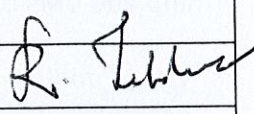


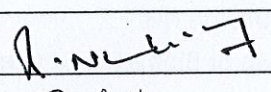
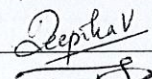
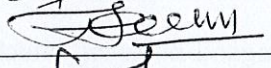
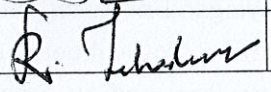
**GOVERNMENT OF INDIA**  
**INDIRA GANDHI CENTRE FOR ATOMIC RESEARCH**  
**COMPUTER DIVISION**  
**KALPAKKAM – 603102**

THIS DOCUMENT IS THE PROPERTY OF INDIRA GANDHI CENTRE FOR ATOMIC RESEARCH.  
THIS SHALL NOT BE REPRODUCED OR COMMUNICATED WITHOUT OWNER'S PERMISSION.

SYSTEM	VIRTUAL DESKTOP INFRASTRUCTURE		
TITLE	Configuration And Usage Of Biometric Access Control System (BACS) Of VDI System		
A	Original Issue	20-05-2019	
No	Revisions	Date	Approved

IGCAR	EIG	RCCG	CD	CSS	VDI	2	REV	A			
-------	-----	------	----	-----	-----	---	-----	---	--	--	--

Electronics Instrumentation Group  
Virtual Desktop Infrastructure

	NAME	SIGN	DATE
PREPARED	R.Nandakumar		10-05-2019
	Deepika Vinod		10-05-2019
REVIEWED	M L Jayalal		19/05/2019
APPROVED	R Jehadeesan		20/05/2019

**Distribution:**

Head, CSS;

Head, CD;

AD, RCCG;

Director, EIG;

**SUMMARY**

This document describes the procedure for configuration and usage of Biometric Access Control System (BACS) commissioned for VDI system. The document describes the major components and functionality of BACS .It also describes various functionalities of BACS like adding user, user finger enrollment, deletion procedure etc.



# **Configuration and Usage of Biometric Access Control System (BACS) of VDI system**

## **1. Introduction**

VDI (Virtual Desktop Infrastructure) is a term used to describe a specific field of virtualization in computing, which deals with creating and maintaining virtual desktops within an organization's IT environment. The VDI allows the migration of desktop operating systems from physical computing resources to Virtual Machines, or VMs, hosted on centralized servers. VDI setup at IGCAR consists of twenty VDI servers, two management servers, and Unified storage with usable space of 185TB. All the servers are configured in high availability and the setup is designed for connecting 1000 thin clients with user VMs. The setup is configured with 700 VMs of windows 10 and 200 VMs of Linux.

VDI is implemented across IGCAR and the centralized datacenter where the virtual desktops are created, managed and delivered is housed in Computer Centre. VDI Server Rack located at Computer Center houses the servers and storage devices of Virtual Desktop Infrastructure (VDI) system. To ensure security of these critical systems, Biometric Access Control System (BACS) has been installed to provide access to different doors of VDI server rack to authorized users.

The manufacturer details of Biometric Access Control System (BACS) are as follows:

Make: Smart-I

Model: BIOLite NG

Model No of Biometric Reader: SBLNG130-AC series

Model No of rack controller: SMNR1012

The BACS is based on Wiegand protocol, which is used widely in access control systems. Wiegand is a communication protocol between a biometric reader (i.e. a card, a fingerprint or other data capture devices) and an access control system. On the physical level, the Wiegand interface consists of three conductors: Data0, Data1 (transmission wires) and Ground wire. The protocol allows one-way communication only, i.e. data is sent from reader to controller.

## **2. Functional Description of BACS**

The VDI setup consists of four server racks (RACK1-4), two cooling racks (ACUNIT-1&2) and a utility rack as shown in figure 1. BACS is installed in the utility rack.



