

This document descripts how to use SIC43NT PC software with SIC PI931 for evaluating and exploring various features of SIC43NT.

### **Revision History**

Revision	Date	Software	Description/Change/Updated/Comment	Product
	Dute	Version		Code
1.0	May 2017	1.1.1	1 <sup>st</sup> Release	SIC43NT
1.1	June 2017	1.1.4	Adding authenticate	

The information herein is for product information purpose. While the contents in this publication has been carefully checked; no responsibility, however, is assumed for inaccuracies. Silicon Craft Technology Co., Ltd. reserves the right to make changes to the products contained in this publication in order to improve design, performance or reliability.

# Contents

1.	Intr	roduction	5
2.	Get	tting Start	5
	2.1	System and Hardware requirements	5
	2.2	Software Installation	6
3.	Qui	ick Stat with Demonstration Software	7
4.	Den	monstration Software	9
	4.1	Port setup and software information	9
	4.1.1	1 Open Port	10
	4.1.2	2 Close Port	10
	4.1.3	3 Tools	11
	4.1.4	4 Help	11
	4.2	Get transponder information	12
	4.2.1	1 Initial	12
	4.2.2	2 Authentication	12
	4.2.3	3 NDEF Information	13
	4.2.4	4 Write Block and Read Block	14
	4.3	Configuration transponder	15
	4.3.1	1 Password Setting	15
	4.3.2	2 NDEF	16
	4.3.3	3 Rolling Code Mode	17
	4.3.4	4 RFD Pin Function	17
	4.3.5	5 Initial Vector, Rolling Code Key and Configuration Lock	19
	4.4	Transaction logs	20



# **List of Figures**

Figure 1 Pi-931 X34CC SIC Reader	5
Figure 2 Pi931 DemoSWManual	6
Figure 3 Demonstration Software 1	Error! Bookmark not defined.
Figure 4 Demonstration Software 2	Error! Bookmark not defined.
Figure 5 COMPORT	8
Figure 6 Example NDEF information	8
Figure 7 Sections in Demonstration software	Error! Bookmark not defined.
Figure 8 Port setup and software information	9
Figure 9 Open Port Menu	10
Figure 10 connected com port and communication speed (kbps)	10
Figure 11 closed com port	10
Figure 12 Tools menu	11
Figure 13 Help menu	11
Figure 14 firmware and software information	Error! Bookmark not defined.
Figure 15 Get Information Session	
Figure 16 Get UID of transponder	
Figure 17 Authenticate	
Figure 18 Example NDEF Information	
Figure 19 Write Block and Read Block	14
Figure 20 Example Read Block	14
Figure 21 Configured Session	15
Figure 22 Password Setting	Error! Bookmark not defined.
Figure 23 NDEF Setting	16
Figure 24 NDEF Type	16
Figure 25 Dynamic Data	16
Figure 26 Rolling Code Mode	17
Figure 27 RF Detection	17
Figure 28 Tamper Detection	
Figure 29 Initial Vector	19
Figure 30 Rolling Code Key	19
Figure 31 Configuration Locked	19
Figure 32 Example Transaction logs	20



# List of Tables

Table 4-1 NDEF Types	
Table 4-2 Rolling Code Mode	
Table 4-3 RF Detection Mode	
Table 4-4 Tamper Detection Mode	



# 1. Introduction

The Pi-931 is a series of miniaturized 13.56MHz RFID reader module. Based on high-performance RFID contactless reader IC SIC9310 from Silicon Craft Technology.



Figure 1 Pi-931 X34CC SIC Reader

This manual describes how to use demonstration software with Pi931-X34CC for evaluating SIC43NT transponder. This software is based on basic command in the standard ISO14443A.

# 2. Getting Start

Before user can operate the demonstration, proper operational environment and the following requirements must be prepared.

