SHA-1/HMAC BASED SECURITY AND AUTHENTICATION IC WITH SDQ INTERFACE

FEATURES

- **Provides Authentication of Battery Packs Through SHA-1 Engine Based HMAC**
- **160 Bytes OTP, 16 Bytes EEPROM**
- **Internal Time-Base Eliminates External Crystal Oscillator**
- **Low Power Operating Modes:**
  - **Active: < 50 μA**
  - **Sleep: 8 μA Typical**
- **Single-Wire SDQ Interface**
- **Powers Directly From the Communication Bus**
- **6 Lead SON Package**

APPLICATIONS

- **Cellular Phones**
- **PDA and Smart Phones**
- **MP3 Players**
- **Digital Cameras**
- **Internet Appliances**
- **Handheld Devices**

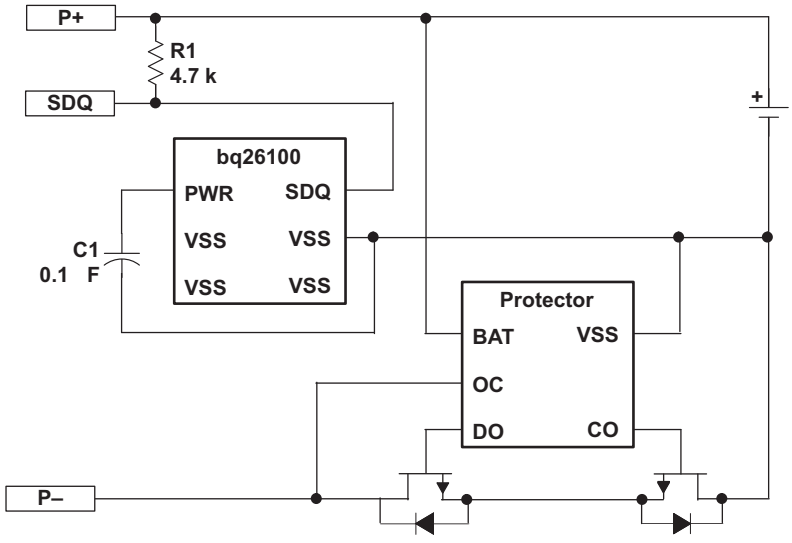
DESCRIPTION

The bq26100 provides a method to authenticate battery packs, ensuring that only packs manufactured by authorized sub-contractors are used in the end application. The security is achieved using the SHA-1 hash function inside the widely adopted HMAC construction. A unique 128-bit key is stored in each bq26100 device, allowing the host to authenticate each pack.

The bq26100 communicates to the system over a simple one-wire bi-directional m /F4 -10 Tf .0.6.d .d0.6 /F4 -10 Tf (x24.f

line via an external capacitor.

TYPICAL APPLICATION



Please be aware that an important notice concerning availability, standard warranty, and use in critical applications of Texas Instruments semiconductor products and disclaimers thereto appears at the end of this data sheet.

PRODUCTION DATA information is current as of publication date. Products conform to specifications per the terms of the Texas Instruments standard warranty. Production processing does not necessarily include testing of all parameters.

Copyright © 2006–2007, Texas Instruments Incorporated

ORDERING INFORMATION(1)

T_A	PACKAGE	PART NUMBER
–40°C to 85°C	6-lead SON	bq26100DRP

(1) For the most current package and ordiering information, see the Package Option Addendum at the end of this document, or see the TI Web site at www.ti.com.

ABSOLUTE MAXIMUM RATINGS(1)

		VALUE	UNIT
	Supply voltage (SDQ all with respect to VSS)	–0.3 to 7.7	V
	Output current (SDQ)	5	mA
T_A	Operating free-air temperature range	–40 to 85	°C
T_{stg}	Storage temperature range	–65 to 150	°C
T_J	Junction temperature range	–40 to 90	°C
	Lead temperature (Soldering, 10 sec)	300	°C

(1) Stresses beyond those listed under *absolute maximum ratings* may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated under *recommended operating conditions* is not implied. Exposure to absolute-maximum-rated conditions for extended periods may affect device reliability.