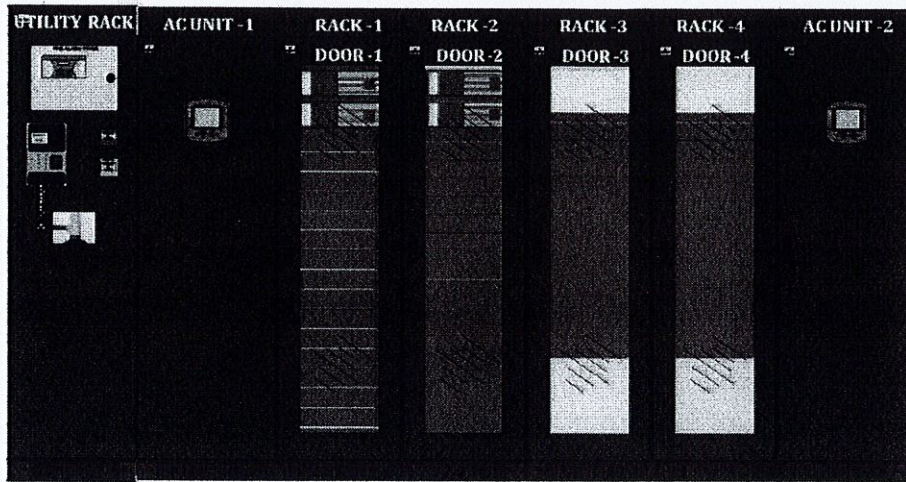


Figure 1: VDI setup with server racks, cooling racks and utility rack

BACS of VDI consist of two components namely, biometric reader and Smart rack controller.

**2.1 Biometric reader:** The biometric reader consists of a graphical LCD to display date and time, finger print sensor for capturing users' finger prints, touch keypad interface for setting the configuration parameters. Figure 2 shows the major components of biometric reader of VDI rack biometric access control system.

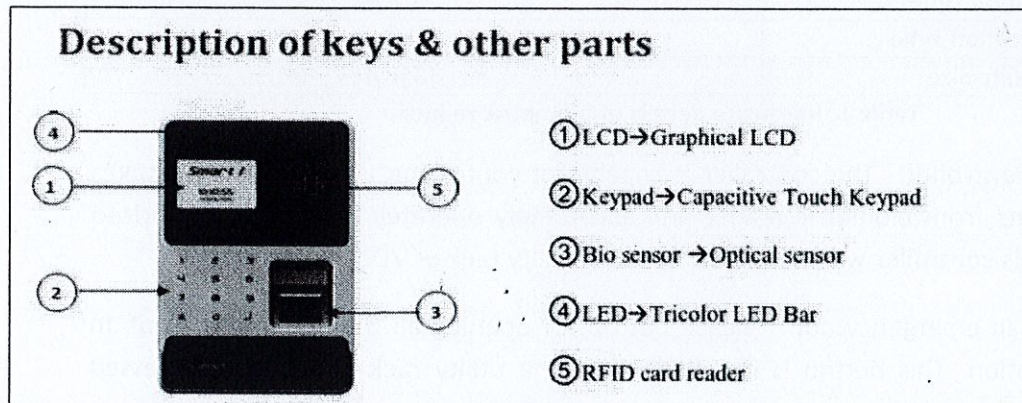


Figure 2: Major components of Biometric reader

The biometric reader is installed on the front side of the utility rack of VDI setup for easy access. It has the following features:

- The system is capable of working under different modes like Smart Card Only, Smart Card plus Finger, Finger Only, UID only etc. In the present setup, finger only mode is enabled.
- Up to 19000 templates ( Finger prints ) can be enrolled
- Maximum number of users can be up to 75000
- Up to 25000 entry logs can be saved.



- Data from the reader can be downloaded to a PC for further analysis/report generation.

Table 1 lists the hardware configuration details of biometric reader.

