Singapore Polytechnic
School of Electrical and Electronics Engineering
ET1205: Wireless Technology Applications

Experiment 01: Setting up RFID Basic Commands and PC Interface

Objectives:

Students will learn

- what are the modules inside the RFID contactless smart card reader and its system to provide different types of applications to enable various services.
- the basic command of a reader module, interface to a PC, and read/ write data of Mifare and I-Code RFID cards.

Introduction:

In lectures, students will learn the basic components of an RFID system. In this experiment, students will learn the basic commands of a reader module and how to read/write I-Code, MiFare RFID cards and MiFare Card Personalization function.

Initial Setup

Procedure:

1. Firstly, the reader module of the Training kit should be connected to a laptop via RS232 cable and then the laptop and the training kit are power on.
2. Launch the Demo Software of RFID training kit double clicking on the RFID shortcut icon at the desktop.

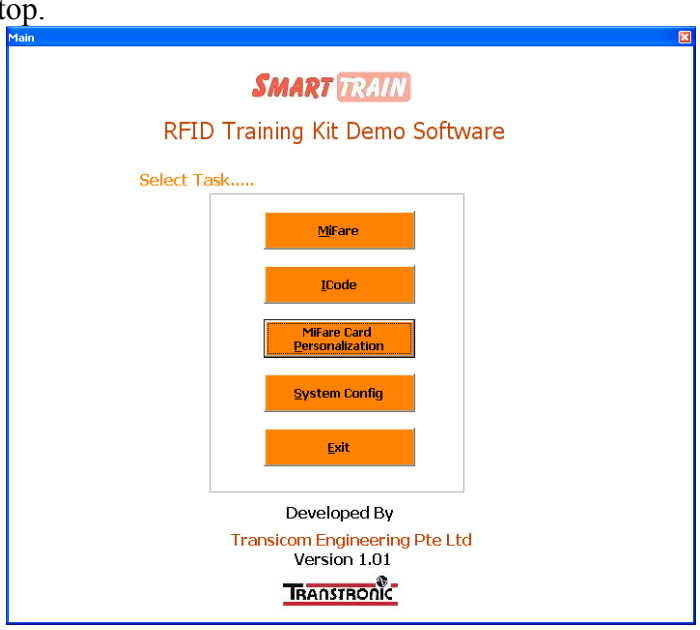

Figure 1: Main system screen

3. Then, click on the **System Config** button to set the communication setting of the com port and the baud rate of the reader. The com port setting can be updated by clicking the update button. It is important to take note that if you want to change the reader baud rate, its initial baud rate and the baud rate of the com port must be same. Click the **Return** button and back to Main menu.