RECOMMENDED OPERATING CONDITIONS

over operating free-air temperature range (unless otherwise noted)

		MIN	MAX	UNIT
V_{sdq}	Pull-up voltage	2.5	5.0	V
T_J	Operating free-air temperature range	–40	85	°C

ELECTRICAL CHARACTERISTICS

all parameters over operating free-air temperature and supply voltage range (unless otherwise noted) (memory programming and authentication were tested with R1 = 4.7 kΩ, C1 = 0.1 µF over pull-up voltage range)

PARAMETER		TEST CONDITIONS	MIN	TYP	MAX	UNIT
	Power up communication delay	Power capacitor charge time		100		ms
I_{sleep}	Sleep current			8	11	µA
$I_{sdq(Vsdq)}$	V_{sdq} Current	$V_{sdq} \geq V_{sdq(min)}$			50	µA
	OTP Memory programming voltage		6.8	7	7.7	V
	OTP Memory programming time			100		µs/byte
	EEPROM Programming current (peak current)			83		µA
	EEPROM Peak current duration			100		µs
	EEPROM Programming time			50		ms
SDQ						
V_{IL}	Input low-level voltage				0.63	V
I_{OL}	Output low sink current	V_{OL} = 0.4 V			1	mA

STANDARD SERIAL COMMUNICATION (SDQ) TIMING

over recommended operating temperature and supply voltage range (unless otherwise noted) (See Figure 1)

PARAMETER		TEST CONDITIONS	MIN	TYP	MAX	UNIT
t_{RSTL}	Reset time – low		480			µs
t_{RSTH}	Reset time – high		480			µs
t_{PDL}	Presence detect – low		60		240	µs
t_{PDH}	Presence detect – high		15		60	µs
t_{REC}	Recovery time		1			µs

STANDARD SERIAL COMMUNICATION (SDQ) TIMING (continued)

over recommended operating temperature and supply voltage range (unless otherwise noted) (See Figure 1)

PARAMETER		TEST CONDITIONS	MIN	TYP	MAX	UNIT
t_{SLOT}	Host bit window		60		120	µs
t_{LOW1}	Host sends 1		1		13	µs
t_{LOW0}	Host sends 0		60		120	µs
t_{LOWR}	Host read bit start		1		13	µs
t_{SLOT}	bq26100 bit window		60		120	µs
t_{SU}	bq26100 data setup				1	µs
t_{RDV}	bq26100 data valid			exactly 15		µs
$t_{RELEASE}$	bq26100 data release		0	15	45	µs

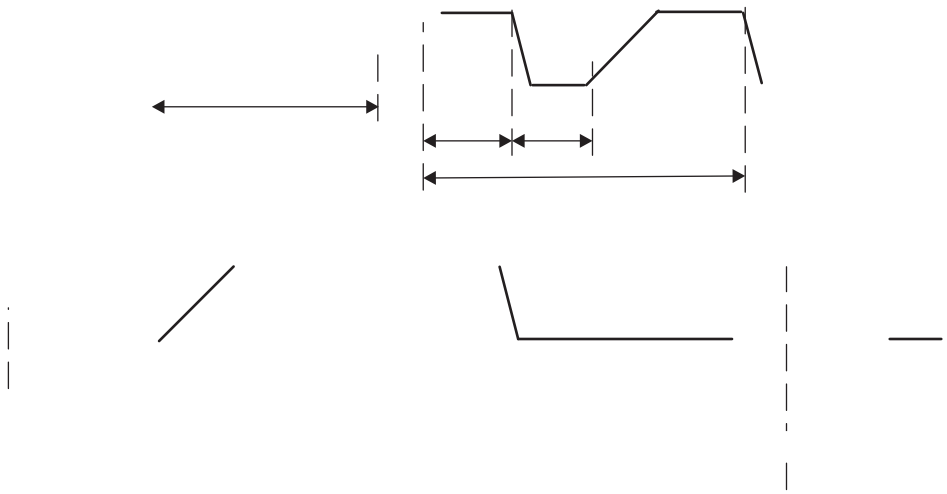


Figure 1. SDQ Timing Diagrams

The SDQ protocol requires a CRC calculation as part of the communication flow. The CRC, based on a polynomial of $x^8+x^5+x^4+1$, is computed to determine data integrity and its use varies in the protocol. The Memory Function flows show what data is shifted through the CRC and when the value is transmitted from the slave. Each data byte used in the CRC calculation is pushed through the CRC shift register from LSB to MSB. The byte wide CRC computation is:

```
for (i = 0; i < 8; i++)
{
    if (crc[0] ^ input[i])
        crc = (crc >> 1) ^ 0x8C;
    else
        crc = crc >> 1;
}
```

