SIC43NT

NFC Type-2 Tag IC with 144-byte user memory and a configurable pin for RF field detection or tamper evidence detection

REV 3.1

Features Summary

Highlight Features

- NFC Forum Type 2 Tag
- A configurable pin for three modes of operation
  - RF field detection
  - Tamper evidence detection
  - Sleep mode
- Dynamic NDEF message
  - contains UID, tamper evidence message, and rolling code
  - mirrored into original NDEF message
  - can be triggered by tamper status of the tag
- Password protection
- Tag authenticity verification using rolling code (optional)
- Secured tamper status decoding to prevent message counterfeiting (optional)

Memory

- Factory programmed 7-byte UID
- Lock bytes with anti-tearing protection
- 144-byte user memory
- Dedicated memory for configuration functions: Password authentication, Pin configuration, and Rolling code configuration
- Dedicated memory for timestamp and tamper status
- EEPROM organization enabling NDEF TLV messages
- EEPROM erase/write cycle up to 500,000 times
- EEPROM memory retention up to 10 years

Operating Condition

- 13.56MHz operating radio frequency
- Operating temperature from -40 to 85°C

Interfaces and Peripherals

- RF interface based on ISO14443A, 106 kbps data rate
- True anti-collision
- Configurable output type in RF detection mode
  - Open-Drain Mode
  - 1.8V-Output Mode
- On-chip capacitance 50 pF

Packages

- 8” Die-On-Wafer with Au-Bump

Supplementary

- Wafer map - XML, TXT, SECSII
- UID summary

Applications

- Anti-tampering sticker and label
- Smart packaging
- Vouchers and coupons
- Product authentication
- NFC-wakeup devices and appliances
- Bluetooth and Wi-Fi pairing
- Toys

Copyright © 2020 Silicon Craft Technology PLC

Revision History

Revision	Date	Description	Change/Update/Comment
2.0	13 Sept 2018	Content Update	• Add Package and Dimension • Add Wafer ring Dimension
3.0	27 Aug 2021	Content Update	• Update Features for SIC43NT Rev G • Add Ordering Information • Add Block Diagram • Add Typical Operating System • Add EEPROM memory map • Add Rolling Code Generator
3.1	24 Feb 2022	Content Update	• Update Part No. in Ordering Information

Copyright © 2020 Silicon Craft Technology PLC

Ordering Information

Part No.	Revision	Description
PNTGDC4PA20SRNT01R5	G	SIC43NT, Die on wafer, Tested, Bump, 276mm, UV, 4mils polishing, Dice
PNTGDC6PA20SRNT01R2	G	SIC43NT, Die on wafer, Tested, Bump, 276mm, 6mils polishing, Dice
PNTGDC6PA20SRNT01R5	G	SIC43NT, Die on wafer, Tested, Bump, 276mm, UV, 6mils polishing, Dice
PNTGDC80A20SRNT01R2	G	SIC43NT, Die on wafer, Tested, Bump, 276mm, 8mils, Dice
PNTGDC80A20SRNT01R5	G	SIC43NT, Die on wafer, Tested, Bump, 276mm, UV, 8mils, Dice

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

Copyright © 2020 Silicon Craft Technology PLC

Functional Overview

SIC43NT is an NFC Forum Type 2 Tag IC with web-based authentication feature and the RF detection pin **RFD**, The RF detection pin can be configured to operate in RF detection mode to wake-up the MCU system from sleep state, or in tamper evidence detection mode for anti-tampering application.