Particulars	Description
CPU	32Bit RISC
Memory	UptoFlash8M
Events/Transactions	2,5
No. of templates in sensor	1
No. of Users	7
Operation Modes	Card Only, UID plus Finger, Card plus Finger, Finger Only, UID only
Sensor	High Quality Scratch Resistance Optical Sensor.
Communications Port	TCP/IP, weigand, RS485
Baud Rate	9600bps
Keypad	Capacitive Touch Keypad
LED	Tricolor LED
Power Supply	12VDC/2A(Min)
Optical Sensor Specification	
Enrollment Time	<1 Sec
Verification Time	<1 Sec
Identification Time	1 Sec
Template Size	384bytes

Table 1: Hardware details of biometric reader

**2.2 Smart rack controller:** The controller is capable of controlling up to 8 doors. It takes finger print inputs from biometric reader and accordingly operates respective authorized door outputs. This controller was installed inside the utility rack of VDI server setup.

The system has an emergency door release button for opening all the doors in case of an emergency situation. This button is installed inside the utility rack and can be accessed without opening the rack door.

The controller is interconnected with Rack Distribution Unit (RDU) of the VDI rack cooling system. RDU is installed inside RACK-2 of VDI system. When the VDI server rack temperature exceeds the maximum set temperature level, RDU sends signal to the smart rack controller for opening all the doors.

The block diagram of BACS depicting various components and their interconnections is shown in figure 3.



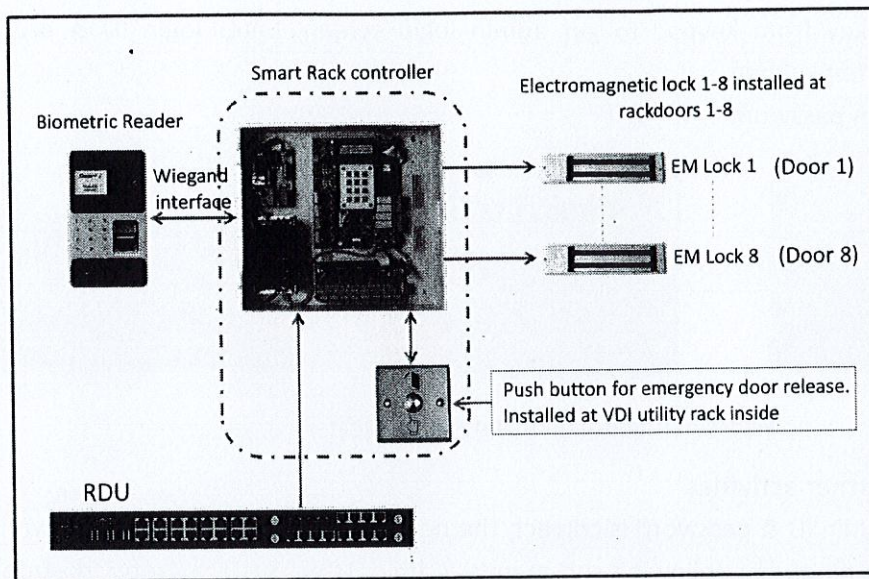


Figure 3: Block diagram of BACS depicting various components and their interconnections

### 3. User Enrollment in biometric reader.

BACS can be accessed only by enrolled users. The keypad provided along with biometric reader is used for user enrollment. Figure 4 shows the keypad of biometric reader. The functionality of different keys is mentioned in table 2.

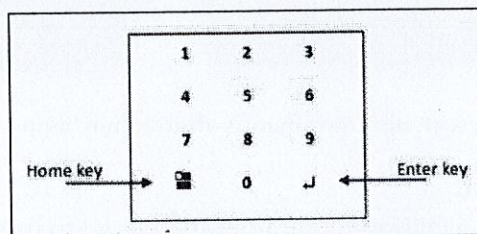


Figure 4: Keypad of biometric reader

Keys	Description
Numeric keys(0-9)	To access keypad functions and to enter User-ID(UID) for verification
Keys 2& 8	Scroll keys to select menu after admin login.
Keys 4& 6	Scroll keys to select options
Home screen key	To go to the home screen
Enter key	Entering into menu parameter and set the values for parameter

Table 2: Functionality of biometric reader keys

Following are the steps to be followed for user enrollment.

