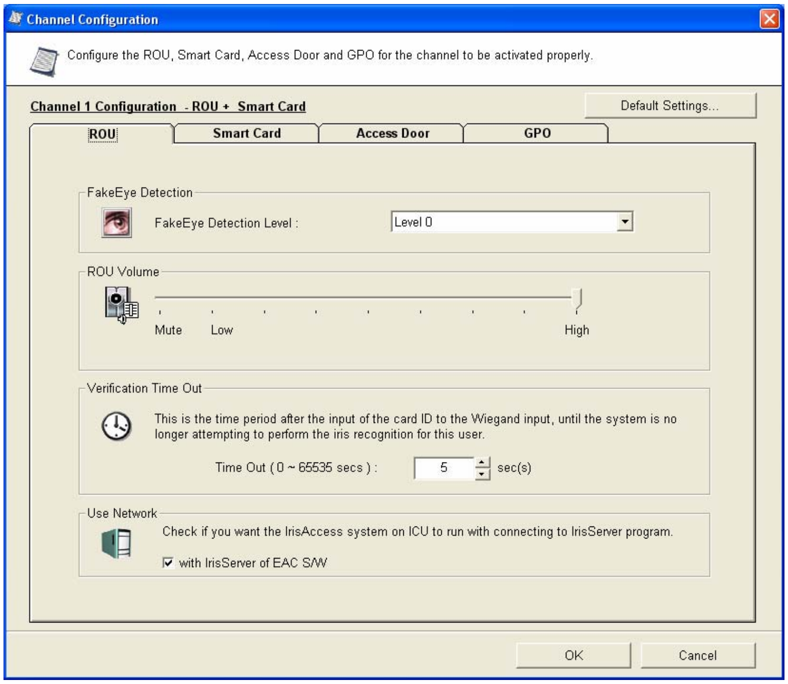
☑ Channel 1	☑ Channel 2	☑ Channel 3	☑ Channel 4
☑ Use Access Panel 1	☑ Use Access Panel 2	☑ Use Access Panel 3	☑ Use Access Panel 4
ROU	ROU	ROU	ROU
Configure Channel 1	Configure Channel 2	Configure Channel 3	Configure Channel 4

☐ When the lid of ICU is opened (ICU Tamper off), Don't stop the IrisRecog program in ICU.

4. At the main ICU configuration screen click on the arrow next to **Before Settings** and choose **Get the settings from an ICU.**
5. Select if you want to save the current configuration displayed on the configuration screen. Typically select No.
6. Enter the IP Address and password for the ICU that is being configured. Click **OK**. The current settings of the ICU will load into IrisICUAdmin.
7. For the channel being configured for smart card support, change the drop down box to **ROU + Smart Card**.
8. Click on **Configure Channel #**. (# Being the channel number to configure)
9. Channel configuration screen – ROU; **Use Network**:

When the box is checked for “with IrisServer of EAC S/W”, the ICU will communicate with the IrisAccess DB to check for user permissions and report back to IrisMonitor the system and user activity that takes place on the ICU.

Without this box checked the ICU will act in “stand-alone” mode, allowing all valid smart cards access and not reporting activity back at the server. Permissions in this mode are handled by an external access control system.



Channel Configuration

Configure the ROU, Smart Card, Access Door and GPO for the channel to be activated properly.

Channel 1 Configuration - ROU + Smart Card

FakeEye Detection

FakeEye Detection Level : Level 0

ROU Volume

Verification Time Out

This is the time period after the input of the card ID to the Wiegand input, until the system is no longer attempting to perform the iris recognition for this user.