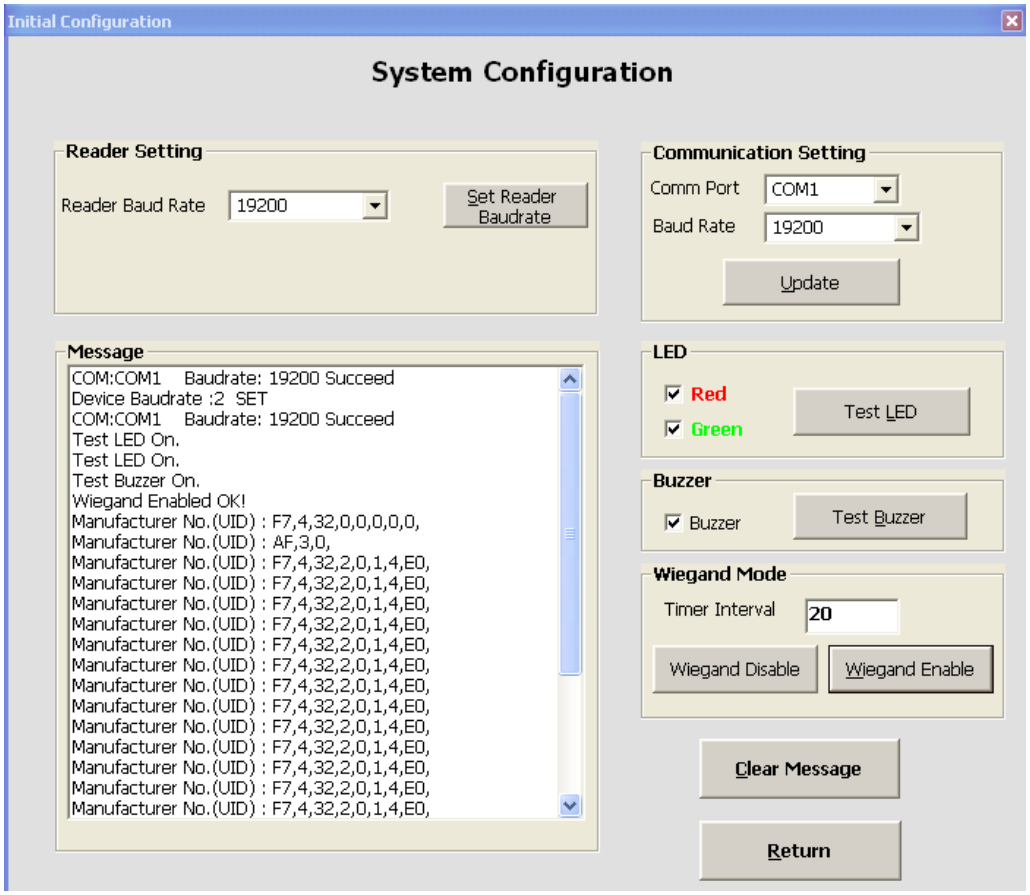

Figure 2: System configuration screen

4. In order to read/write the I-Code RFID tag, click the I-Code button. From the I-Code function window, you are allowed to experiment the I-Code basic commands such as select, reset, read, write and flag setting.

I-Code function

I-Code II Contact less card is complied with ISO15693 standard.

The memory map of the I-Code SL2 chip is as shown in the following Figure. The 1024 bit EEPROM memory is divided into 32 blocks. Each I-Code contains 28 accessible blocks for read/write operations. Each block can hold 4 bytes. The 8 byte-manufacturer number is stored in the block -3 and -4. The EAS, AFI, DSFID are stored in the block-2.

	Byte0	Byte1	Byte2	Byte3	
Block -4	UID0	UID1	UID2	UID3	Unique Identifier Lower bytes
Block -3	UID4	UID5	UID6	UID7	Unique Identifier Higher bytes
Block -2	IntUse	EAS	AFI	DSFID	EAS, AFI, DSFID
Block -1	00	00	00	00	Write Assess Conditions
Block 0	X	X	X	X	
Block 1	X	X	X	X	
Block 2	X	X	X	X	User Data
Block 26	X	X	X	X	
Block 27	X	X	X	X	