## 2.1 System and Hardware requirements

- Computer
- : PC
- Operating System
- RFID Reader
  - Software Requirement:
- Others

- : PC with USB Port
- : Window XP, Window 7, 8, 10
- : Pi-931 Reader
- : .NET framework version higher than 4.0 Installed
- : Card, Tag, DC Adaptor (if it is required in some model)



## 2.2 Software Installation

Refer to document "SIC\_PD\_DTS\_0009\_Pi93\_DemoSWManual\_Rev2\_0\_20121115"

Demonstration Software	User Manual	
Copyright © 2010, All Rights Res No part of this publication may b means, or stored in a data b permission from Silicon Craft Co.	erved be reproduced or distri base or retrieval syst , Ltd.	buted in any form or by any em, without prior written
Silicon Craft Co., Ltd. www.sic.co.th		

Figure 2 Pi931 DemoSWManual

# 3. Quick Stat with Demonstration Software

The demonstration software is "" SIC43NT Configuration Software.exe" There is no software setup required. The demonstration software can run either from hard drive. The GUI of software is shown in Figure 22 and ready to use.

Get li	nformation Session		Config	urad Session		
Get ii	niormation Session		Coning	jured Session		
	Authentication					
	Password	Password Setting		HFD Pin Function		
tus Req Anti	Select Status Author	n ( ) Disable		RF Detection		
1.7		C Enable	0.5.10	Ingger Event	No	O Select
ntormation		Protection  Write Only	O Read/Write	Sleep Mode	Ist SOF	O Freseni
Туре	lamper Mode	Protected Address	uun-sun	Detect Mode	Disable	
Flag Value	Rolling Code Mode	Password	8 HEX Characters	Output Type Mode		O Putto
essage		Password ACK	0000h-FFFFh	ouput type mode	Openbrain	U Push-Pui
	Read NDEF	Authen Limitation	0-7, 0 is no limit	Tamper Detection		
lock	Read Block			Tamper Flag Value	(A.	SCII)
(HEX)	Block (HEX)	NDEF Message		Tamper Bias Current	6.4 uA	🔘 1.6 uA
(HEM)		NDEE Type UBL	V U		○ 3.2 uA	○ 0.8 uA
				Check Tamper Mode	Continue	PowerUp
\ \	Write Rea	Put S{DYN} for c	dynamic, NDEF data	Auto Program Tamper	Disable	<ul> <li>Enable</li> </ul>
		Dynamic Data		Pin		
		Dynamic Provider VIIID V	Tdata 🔽 Bolling Code	1/0	Туре	
		Pointer Page 7	Bute 0	Function		
		Tomos Tago	5,10			
		Rolling Code Mode		Initial Vector (HEX)		
		<ul> <li>Rolling Code is always fixed</li> </ul>				
		<ul> <li>Rolling Code runs when tamper eviden</li> </ul>	ce is detected	Rolling Code Key (HEX)		
		<ul> <li>Rolling Code runs when tamper eviden</li> </ul>	ce is NOT detected			
		<ul> <li>Rolling Code will run regardless of the t</li> </ul>	amper status	Configuration Looked		
		01.1				
		Status				Program

Figure 3 Demonstration Software 1

Get In	formation Session			Config	gured Session 🥑		
tial	Authentication	(4) Configuration					
	Password	Password Setting			RFD Pin Function		
Status Reg Anti S	Select Status Aut	e Disable			RF Detection		
		O Enable			Trigger Event	No     No	O Select
DEF Information		Protection	Write Only	<ul> <li>Read/Write</li> </ul>	21 M J	O 1st SOF	O Present
EF Type	Tamper Mode	Protected Address		00h-30h	Sleep Mode	() Disable	O Enable
mper Flag Value	Rolling Code Mode	Password		8 HEX Characters	Detect Mode	( ) Manual	<ul> <li>Auto</li> </ul>
ef Message	0	Password ACK		0000h-FFFFh	Output Type Mode	<ul> <li>OpenDrain</li> </ul>	<ul> <li>Push-Pull</li> </ul>
	5 Read NDEF	Authen Limitation		0-7, 0 is no limit	O Tamper Detection		
ite Black	Read Block				Tamper Flag Value	(A	SC11)
ale duck	Diada diCX	NDEF			Tamper Blas Current	(i) 6.4 uA	🔿 1.6 uA
		NDEE Tures	URI	10		🔿 3.2 uA	🔘 0.8 uA
ta (HEX)		NDEF type	UNL		Check Tamper Mode	Ontinue	O PowerUp
W	Vrite Re	ad University	D. + eloval (+-	NDEE Jake	Auto Program Tamper	① Disable	<ul> <li>Enable</li> </ul>
		Denvis Data	Fut \$10 HN/ for dy	Namic NUCF data	Pin		
		Dynamic Data	Di un tri	En la	1/0	Туре	
		Dynamic Provider		Idata M Kolling Code	Function		
		Pointer	Page 7	Byte U			
		Rolling Code Mode			Initial Vector (HEX)		
		Rolling Code is alw	aya fixed				
		Rolling Code runs v	when tamper evidence	e is detected	Rolling Code Key (HEX)		
		Rolling Code runs v	when tamper evidence	e is NOT detected			
		(ii) Rolling Code will rul	n regardless of the ta	mper status			
	0		0		Configuration Locked	-	
	(7)		(9)			(10)	