Time Out (0 ~ 65535 secs) : 5 sec(s)

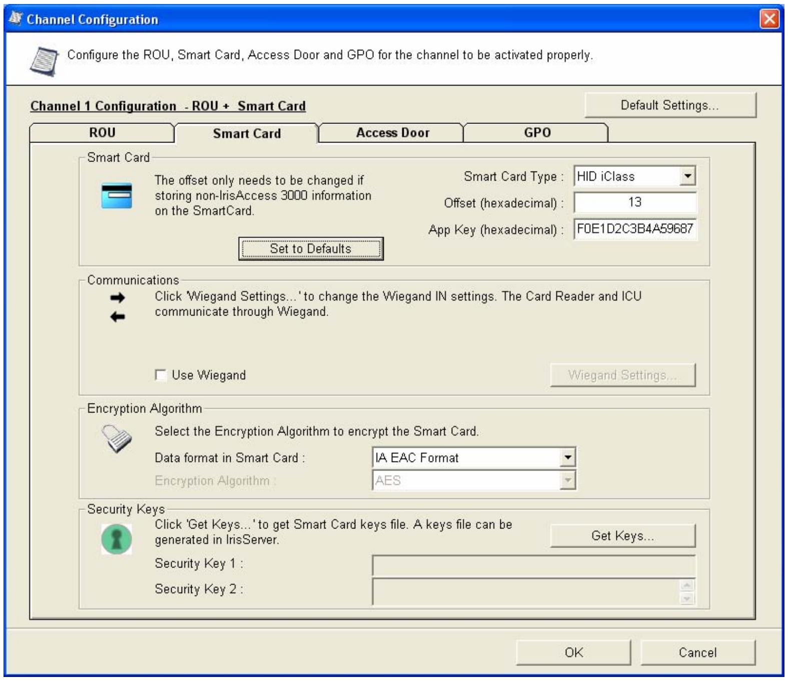
Use Network

Check if you want the IrisAccess system on ICU to run with connecting to IrisServer program.

☑ with IrisServer of EAC S/W

Channel Configuration Screen : ROU

4. Click on the **Smart Card** tab to go to the Smart Card options screen.



Channel Configuration

Configure the ROU, Smart Card, Access Door and GPO for the channel to be activated properly.

Channel 1 Configuration - ROU + Smart Card

Smart Card

The offset only needs to be changed if storing non-IrisAccess 3000 information on the SmartCard.

Smart Card Type : HID iClass

Offset (hexadecimal) : 13

App Key (hexadecimal) : F0E1D2C3B4A59687

Communications

Click 'Wiegand Settings...' to change the Wiegand IN settings. The Card Reader and ICU communicate through Wiegand.

☐ Use Wiegand

Encryption Algorithm

Select the Encryption Algorithm to encrypt the Smart Card.

Data format in Smart Card : IA EAC Format

Encryption Algorithm : AES

Security Keys

Click 'Get Keys...' to get Smart Card keys file. A keys file can be generated in IrisServer.

Security Key 1 :

Security Key 2 :

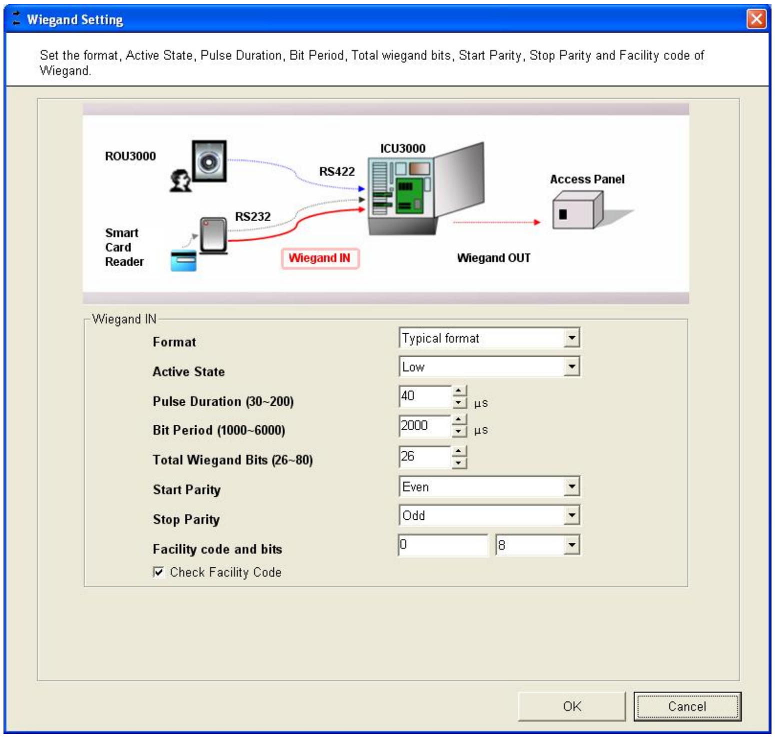
5. Select the **Smart Card Type**: BQT BT-815, HID iClass or Indala DESFire