Figure 3: EEPROM memory map of I-Code SL2

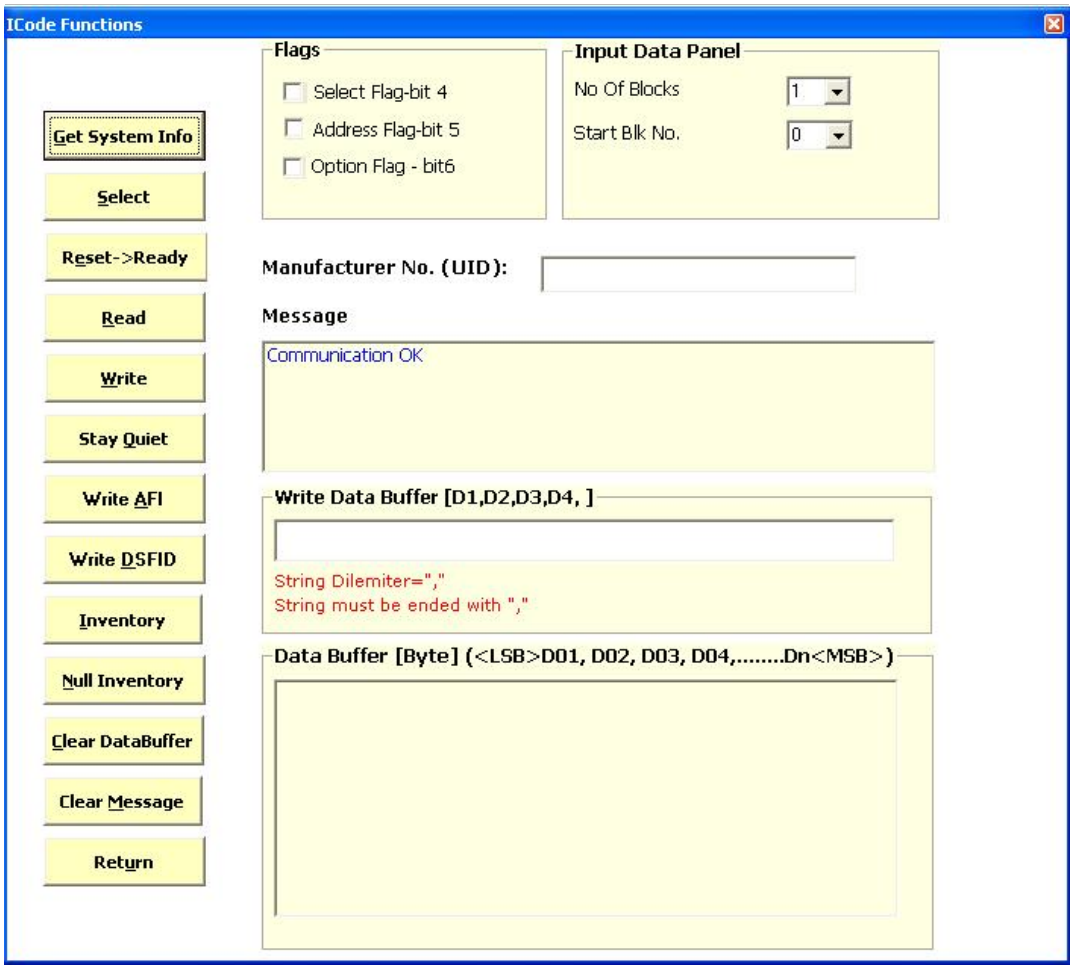

Figure 4: I-Code command screen

I-Code commands:

Procedure

In this section you are required to carry out few I-Code commands to test with the **three** I-Code cards.

1. Launch the I-Code Function window by clicking the ICode button at Main screen.
2. Place one of the I-Code cards on the reader.
3. From the I-Code Function window, click on the **Get System Info** that will Read **8** bytes UID (Unique Identifier), **1** byte DSFID and **1** byte AFI from card. Record the card information in Table 1.
4. Repeat the step 2 and 3 with others two I-Code cards.

Card No.	UID	DSFID	AFI	Remark
1				
2				
3				

Table 1

5. Using **Input Data panel** and **Read** button to retrieve the user data from block 0 to block 3 and record the data.
   Setting: No. of Block: _____, Start Block No.: _____Data.

6. Using **Input Data panel** and **Write** button to write the data "8,9,A,B," at block no. 6 and show it to the lecturer and then rewrite the data "0,0,0,0,".
7. Write **AFI** (Application Family Identifier) as "1" and rewrite "0". AFI value should be keyed in at Write Data Buffer as Hexa Decimal value of **one byte**.
8. Write **DSFID** (Data Storage Format ID) as "1" and rewrite "0". DSFID value should be keyed in at Write Data Buffer as Hexa Decimal value of one byte.
9. To test on the **Select** command, firstly place one of the cards on the reader and click on **Get System Info** to get UID, tick on the **address flag** to be checked and then click on the "Select" button. Then, place all the three cards on the reader and click on Read button. Which card is read?

   Selected One: ☐ One of the other two cards: ☐

10. Click **Reset->Ready** that will reset the card from the selected state to ready state.
11. To test on **Stay Quiet** command, place one of the cards on the reader, click on the **Get System Info** and tick on the **address flag** to be checked. Then, click **Stay Quiet command** button to issue a successful **Stay Quite** Command process. Then, the tick on the address flag to be unchecked. After the **Stay Quite** command has successfully issued, the card will not reply the commands until it is given **Reset -> Ready** command.
    Note: The card at the Stay Quite state shall respond to the commands in address modes.
12. **"Null Inventory"** command: When this command is issued, the UID of one card will return the data if there are more than one card are in the RF field. As an example, if you put card A and card B, and then issue **Null Inventory** command, either A or B with return. After giving Select command to the firstly returned card and issue Stay Quiet command, the card will be in Quiet mode. At this point, again if you give the Null Inventory having both cards A and B in the RF field, the other unchosen card, i.e card B, must reply, since card A is in the **Stay Quite** mode.
13. **Inventory** command: This command will run the anti-collision loop, you may get a card's UID by this command among many cards. The main difference between the NULL INVENTORY and INVENTORY itself is the requirement for UID input when the command is issued. The NULL INVENTORY does not require the UID.