Figure 4 Demonstration Software 2





1) Connect a Pi-931 device to comport and wait until computer recognize COMPORT as shown in Figure 24. Then, click "OPEN PORT" Manu tap to query available COMPORT in computer.

🙎 SIC43NT Configuration Software





Available COMPORT in computer is shown. Click the COMPORT number belonging to reader hardware. If connection successful, there will be the connected comport with communication speed displayed at the bottom of the GUI.

- 2) Click "**Req Anti Select**" to get transponder UID. UID will be shown in the UID tab above.
- 3) Show status of Req-Anti-Coll command. Green means transponder has been requested. Red means it cannot get transponder UID.
- 4) Authenticate transponder to access the configuration or memory. Fill password and then click "**Authen**" for authentication.
- 5) Read NDEF information part by click "Read NDEF". Example NDEF data is shown in Figure 25

NDEF Information			
NDEF Type	URL	Tamper Mode	Power Up
Tamper Flag Value	00	Rolling Code Mode	Mode 3
Ndef Message	http://www.si	c.com/3949FFFF000087000	0000F5E8F39E
		Re	ad NDEF

Figure 6 Example NDEF information

- 6) Read others information in transponder or write data to transponder.
- 7) Save LOG or clear LOG
- 8) Configuration part to configure the transponder such as NDEF message, Password setting, Tampering mode etc.
- 9) Show status of configuration part. Green means successful configuration. Red means configuration is fail.
- 10) Click "Program" to set up transponder.

The information herein is for product information purpose. While the contents in this publication has been carefully checked; no responsibility, however, is assumed for inaccuracies. Silicon Craft Technology Co., Ltd. reserves the right to make changes to the products contained in this publication in order to improve design, performance or reliability.

# 4. Demonstration Software

This software mainly consists of four sections as shown in Figure 26 namely.

- 1) Port setup and software information
- 2) Get transponder information
- 3) Configuration transponder
- 4) Transaction logs

Get Information Session		Configured	Session		
al Authentication	Configuration				
Password	Password Setting	I	RFD Pin Function		
atus Reg Anti Select Status Auth	Disable		RF Detection		
	O Enable		Trigger Event	No	<ul> <li>Select</li> </ul>
F Information	Protection    Write Only	) Read/Write		O 1st SOF	O Present
F Type Tamper Mode	Protected Address	00h-30h	Sleep Mode	Disable	🔘 Enable
er Flag Value Rolling Code Mode	Password	8 HEX Characters	Detect Mode	(i) Manual	🔿 Auto
Message	Password ACK	0000h-FFFFh	Output Type Mode	OpenDrain	O Push-Pull
Read NDEF	Authen Limitation	0-7, 0 is no limit	Tamper Detection		
- Dead Deals			Tamper Flag Value	(A.	SC11)
e block nead block	NDEF		Tamper Blas Current	(i) 6.4 uA	🔿 1.6 uA
	NDEF Message			🔘 3.2 uA	🔘 0.8 uA
(HEX)	NDEP Type One O		Check Tamper Mode	Ontinue	O PowerUp
Write Re:	ad ORI/ORL (ASC/)	NOTE	Auto Program Tamper	Disable	🔿 Enable
	Fut s(D TN) for dynami	s NUEF data	Pin		
0	Dynamic Data	Rob Ch	1/O	Туре	
4)	Dynamic Provider 💟 DiD 💆 Toata	I M Rolling Code	Function		
	Pointer Page 7	Byte 0			
	Rolling Code Mode		Initial Vector (HEX)		
	Rolling Code is always fixed				
	<ul> <li>Rolling Code runs when tamper evidence is a</li> </ul>	etected	Bolling Code Key (HEX)		
	Rolling Code runs when tamper evidence is f	IOT detected			
	Rolling Code will run regardless of the tamper	status			
			Configuration Locked		
	Status				Program

Figure 7 Section in Demonstration Software

## 4.1 Port setup and software information

This section consists of Menus related to hardware setup namely OPEN PORT, CLOSE PORT, GET FW VERSION and ABOUT.