Note: The following settings only apply when using the HID iClass cards and are storing non-IrisAccess data on the smart card. These settings may not be available depending on the card format and encryption method selected.

6. Change **Offset** if needed, this is the location on the smart card where the iris data block starts. By default, this must match the setting in IrisEnroll.
7. Change **App Key** if needed, this is the application key used to access the data on the smart card (hexadecimal format). By default, this must match the setting in IrisEnroll.

Note: **Set to Default** button will restore the **Offset** and **App Key** settings to the IrisAccess™ 3000 defaults.

8. Check the box for **Use Wiegand** (HID iClass only) and click on the **Wiegand Settings** button.



Wiegand Setting

Set the format, Active State, Pulse Duration, Bit Period, Total wiegand bits, Start Parity, Stop Parity and Facility code of Wiegand.

Wiegand IN

Format	Typical format
Active State	Low
Pulse Duration (30~200)	40 µs
Bit Period (1000~6000)	2000 µs
Total Wiegand Bits (26~80)	26
Start Parity	Even
Stop Parity	Odd
Facility code and bits	0 8

☑ Check Facility Code

9. The default settings of the Wiegand In, is for that of a HID iClass smart card reader.
   - Format: Typical
   - Active State: Low
   - Pulse Duration: 40uS
   - Bit Period: 2000uS
   - Total Wiegand Bits: 26
   - Start Parity: Even
   - Stop Parity: Odd
   - Facility Code: 1 (see step 15)
   - Facility Code Bits: 8

10. Facility code may be different, change as needed or uncheck **Check Facility Code** to ignore the facility code of the iClass card.

11. Click **OK** to continue and go back to the channel configuration: Smart Card screen.

12. Select the **Encryption Algorithm** used to encrypt the smart card. There are two data formats available:
    - **IA EAC Format** (IrisAccess Entry Access Control) – This is the format of the card when it is written using an LG IrisAccess™ 3000 enrollment station. This is the default format. AES encryption is the only encryption method available.
    - **GSC-IS Format** (Government Smart Card-Interoperability Specification) – This format is used when the smart cards used are encoded in a GSC-IS format. The following encryption algorithms are supported in this format: AES, DES, DES3 (Triple DES), or no encryption.

13. Security Keys must be entered when using encryption. Click the **Get Keys** button to open the Load Encryption Keys screen.

14. Click the **Load** button for the Open dialog and point to the .dat file created in IrisServer. (My Documents is the default location where the .dat file is saved)

15. Click **OK** to "**Succeed to loading data file for Smart Card Keys**" dialog.

16. Click **OK** to go back to the Smart Card configuration screen.

17. Click **OK** to go back to the main ICU configuration screen.

At this point the channel has been configured for smart card support. Repeat the steps starting at **ICU configuration for smart card support,** step 6 to configure the second channel of the ICU if required.