Block Diagram

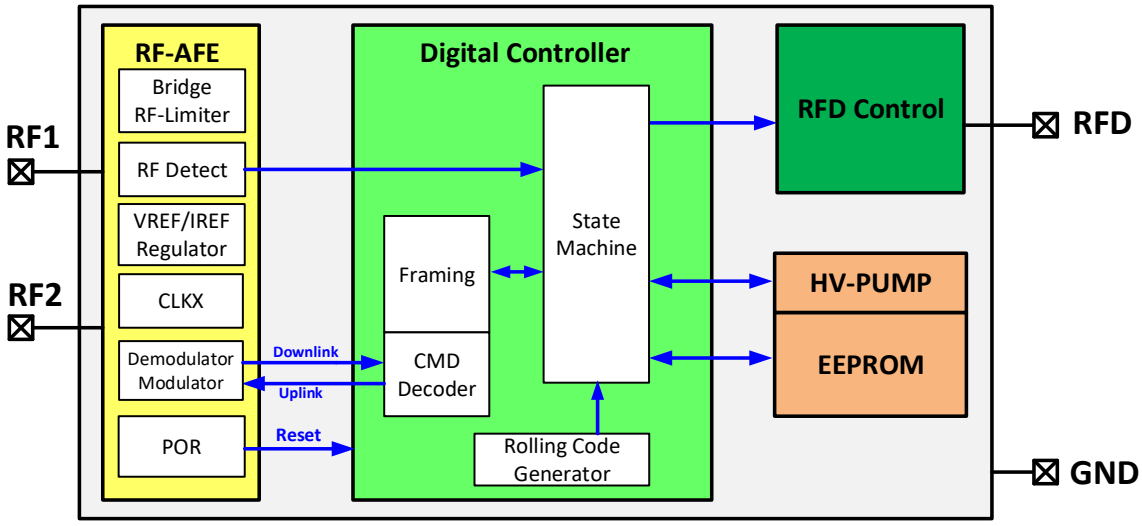

Figure 1: Functional Block Diagram

Figure 1 shows a conceptual block diagram of SIC43NT which consists of four parts

The RF Analog-Front-End (RF-AFE), which has RF1 and RF2 terminals for connecting to an external coil, harvests RF power to supply the internal circuit. The RF-AFE provides facilities for RF communication such as a Modulator for uplink data communication, a Demodulator for downlink data communication, a clock extractor for system clock and data synchronization, and a RF field detector for detecting the presence of RF field.

The digital controller controls data transaction between the RF-AFE and the EEPROM. The digital controller handles the following operations:

- Decoding incoming RF downlink commands and encoding RF uplink data/response
- Reading and programming data from/to the EEPROM
- In RF detection mode, generate output to pin RFD corresponding to RF field
- In tamper detection mode, monitor status at pin RFD and store it into EEPROM
- Generate rolling code
- In sleep mode, monitor status at pin RFD and enter sleep state

The EEPROM memory is used to store an UID, user data, and a memory lock control bit to serve NFC applications. The EEPROM also contains device configuration bits, configuration data for rolling code generator, and tamper evidence of the tag.

Depending on the configuration bits, pin RFD can be either an input or an output. For RF detection, the pin RFD is in output mode. For tamper evidence detection, it is in input mode. SIC43NT can enter sleep mode by tying the pin RFD to logic '0' before presence of RF field. The pin functionality and I/O type can be set via device configuration page.

Copyright © 2020 Silicon Craft Technology PLC

Typical Operating System

SIC43NT RFD pin can be configured to operate in different application as list below.

- RF field detection when I/O is set in an open drain mode (Figure 2)
- RF field detection when I/O is set in a 1.8V mode (Figure 3)
- Tamper evident detection (Figure 4)