Figure 8 Port setup and software information



## 4.1.1 Open Port

**Open Port** is used to query and open communication port to the reader device.



Figure 9 Open Port Menu

Following steps describe opening the communication port with Pi-931.

- Click **Open Port** menu to search available com port present in computer.
- Available COM ports are shown in menu content under **open Port** menu.
- Click on the COM port number belonging to reader hardware being operated to open communication.
- If connection is successful, there will be a connected comport with communication speed displayed at bottom of the GUI, as shown in Figure 29.

		Save	Clear
Open COM3 115200			

Figure 10 connected com port and communication speed (kbps)

### 4.1.2 Close Port

**Close Port** is used to close current communication port.

- Click **CLOSE PORT** to close current operating COM port.
- The connection shown at bottom of the GUI indicated that the comport was closed, as shown in Figure 30.

	Save
COM3 Closed	

Figure 11 closed com port

## 4.1.3 Tools

Tools is used to control the field of SIC PI931 ightarrow on field, off field or reset field

SIC43NT Configuration Software						
Open Port	Close Port	Tools	Help			
	Ge	0	n Field	ssion		
Initial		Re	eset	tication -		
UID						



### 4.1.4 Help

Help is shown about software information

🙎 SIC43NT (	Configuration	Software	2		
Open Port	Close Port	Tools	Help		
	Ge	et Infor		About	

Figure 13 Help menu

- Show firmware version
- Show software version
- Can access to our website



Figure 14 Firmware and Software information



## 4.2 Get transponder information

Initial UID Status Reg Anti	Authentication Password Select Status	Auther
NDEF Information NDEF Type Tamper Rag Value	Tamper Mode Rolling Code Mode	
Ndef Message		Read NDEF
Write Block Block (HEX)	Read Block Block (HDQ)	

Figure 15 Get Information Session

## 4.2.1 Initial

"Req Anti Select" button to get UID of transponder

Initial	
UID	3949FFFF000087
OK	Req Anti Select

Figure 16 Get UID of transponder

## 4.2.2 Authentication

Fill password and then click "Authen" button to authenticate transponder in order to access its memory.

Authenticatio	n	
Password	FFFFFFF	
PASS		Authen

Figure 17 Authenticate



### 4.2.3 NDEF Information

NEFD information is shown NDEF message in transponder

NDEF Information			
NDEF Type	URL	Tamper Mode	Power Up
Tamper Flag Value	00	Rolling Code Mode	Mode 3
Ndef Message	http://www.si	c.com/3949FFFF000087000	000101BDD4C
		Rea	ad NDEF



4.2.3.1 NDEF Type NFC Data Exchange Format Type is shown in the table 1

Table 4-1 NDEF Types

NDEF Type	Description
URI/URL	Open URL via default browser
Plaintext	Record containing UTF-8 text data.
Application	Use Package name to Open Application.
Mail	NDEF record used to prompt the creation of a new email on the device.
Contact	Share contact data using the vCard 2.1 data format.
Phone number	Record phone number.
SMS	Write message and prepare to send to
Location	Display a geographic point in a mapping application on the device.
Address	Record address
Bluetooth connection	Pairing device via Bluetooth by using MAC address
Wi-Fi direct	Connect Wi-Fi
Custom record	Customize NDEF message

- **4.2.3.2 Tamper Flag Value** Tamper status that store in the memory. This value is recommended to be in readable ASCII format.
- 4.2.3.3 Ndef Message NDEF message that store in transponder's memory
- **4.2.3.4 Tamper Mode** Tampering checking mode can be 2 modes; Check Tampering Continuously and Check Tampering at Power up.