Where did the magic number 0x8C come from? CRC polynomials are defined such that the highest order simply shows the number of bits, so $x^8+x^5+x^4+1$ defines an 8-bit value with a binary value of 00110001 (bits 0, 4, and 5 are 1 and all others are 0). Since the SDQ CRC is computed by shifting in the LSB, the polynomial must be used in reverse bit order – binary 10001100 or hexadecimal 0x8C.

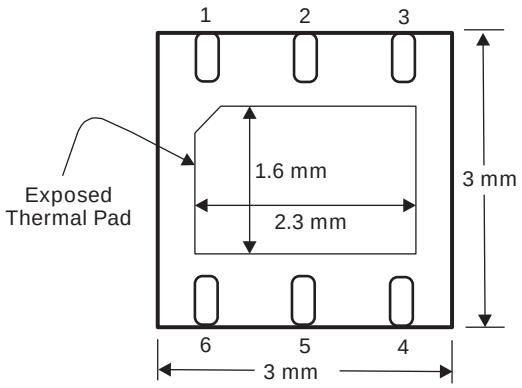
The CRC value is reset to 0 prior to the first byte being shifted through. The CRC is also reset when the CRC is shifted out as part of the SDQ protocol.

PARAMETER		TEST CONDITIONS	MIN	TYP	MAX	UNIT
t_{pon}	Program setup time		2			ms
t_{rise}	Pulse rise time		1		10	ms
t_{prog}	Pulse high time	Single byte programming	300			ms
		Key programming	3			ms
t_{fall}	Pulse fall time		1		10	ms

Figure 5. pdSat00 Communication to OTP Programming Pulse Diagram

Figure 3. OTP Programming Pulse Detail

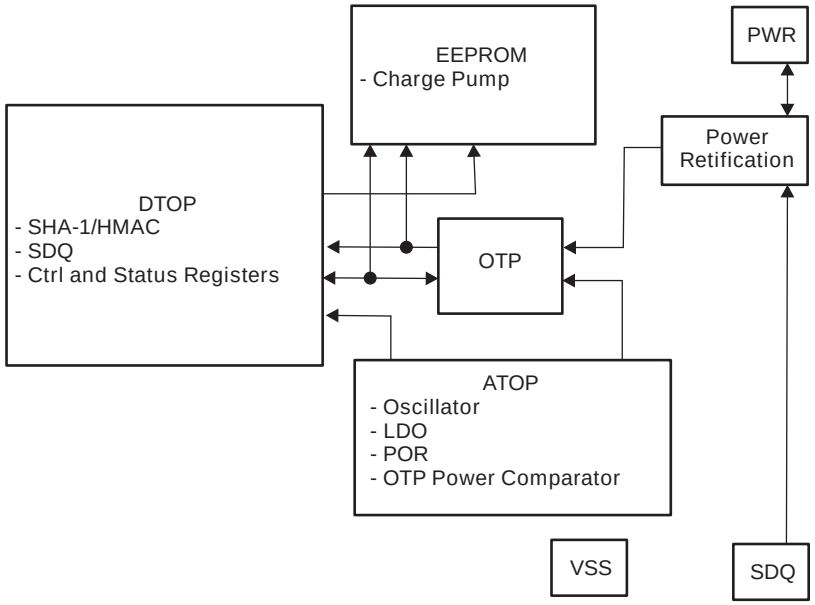
PIN ASSIGNMENT



TERMINAL FUNCTIONS

TERMINAL		I/O	DESCRIPTION
NAME	NO.		
PWR	1	I/O	Power capacitor connection
SDQ	6	I/O	Single wire SDQ interface to host
VSS	2, 3, 4, 5	I	Ground

FUNCTIONAL BLOCK DIAGRAM



FUNCTIONAL DESCRIPTION

The bq26100 provides the same basic functionalityVSSVSSVSS

writes a random 20-byte message to the bq26100 and sets the AUTH bit in the CTRL register. The bq26100 calculates the HMAC digest in less than 500 µs, replacing the random message sent by the host with the HMAC result. To complete the authentication process, the host computes the HMAC function with the same 20-byte random message originally written to the bq26100. The result is compared to the HMAC result computed by the bq26100. If the values match, the pack is authenticated.