18. At the main ICU configuration screen click on the arrow next to **After Settings** and choose **Send to an ICU.**

19. Enter the IP Address and password for the ICU that is being configured. Click **OK**

20. Click **Yes** to restart the ICU and **OK** to the dialog.

6. Software Operation with Smart Cards

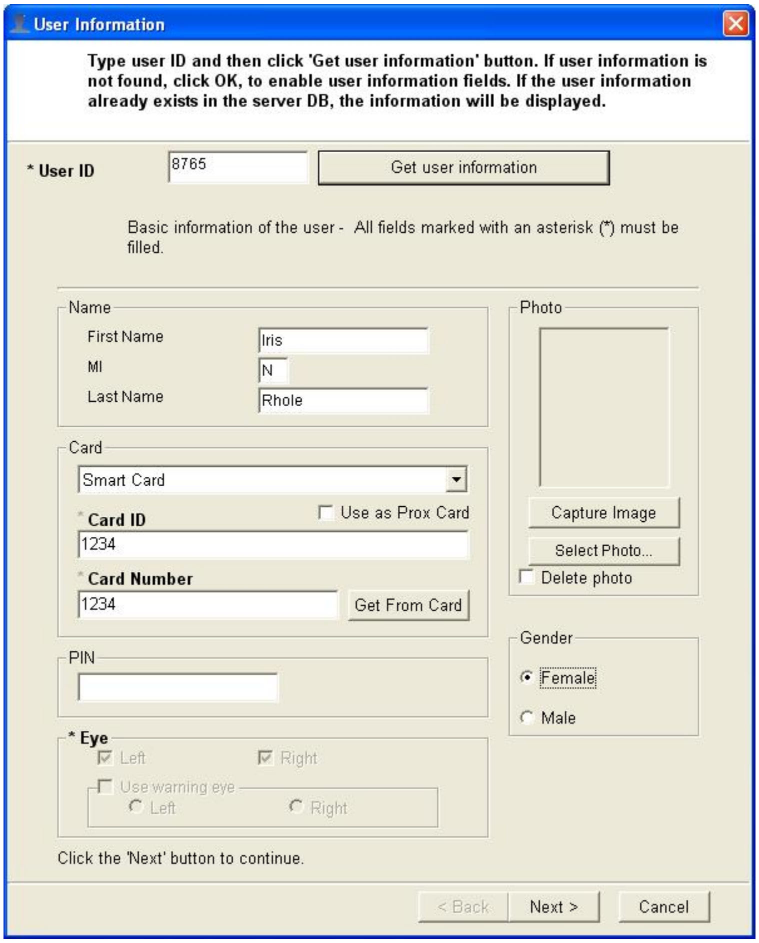
6.1 Using the LG IrisAccess™ System with Smart Cards

6.1.1 Enrolling a user to the smart card

Note: HID iClass 16K/2, HID iClass 16K/16, and IE MiFARE DESFire 4K cards are capable of holding both right and left iris templates. The BQT cards can hold only one iris template. If both irises are enrolled, and a BQT card is used, only the users' right iris is stored on the card.

The IrisEnroll application is used to enroll the users' iris template(s) on to a smart card. Smart cards can be issued during a new enrollment (iris template not already in the system) or from the Card selection in IrisEnroll when the users iris templates have been stored in the IrisAccess DB.

1. During the users' enrollment process select **Smart Card**, and then enter a **Card ID** (Card ID can be a number from 0 to 9999999999999999999). When Smart Card is selected this will open the "Issue card" dialog display at the end of the normal enrollment procedure.



User Information

Type user ID and then click 'Get user information' button. If user information is not found, click OK, to enable user information fields. If the user information already exists in the server DB, the information will be displayed.

* User ID: 8765

Basic information of the user - All fields marked with an asterisk (*) must be filled.