#### Home Screen and Admin login

1. Power on finger print reader unit. The unit shows the home screen (titled as 'SMART-i') as shown in figure 5.



2. Press Home key from keypad to get admin login screen. Enter login ID & press "Enter" key from keypad.
3. Enter the login password.

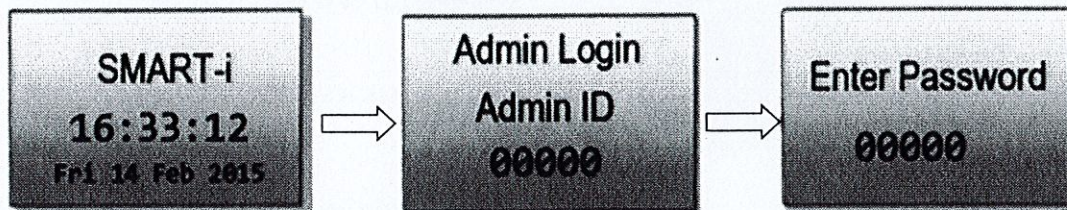


Figure 5: Home screen and Admin login

**a. Screen for further activities**

1. If entered admin ID & password is correct, the next level screen appears as shown in figure 6. This menu has following sub menus: Admin, User, System, Network, Door, Trouble shoot, Device info and logout.
2. For enrolling new user, select "User" with the help of scroll keys (2&8) and press enter key.

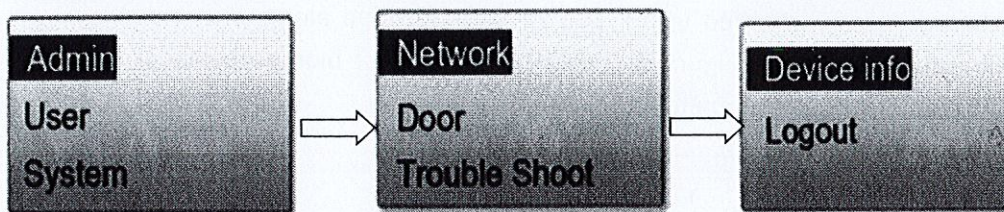


Figure 6: Screen with different menus after admin login

**b. Screen for user management**

1. This menu is used to access all different parameters related to user such as add user, delete user, search user, change pin, add user data and add finger to ID as shown in figure 7.

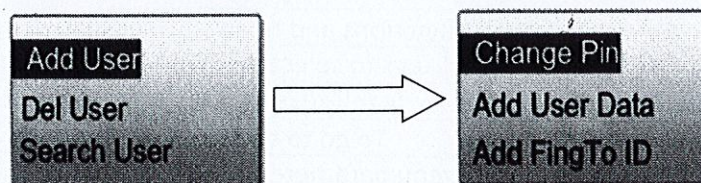


Figure 7: Screen for user management

2. **Adding User:** Select 'Add User'. Enter the UID (user ID = IC no) and press enter key as shown in figure 8. Next select finger addition Yes or No option by 4 and 6 keys. Select 'Yes' option to enroll the finger. Then it asks to place finger with sensor ON. Once finger gets added, it shows score of finger and then asks for 2<sup>nd</sup> time. The user needs to put the same finger again and Press 'YES'.



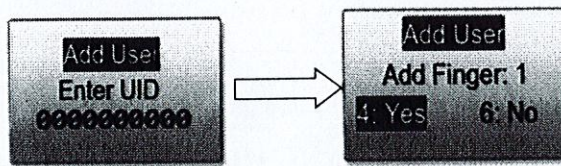


Figure 8: Screen for adding user

3. **Deleting User:** Select 'Del user'. In this menu, enter the UID number and press enter to delete that user and the corresponding enrolled fingers as shown in figure 9.



Figure 9: Screen for deleting user

1. **Adding Finger to a ID:** Users who are already enrolled can use this option to add more fingers. Users can add up to 8 fingers using this option. Select 'Add Fing to ID'. After selecting this menu, enter the UID number and press enter as shown in figure 10. Sensor gets ON to add fingers for that particular UID with score.