The key is separated into two 64-bit spaces, allowing multiple parties to program

Communicating with the bq26100

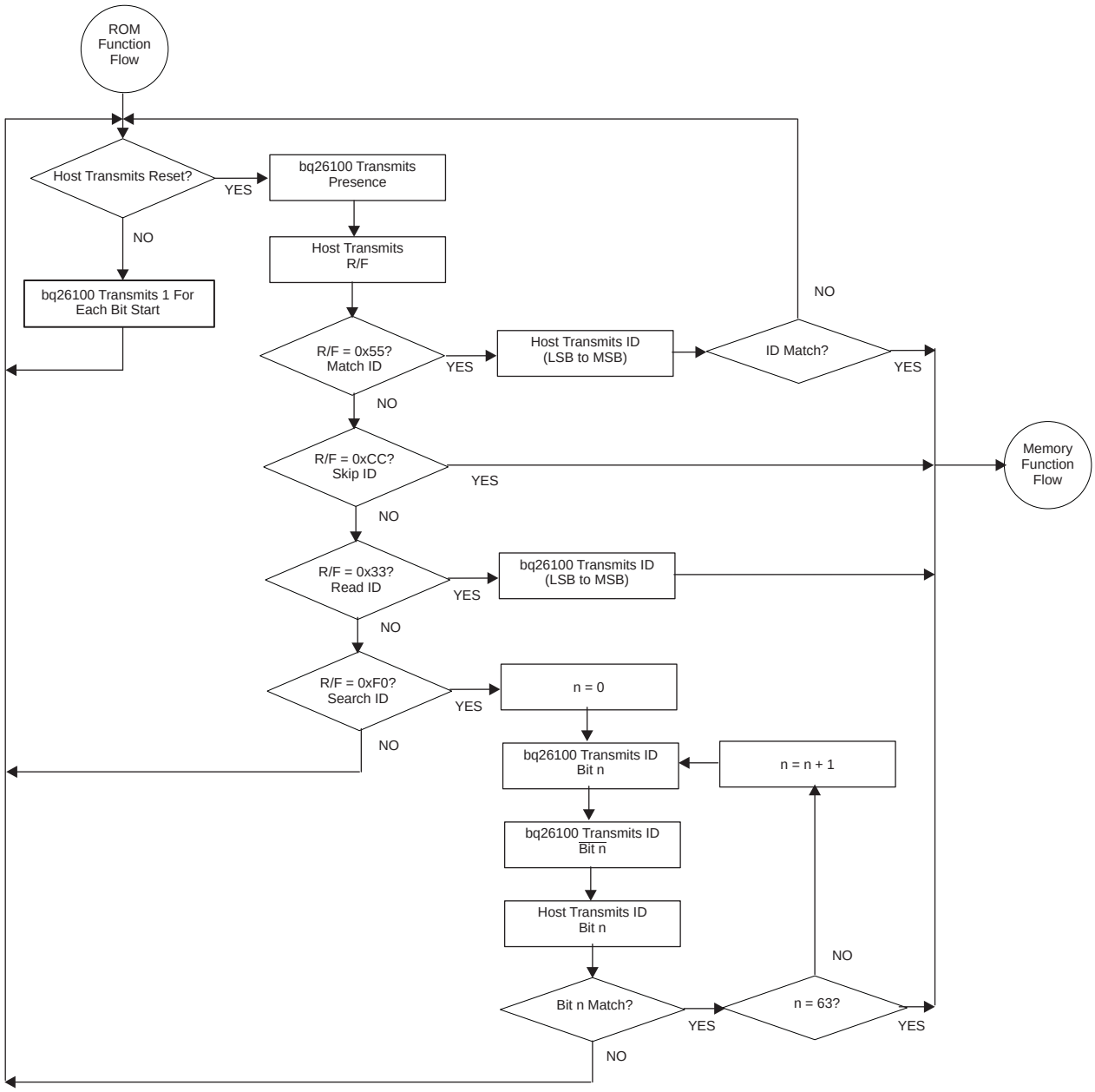


Figure 4. ROM Function Flow Chart

The 64-bit device ID is made up of an 8-bit family code, 48-bit random value, and a final 8-bit CRC.

ID MSB		ID LSB
CRC (8 bits)	Random Data (48 bits)	Family Code (8 bits, defaults to 0x09)

Contact Texas Instruments if specific data should be programmed into the ID.

After the ROM function command is issued and the bq26100 is selected, a Memory Function command can be issued. The Memory Function commands are Read Memory, Read EEPROM, Read Status, Read Page, Read Page 4, Read Digest, Read Control, Write Memory, Write Page 4, Write EEPROM, Write Status, Write Message, Write Control, and Profile.