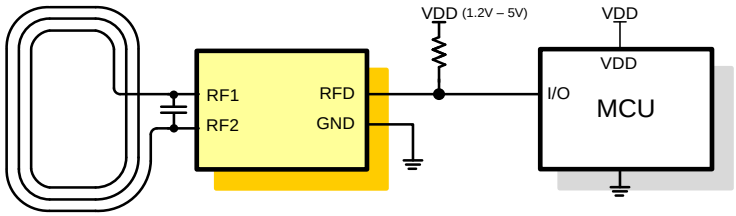

Figure 2: SIC43NT with RF detect pin operating in an open-drain mode

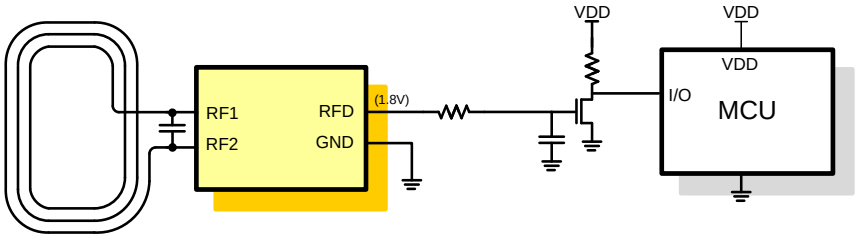

Figure 3: SIC43NT with RF detect pin operating in a 1.8V output mode

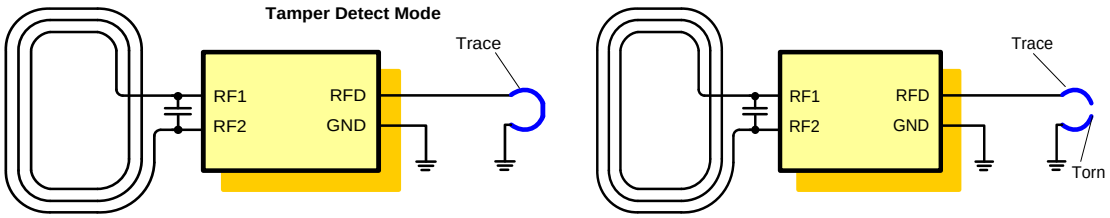

Figure 4: SIC43NT operating in tamper evident detection mode

Copyright © 2020 Silicon Craft Technology PLC

Packaging and Dimension

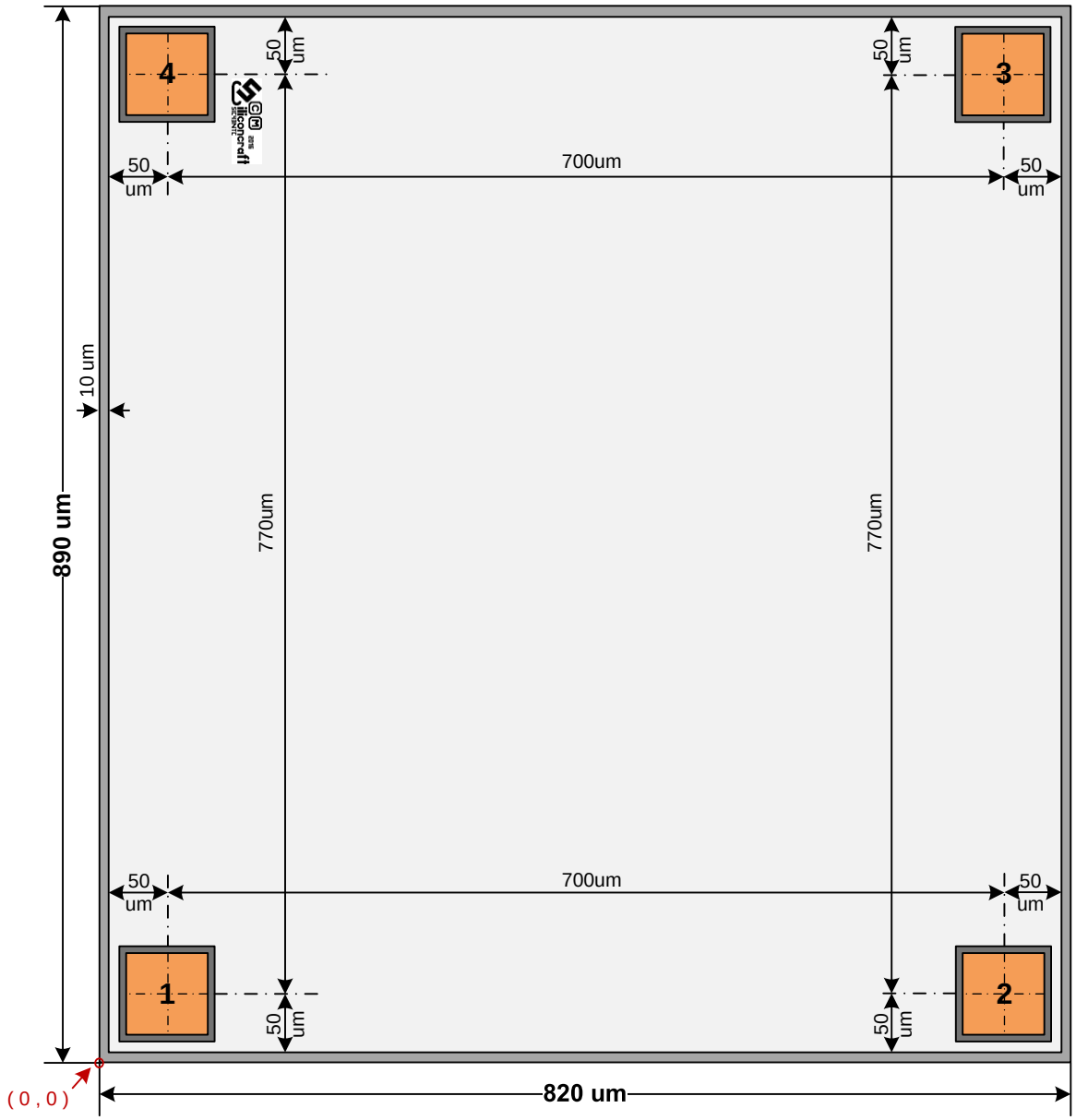

Figure 5: SIC43NT Die Dimension (Top View)

Copyright © 2020 Silicon Craft Technology PLC

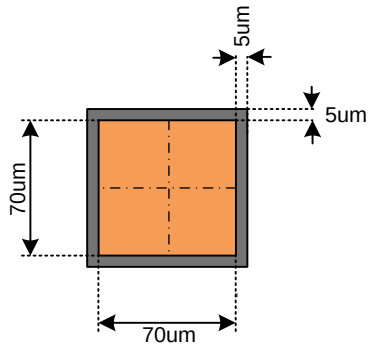

Figure 6: SIC43NT Pad Dimension (Top View)

Table 1: SIC43NT pad description

Pad	Symbol	Type	Center of Pad Co-Ordinate	Pad Size (µm)	Description
1	**RF1**	RF	(60, 60)	70x70	RF pin1 for coil connection
2	**RF2**	RF	(760, 60)	70x70	RF pin 2 for coil connection
3	**GND**	Power	(760, 830)	70x70	Ground
4	**RFD**	I/O	(60, 830)	70x70	RFD pin

Memory

Page (Hex)	Page (Dec)	Byte 0	Byte 1	Byte 2	Byte 3	Memory Type	Description	Note