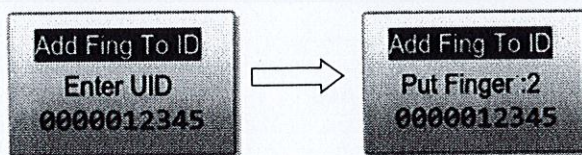


Figure 10: Screen for adding finger to a User ID

2. **Setting access to specific door numbers:** This option is used to give enrolled users access to specific doors. Select 'Set Door No'. In this menu, accesses to required doors are allowed to users as required. Enter the user ID and press enter as shown in figure 11. Then enter door no (from 01 to 08) which requires access and press enter key to add that door to user.

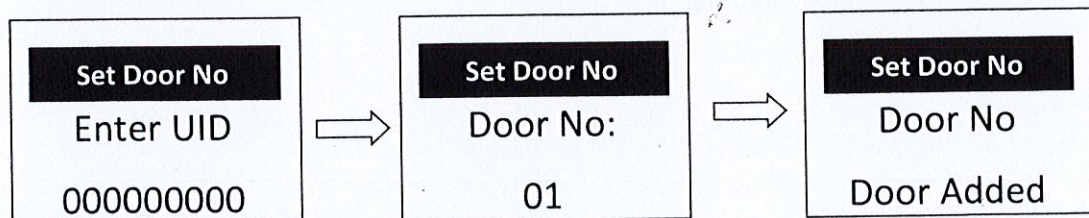


Figure 11: Screen for setting access to specific door numbers

3. **Setting access to all doors:** This option is used to give enrolled users access to all doors. Select 'Set All Doors'. In this menu we can allow to access all doors to users. Enter the user ID and press enter as shown in figure 12. Select **4** to set all doors or select **6** to delete all doors for that user.



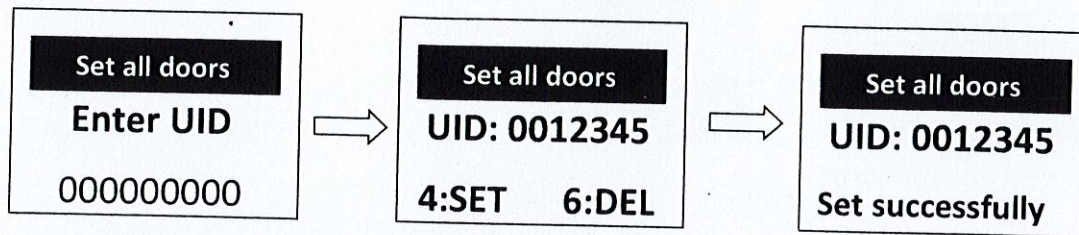


Figure 12: Screen for setting access to all doors

#### 4. User Access through BACS

Put the enrolled finger in to the biometric sensor. If the finger is authorized, "Select Door" screen will appear. Enter the required door no and press enter key as shown in figure 13. The corresponding door/doors will be opened.

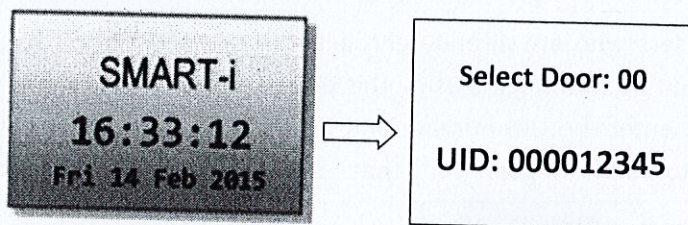


Figure 13: Screen for user access through BACS

#### 5. Conclusion

Biometric access control system provides security to the VDI (Virtual Desktop Infrastructure) setup installed at Computer Centre. BACS consist two parts namely, biometric reader and Smart rack controller. Biometric reader is used for user enrollment and user access. Smart rack controller takes finger print inputs from biometric reader and accordingly operates respective authorized door outputs. The document describes the major components and functionality of BACS .It also describes various functionalities of BACS like adding user, user finger enrollment, deletion procedure etc.