Figure 5 shows the flow for the Memory Function selection. Figure 6 through Figure 12 illustrate the flow for each memory function.

MEMORY DESCRIPTIONS

The bq26100 has a memory and command structure that is compatible with the bq2022, however additional memory and commands have been added. The bq26100 uses a combination of non-volatile One-Time-Programmable (OTP), non-volatile EEPROM, and volatile registers. The memory is split into the following sections:

Non-Volatile OTP Memory

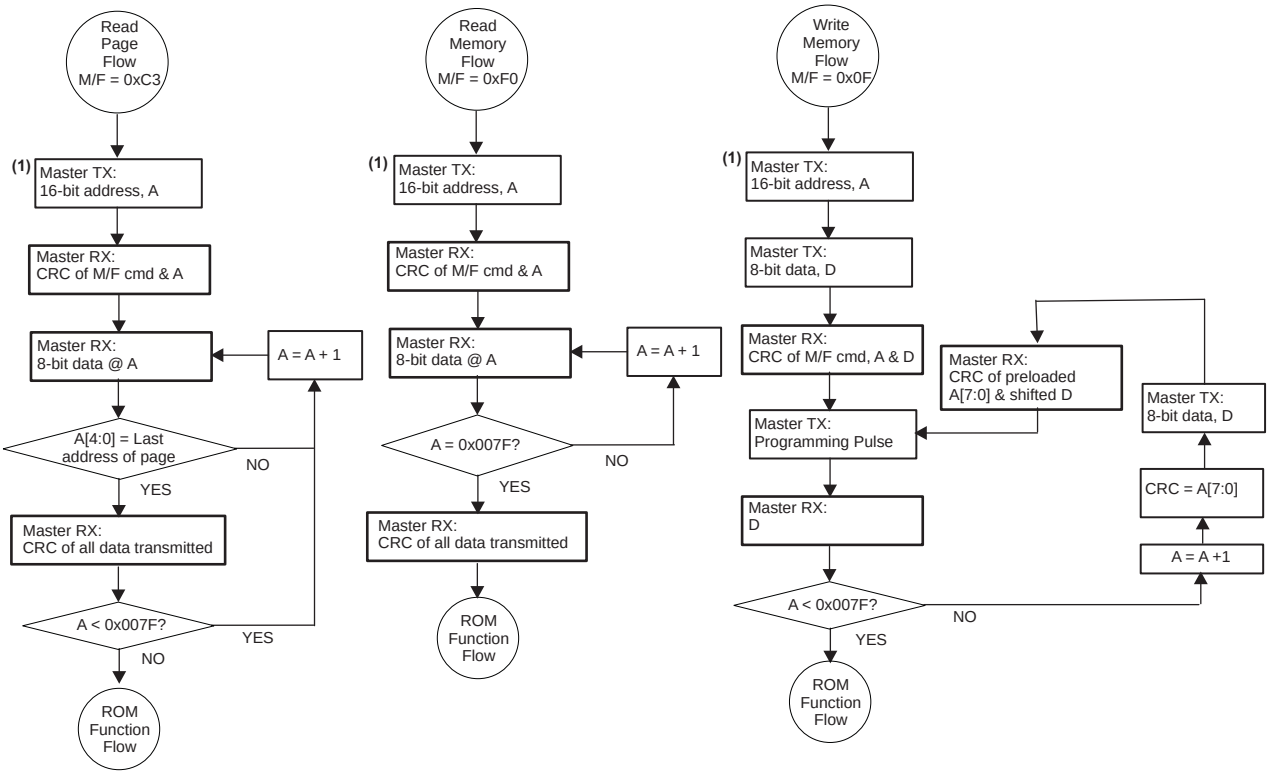
The One Time Programmable (OTP) memory is intended for factory programming. Programming the OTP requires putting a 7-V pulse on the communication pin after writing the data to the intended address.