**4.2.3.5** Rolling Code Mode Rolling Code rule is shown in table 4-2.

Table 4-2 Rolling Code Mode

Mode	Description
0	Rolling Code is always fixed
1	Rolling Code runs when tamper evidence is detected
2	Rolling Code runs when tamper evidence is <b>NOT</b> detected
3	Rolling Code will run regardless of the tamper status(default)

## 4.2.4 Write Block and Read Block

Write Block	Read Block
Block (HEX)	Block (HEX)
Data (HEX)	
Write	Read

Figure 19 Write Block and Read Block

Write or read data in memory of transponder. The user memory is separated in to 36 blocks. Each block is 4 bytes. Read block command are shown data 16 bytes start at that block number as in Figure 39.

Write Block	Read Block			
Block (HEX)	Block (HEX) 7			
Data (HEX)	6F6D2F33393439464646463030303038			
Write	Read			
- Command> Read Block: 0x07 Transfer> 3007 Response> 6F6D2F33393439464646463030303038 Transmission Completed				

Figure 20 Example Read Block



(1)				
Password Setting		RFD Pin Function		
Disable		RF Detection		
O Enable		Trigger Event	No	O Select
Password (HEX)			) 1st SOF	Present
Password ACK	0000h-FFFFh	Sleep Mode	<ul> <li>Disable</li> </ul>	<ul> <li>Enable</li> </ul>
Protected Address	00h-30h	Detect Mode	Manual	O Auto
Authen Limitation	0-7, 0 is no limit	Output Type Mode	OpenDrain	O Push-Pul
NDEE		O Tamper Detection		
NDEF Message		Tamper Flag Value	(A	SCII)
NDEF Type URL	~ U	Tamper Bias Current	(e) 6.4 uA	🔿 1.6 uA
URI/URL (ASCII)			O 3.2 uA	🔘 0.8 uA
Put s{DYN	I) for dynamic NDEF data	Check Tamper Mode	Ontinue	O PowerUp
Dynamic Data		Auto Program Tamper	Disable	🔘 Enable
Dynamic Provider VID	Tdata Rolling Code	Pin		
Pointer Page	5 Byte 3	I/O Output	Туре	Open Drain
		Function Pull low when	RF field is detected	
Bolling Code Mode				
Bolling Code is always fixed		Initial Vector (HEX)		
Rolling Code to almoyer tool				
Rolling Code runs when tamper e				
Poling Code will an manuface a	files towner at the			
Trolling Code will fail regaratess o				
		Configuration Locked		
Status				Drogram

## 4.3 Configuration transponder

Figure 21 Configured Session

## 4.3.1 Password Setting

This password will protect memory from unauthorized modification. It consists of 4 parts in this setting.

🗹 Pa	assword Setting		
(	) Disable		
(	Enable		
	Protection	Write Only	○ Read/Write
	Protected Address		00h-30h
	Password		8 HEX Characters
	Password ACK		0000h-FFFFh
	Authen Limitation		0-7, 0 is no limit

#### Figure 22 Password Setting

4.3.1.1	Protection	Protection Configure
4.3.1.2	Password	4 Bytes data
4.3.1.3	Password ACK	The respond when SIC43NT receive a matched password
4.3.1.4	Protected Address	Start protected area
4.3.1.5	Authen Limitation	Limitation of negative password





### 4.3.2 NDEF

NDEF message is stored in SIC43NT's memory including rolling code.

NDEF NDEF Message			
NDEF Type	URL	~ U	
URI/URL (ASCII)			
	Put \${DY	N} for dynamic N[	DEF data
Dynamic Data			
Dynamic Provider		🗹 Tdata	Rolling Code
Pointer	Page	5	Byte 3

Figure 23 NDEF Setting

#### 4.3.2.1 NDEF Message

NDEF Type	URL 🗸
URI/URL (ASCII)	Text
	Bluetooth Application
Dynamic Data	CustomMIME

Figure 24 NDEF Type

The NDEF message can be many types. In this software can set NDEF message be URL, Text, Bluetooth, Application or CustomMIME.

### 4.3.2.2 Dynamic Data

Choose Dynamic data that is a part in NDEF message. Tdata is tamper status and Rolling Code is generated from rolling code key and time stamp.

Dynamic Data				
Dynamic Provider		🗹 Tdata	🗹 Rolling	Code
Pointer	Page	5	Byte	3





## 4.3.3 Rolling Code Mode

Rolling code mode is for controlling the dynamic NDEF message. Rolling Code action can be controlled by refer to tamper status.