0x00	0	UID0	UID1	UID2	BCC0	R/O	UID / Lock / CC	64-byte NFC Static Memory
0x01	1	UID3	UID4	UID5	UID6	R/O		
0x02	2	BCC1		Lock0	Lock1	R/O, R/W-(OTP)		
0x03	3	CC0	CC1	CC2	CC3	R/W-(OTP)		
0x04	4	Data R/W	Data R/W	Data R/W	Data R/W	R/W	48-byte User Data	
…	…	Data R/W	Data R/W	Data R/W	Data R/W	R/W		
0x0F	15	Data R/W	Data R/W	Data R/W	Data R/W	R/W		
0x10	16	Data R/W	Data R/W	Data R/W	Data R/W	R/W	96-byte User Data	NFC Dynamic Memory
…	…	Data R/W	Data R/W	Data R/W	Data R/W	R/W		
0x27	39	Data R/W	Data R/W	Data R/W	Data R/W	R/W		
0x28	40	Lock2	Lock3	Lock4		R/W-(OTP)	Lock Byte	
0x29	41	FDP	Tdata0	DYN_PAGE_PTR	AUTH0	R/W	Configuration 0	
0x2A	42	AUTHL	Tdata1	RFD_CFG	DYN_DATA_CFG	R/W	Configuration 1	
0x2B	43	PWD	PWD	PWD	PWD	W/O	Password	
0x2C	44	PACK	PACK			W/O	Password ACK	
0x2D	45	KEY9	KEY8	KEY7	KEY6	W/O	KEY9-6	
0x2E	46	KEY5	KEY4	KEY3	KEY2	W/O	KEY5-2	
0x2F	47	KEY1	KEY0			W/O	KEY1-0	
0x30	48	IV3	IV2	IV1	IV0	R/W	Initialization Vector	