General Use – Memory Function Commands 0xF0 (Read) and 0x0F (Write)

The general use space is erased to read 0x00. Data written to the general space is ORed with data already present at the address to be written. A bit can only be flipped from **0** to **1**.

Table 1. General Memory Space Addressing

ADDRESSES	FUNCTION
0x007F – 0x0060	Page 3 – 32 bytes general use
0x005F – 0x0040	Page 2 – 32 bytes general use
0x003F – 0x0020	Page 1 – 32 bytes general use
0x001F – 0x0000	Page 0 – 32 bytes general use



(1) 16-Bit address is sent with lower 8-bit address followed by higher 8-bit address with least significant bit first.

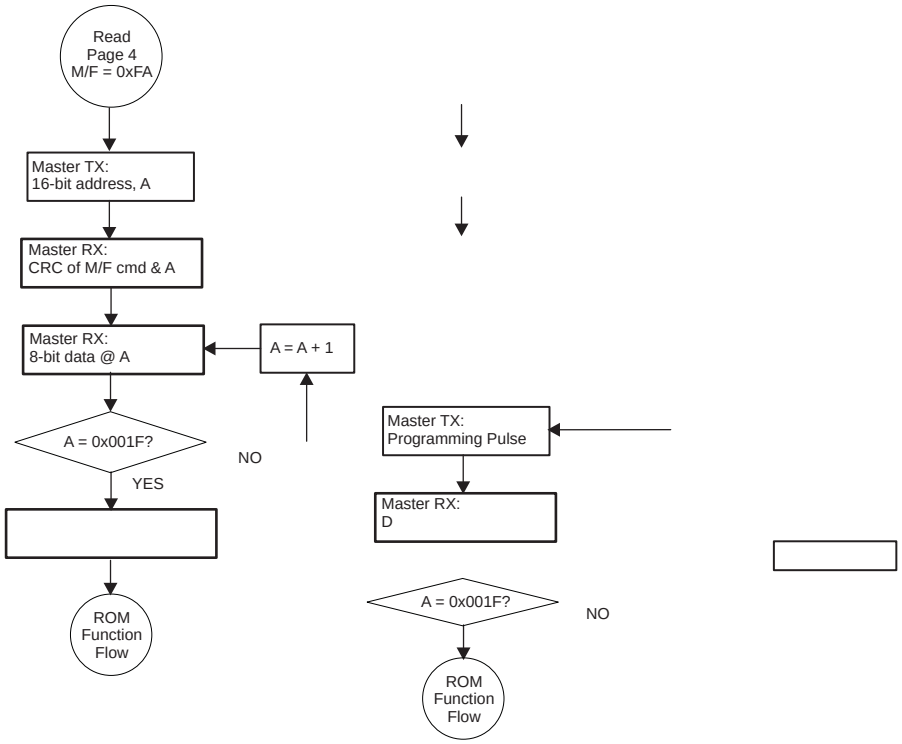
Figure 6. General Memory OTP Write/Read Flows

General Use — Memory Function Commands 0xFA (Read) and 0xAF (Write)

The general use space is erased to read 0x00. Data written to the general space is ORed with data already present at the address to be written. A bit can only be flipped from **0** to **1**.