Rolling Code	Mode
--------------	------

O Rolling Code is always fixed

O Rolling Code runs when tamper evidence is detected

O Rolling Code runs when tamper evidence is NOT detected

Rolling Code will run regardless of the tamper status

Figure 26 Rolling Code Mode

## 4.3.4 **RFD Pin Function**

SIC43NT RFD Pin can be set as 2 functions.

#### 4.3.4.1 RF Detection

RF detection is detected when the transponder is in represent field of reader or NFC phone.

RF	D Pin Function		
0	RF Detection		
	Trigger Event	<ul> <li>No</li> <li>1st SOF</li> </ul>	<ul> <li>Select</li> <li>Present</li> </ul>
	Sleep Mode	Disable	O Enable
	Detect Mode	Manual	<ul> <li>Auto</li> </ul>
	Output Type Mode	OpenDrain	O Push-Pull

Figure 27 RF Detection

Table 4-3 RF Detection Mode

## **RF** Detection Mode

RF detection	Items	Description		
Trigger Event	No Field Detect	No RF field present		
	1 <sup>st</sup> SOF	First Start of Frame		
	Select	Select state		
	Field Present	RF field present		
Sleep Mode	Disable	None sleep		
	Enable	Sleep Enable		
Detect Mode	Manual	Manual Configuration Pin behavior define from		
		Output Type		
	Auto	Auto Detect		
Output Type Mode	Open Drain	Pull low when RF field is		
		detected		
	Push Pull	Logic high when RF field is detected		





### 4.3.4.2 Tamper Detection

Tamper Detection	n			
Tamper Flag Valu	ie 🗌	(	(ASCII)	
Tamper Bias Curr	ent 🔘	) <b>6.4 u</b> A	0	1.6 uA
	С	) 3.2 uA	0	0.8 uA
Check Tamper M	ode 💿	) Continue	0	PowerUp
Auto Program Ta	mper 🔘	) Disable	0	Enable
Pin				
I/O Input		Туре	Input	
Function Tamp	ering detection r	mode		

Figure	28	Tamper	Detection
--------	----	--------	-----------

Table 4-4 Tamper Detection Mode

TP detection	Items	Description
Tamper Flag	-	HEX data for Tamper status
Tamper Bias Current	6.4 uA	Current detect tamper
	3.2 uA	status
	1.6 uA	
	0.8 uA	
Check Tamper Mode	Continue	Always check tamper pin
	Power up	Check only power up
Auto Programing Tamper	Disable	Doesn't program status to
		EEPROM
	Enable	Program status to EEPROM

## **Tamper Detection Mode**



## 4.3.5 Initial Vector, Rolling Code Key and Configuration Lock

### 4.3.5.1 Initial Vector

The 32 bits Initial Vector **IV** serves an initial value for the Time Stamp. The data in this address will be automatically updated for generating next rolling code

✓ Initial Vector (HEX)

Figure 29 Initial Vector

### 4.3.5.2 Rolling Code Key

The rolling code generator uses 10 bytes of **KEY** 

Rolling Code Key (HEX)

Figure 30 Rolling Code Key

### 4.3.5.3 Configuration Lock

Lock the configuration to ensure that no one can change the setting.

Configuration Locked

Figure 31 Configuration Locked



## 4.4 Transaction logs

Transaction log is shown each command that send through reader to SIC43NT and respond from transponder

Setup Reader => Complete Communicate! ISO14443A => Complete Communicate! Request Anti-Coilsion Selection => Complete Communicate! Response> 01 - Resp OK UID Cascade> 2 Level - (UID 7 Bytes) SAK> 00 - UID Complete ,Not compliant Lv4 UID> 3949FFFF000087		^
- Command> Read Tamper Transfer> AF00 Response> 000000000000000000000000000000000000		
- Command> Read Register -> Block: 0x29 Transfer> 3029 Response> 313007FF293018F80000000000000000 Transmission Completed		
- Command> Read NDEF -> Block: 0x04 Transfer> 3004 Response> 032DD1012955017369632E636F6D2F33 Transmission Completed	Save	Clear

Figure 32 Example Transaction logs