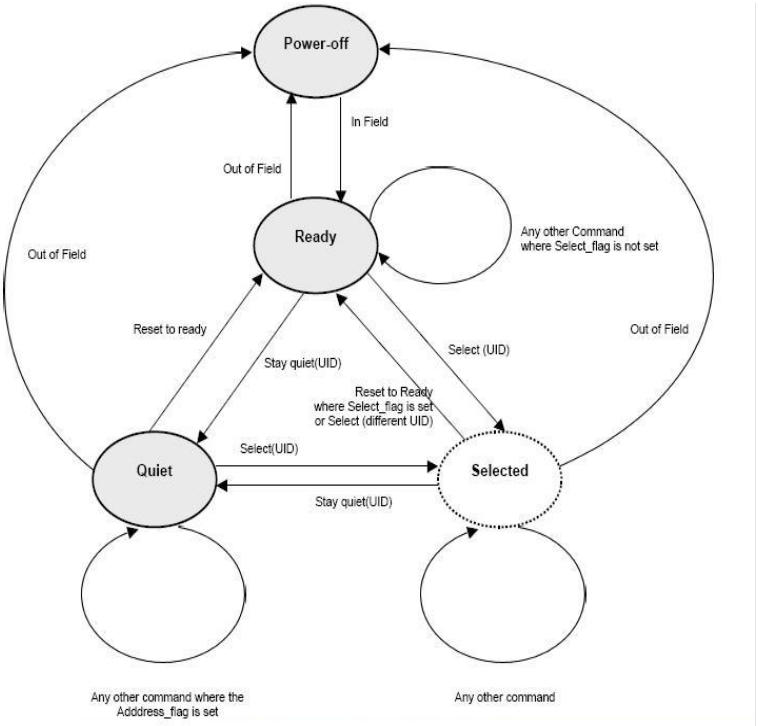

Figure 5: I-Code state diagram

Mifare Function:

In order to read/write the Mifare RFID tag, click the MiFare button. From the MiFare function window, you are allowed to experiment the MiFare basic commands such as:

a. Load Key (to reader)
b. Store Key (in reader)
c. Request/Request All
d. Anti-collision
e. Select
f. Authentication
g. Read
h. Write
i. Increment value
j. Decrement value
k. HighLevel Read
l. HighLevel Write

MiFare contactless smart cards are complied with ISO/IEC 14443A. When the card is positioned in the proximity of the Read Write Device antenna, RF communication interface allows to transmit data to the card.

Each of the MiFare cards contains 16 sectors with 4 blocks each. One block can store 16 bytes of data. At a time, 1 to 4 blocks in one sector of data can be read from the card. Each sector can have individual security key of its own. Before any read or write memory operation, key for each sector has to be authenticated by the loaded key. However, changing security key should be done by experienced person to avoid unnecessary damage to the card.

Card Read/Write Sequence

Mifare Card Function sequence as follow:

a) Select Sector number
b) Select number of blocks to Read (or) Select block number to Write (or) Select block number to Initialize Value Block
c) Request
d) Anti-Collision
e) Select
f) Load Key (not necessary to be in this exact sequence)
g) Authentication
h) Read (or) Write (or) Initialize Value Block

High Level Mifare Card Function sequence as follow:

a) Store Key
b) Select Sector number
c) Select number of blocks to Read (or) Select block number to Write
d) HighLevel Read (or) HighLevel Write

Security key is stored in block 3 of each block. This is also called as Sector trailer. Manufacturer serial number (UID) and data are stored in sector 0 of block 0. This is also called as Manufacturer block.