Figure 7: SIC43NT EEPROM memory map

Copyright © 2020 Silicon Craft Technology PLC

Rolling Code Generator

Rolling Code Generator is a secure stream cipher operating as a pseudo-random generator. It uses 80 bits of KEY and 32 bits of Time Stamp (TS) stored in the EEPROM as inputs. Then, it generates 32 bits of rolling code (RND). The TS and RND are combined to create a 64-bit rolling code (RLC). Rolling code generation is enabled by setting **DYN_RLC_EN** bit to '1'.

To enhance security and integrity of the NDEF message, SIC43NT can be configured such that the value of rolling code RLC depends on tamper status of the tag. This feature is called "Secured Tamper Status Decoding". Users can select whether to include tag tamper status into RLC calculation by configuring bit **SEC_TAMPER_EN**.

With configuration bit **SEC_TAMPER_EN** set to '0', the generator uses only KEY and TS for RLC calculation (Figure 8)

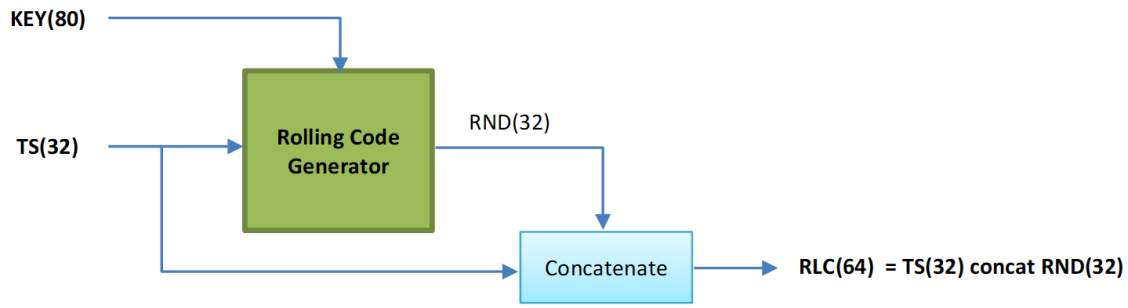

Figure 8: Rolling Code Generation Block Diagram when **SEC_TAMPER_EN** = '0'

With configuration bit **SEC_TAMPER_EN** set to '1', the generator is modified to include tag's tamper status into the calculation.

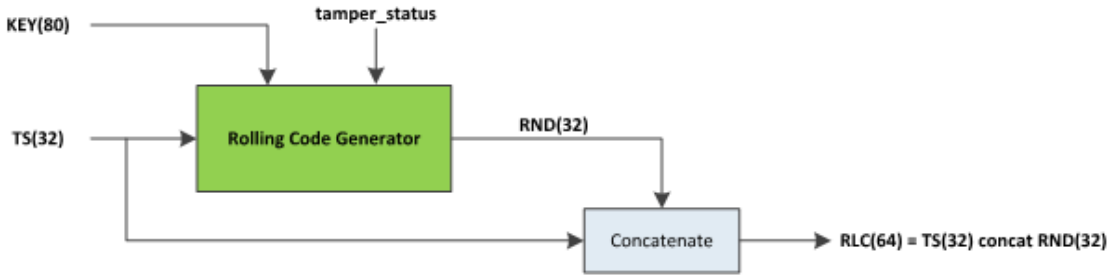

Figure 9: Rolling Code Generation Block Diagram when **SEC_TAMPER_EN** = '1'

Copyright © 2020 Silicon Craft Technology PLC