Name

First Name: Iris

MI: N

Last Name: Rhole

Card: Smart Card

* Card ID: 1234

□ Use as Prox Card

* Card Number: 1234

PIN:

* Eye

☑ Left ☑ Right

□ Use warning eye ○ Left ○ Right

Photo

□ Delete photo

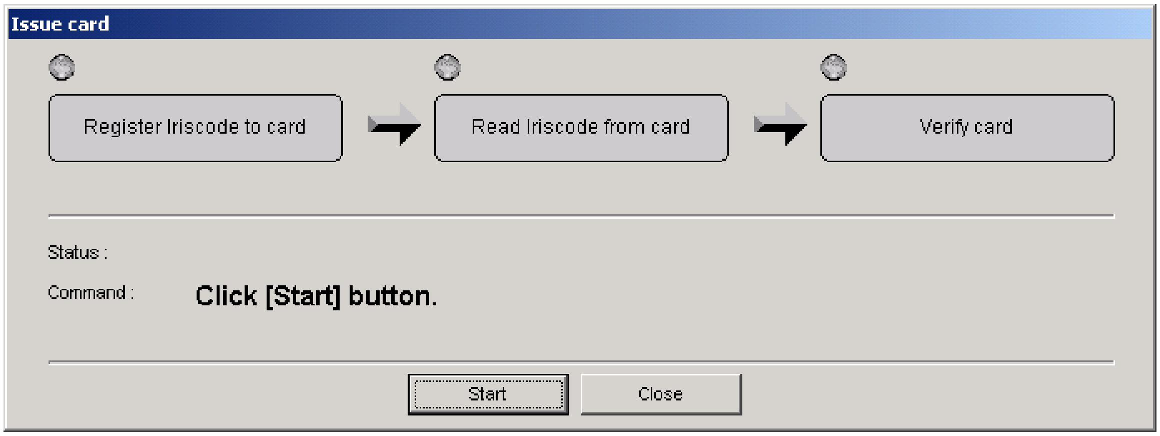
Gender

● Female

○ Male

Click the 'Next' button to continue.

2. At the Issue Card dialog click on **Start.**



Status :

Command : Click [Start] button.

3. Place a hold the smart card on the smart card reader for the duration of the card issue process. First the iris template(s) will be written to the card, and then the information written is verified by reading the card and verifying the users' iris(es) against the stored template(s). The dialog will prompt which eye the user needs to verify.
4. The user is now enrolled in the system and their iris template(s) are stored on the smart card.

6.1.2 Issuing a Smart Card for Enrolled Users

A smart card can be issued for user whom are already enrolled in the IrisAccess database.

1. In IrisEnroll click on **Card.**
2. Enter the User ID of the user and click on "Get user information".
3. When a matching User ID is found, the user's information will display.
4. Verify the information and click Finish to open the Issue Which Eye dialog.
5. Select which eyes will be enrolled onto the card.
    - **Right Eye**
    - **Left eye**
    - **Both eyes**

6. Click **Issue SmartCard** to open the Issue Card dialog.
7. Click **Start** to begin smart card encoding process.
8. Place a hold the smart card on the smart card reader for the duration of the card issue process. First the iris template(s) will be written to the card, and then the information written is verified by reading the card and verifying the users' iris(es) against the stored template(s). The dialog will prompt which eye the user needs to verify.
9. The user is now enrolled in the system and their iris template(s) are stored on the smart card.

6.1.3 Verifying User’s Smart Card from IrisEnroll

1. Open the IrisEnroll application.
2. Click on **Verify**.
3. Click on **Verify with Smart Card**.
4. At Verify with Smart Card dialog, click **Start**, present and hold smart card to the enrollment smart card reader.
5. Camera will prompt to “Please center your eyes in the mirror”; the user should then present their eyes in the mirror.
6. A Dialog will display with verified if successful and list which iris was read.

6.1.4 Verifying the User’s Smart Card at a Remote Unit (iCAM or ROU3000)

1. The user presents and holds their smart card to the smart card reader until the tones complete sounding.
2. With a successful read of the card, the iris camera will prompt the user to “Please look into the mirror”
3. The user presents their eye(s) to the iris camera for verification.
4. Upon successful verification, the Card ID will be sent via Wiegand to an external access system.