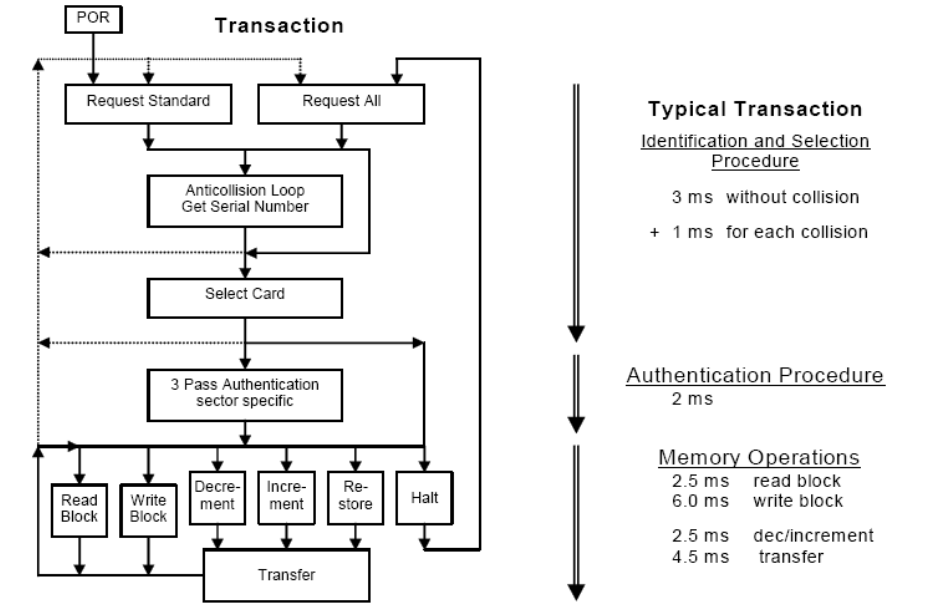

Figure 6: Three pass authentication

Sector	Block	Byte Number within a Block															Description
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Figure 7: EEPROM memory map of MiFare MF1ICS50

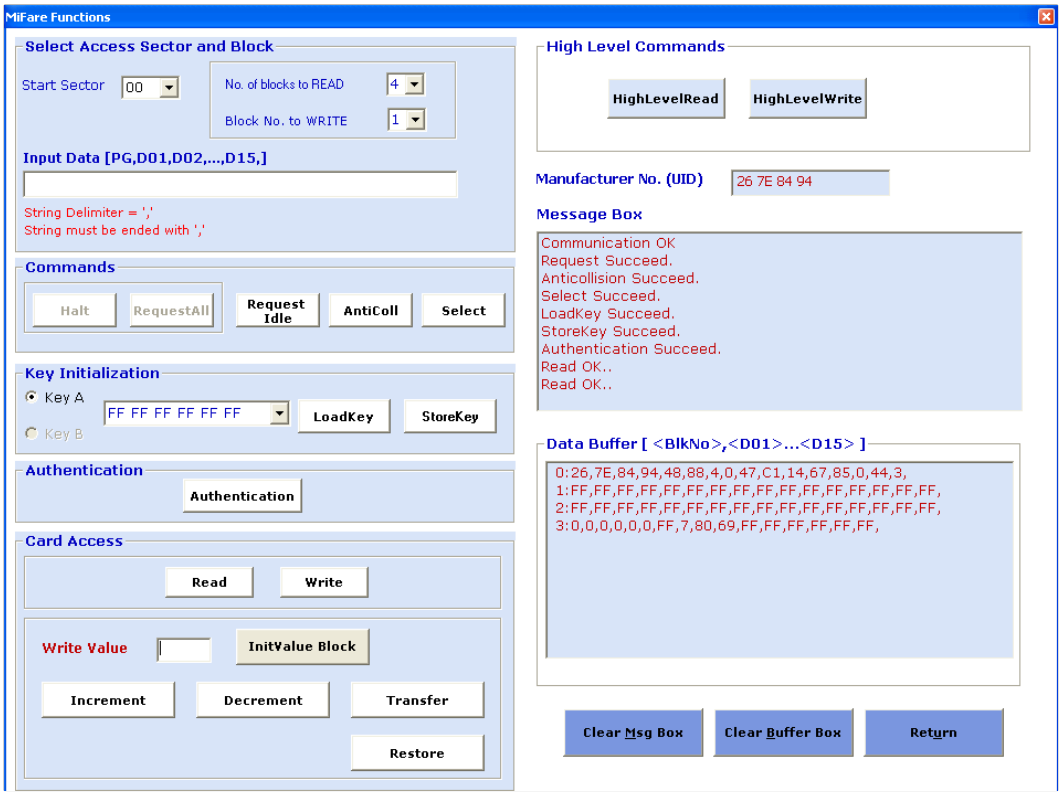

Figure 8: MiFare command screen

Mifare commands:

Procedure

In this section you are required to carry out few MiFare commands to test with the **five** MiFare cards.

1. Launch the MiFare Function window by clicking the MiFare button at Main screen.
2. Place one of the MiFare cards on the reader.
3. From the MiFare Function window, Select Sector number (Default sector "0") > Select number of blocks to Read (Default "1"), Then, click **Request All** > **Anti-Collision** > **Select** > **Load Key** > **Authentication** > **Read**. This sequence will read the **4** bytes UID (Unique Identifier) of the MiFare card that cannot be modified by user. Record the UID of the card in Table 2.
4. Repeat the step 2 and 3 with others four MiFare cards.

Card No.	UID	Remark
1		
2		
3		
4		
5		

Table 2

5. **Read** the data block 0 to 3 of sector 0 of the one of the cards. Record the data in the Table 3.

Setting: Start sector: _____No. of Block to READ: _____,

Data:

Block 0:

Block 1:

Block 2:

Block 3:_____.

6. **Write** the data block of the card no. 1 with the data "A,B,C,D,A,B,C,D,A,B,C,D,A,B,C,D," at the block no. 12 of sector 3 and record the required setting and the whole sequence.

Setting: Start sector: _____Block No. to WRITE: _____.
Sequence: _____
_____.

The following step **7 to 12 are optional**. These are for advanced users.

7. **HighLevelRead** command: High Level Read command combines all the necessary steps needed to carry out reading each block in a single command. Before carrying out using the HighLevelRead command, the Key has to be loaded by Store Key command. The required sector and number of blocks can be chosen in the Select Access Sector and Block Panel.
8. **HighLevelWrite** command: High Level Write Command combines all the necessary steps for writing to a memory block in a single command. As the HighLevelRead command, the key has to be loaded by Store Key command to the requested block.

9. **InitValue Block** command**:** Create and initialize a Value Block in card memory. Select sector number and write Block number from Access Sector and Block Panel to define value block. Since it is a memory operation to the card, the sequential commands of RequestIdle, AntiColl, Select, Authentication and also LoadKey are required to be carried out before this InitValue Command. The Mifare Init Value Block will be created with Mifare Value Block Format.
10. **Increment** command: Add input value to the specified value block. The incremented valued which is stored in MiFare Reader Chip internal value buffer register, will not be written to the Value Block until Transfer command is sent.
11. **Decrement** command: Decrease input value from the specified value block. Decremented value will be updated only after Transfer command is sent. Otherwise value will be still in the internal value buffer register. Before Increment and Decrement commands, the Value Block must be first formatted with the MiFare Value Block Format with InitValue Block Command.
12. **Transfer** command**:** To transfer the data from MiFare Reader's internal Value buffer register to the selected value block.

Questions:

1. What are the basic components of an RFID reader?

2. What are the modules required for an RFID system?

3. What is the maximum size of memory bytes for **user data** of I-Code RFID tag?

4. Understand the select function and describe the command sequence of a select function for the I-Code card.

5. What is the maximum size of memory bytes for the MiFare RFID tag?

6. Describe the command sequence of a MiFare Write operation.

7. Compare the security features of I-Code and MiFare cards.

8. What is the RF frequency used in I-Code system?

9. What is the RF frequency used in MiFare system?

10. Measure the reading range of I-Code and MiFare Card using a ruler and compare their ranges.

11. Draw a table as follow and make comparison between I-Code and MiFare Cards base on their characteristics, features and applications.

Serial No.	Descriptions	I-Code	MiFare	Remarks
1	Frequency			
2	Anti-collision			
3	UID			
4	Memory Size			
5	Security			