Table 2. General Memory Space Addressing

ADDRESSES	FUNCTION
0x001F – 0x0000	Page 4 – 32 bytes general use



(1) 16-Bit address is sent with lower 8-bit address followed by higher 8-bit address with least significant bit first.

Figure 7. General Memory OTP Write/Read Flows

Status – Memory Function Commands 0xAA (Read) and 0x55 (Write)

Unlike the general use pages, the status bytes read 0xFF when not programmed and a bit is programmed from **1** to **0**. A zero represents the active state.

Address 0x0007 Reserved

Default value is 0xFF

Address 0x0006 Key Index

The host can determine which one of multiple keys was programmed into the bq26100 by reading the key index value.

Address 0x0005 – 0x0001 Page Redirection

A pointer for alternative page information, these bytes can be used if information in the original page has been invalidated. The host can read these locations and direct reads and/or writes to the page pointed to by the value in the register. For example, if the data in page 2 is corrupted by an incorrectly written data value, and the corrected data is in page 1, the value written to address 0x0003 would be 0xFE (1's complement value of 0x01). Upon reading address 0x0003, the host would receive 0xFE and would take the 1's complement to determine that page 1 contains redirected data.

Table 3. Page Redirection

ADDRESS	PAGE REDIRECTED
0x0005	Page 4
0x0004	Page 3
0x0003	Page 2
0x0002	Page 1
0x0001	Page 0

There is no hardware mapping of the page redirection bytes. The host is responsible for sending the correct address for a redirected page.

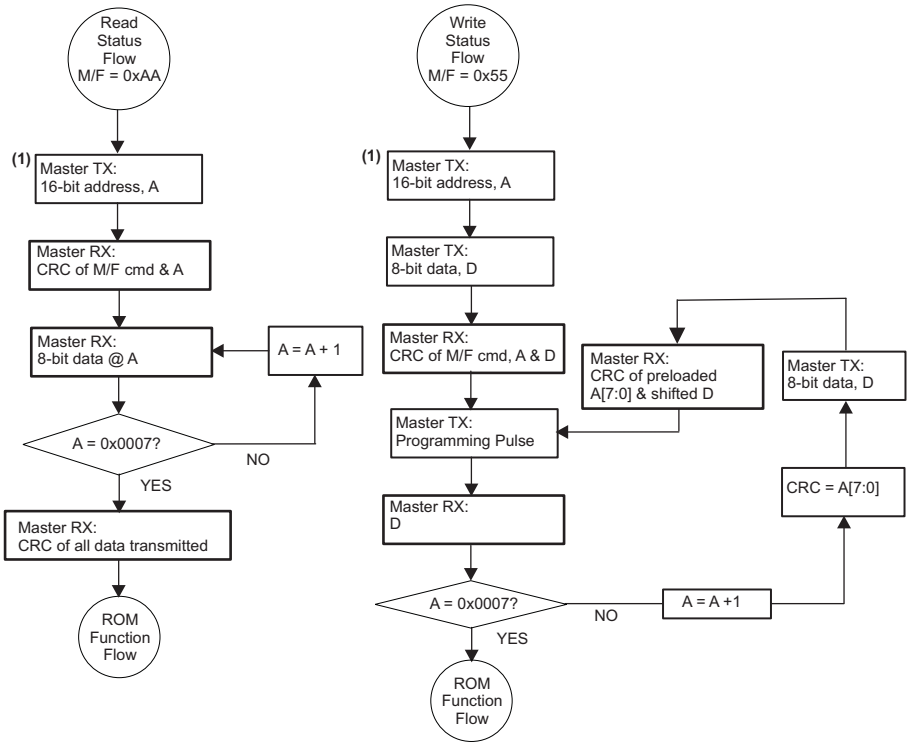
Address 0x0000 PAGE LOCK

	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
FUNCTION	LOCKK1	LOCKK0	RSVD	PAGE 4	PAGE 3	PAGE 2	PAGE 1	PAGE 0

LOCKK1 Programming this bit to **0** locks the upper 64 bits of the device key, preventing additional writes. This bit can only be written once.

LOCKK0 Programming this bit to **0** locks the lower 64 bits of the device key, preventing additional writes. This bit can only be written once.

PAGEx Programming this bit to **0** locks page designated by x, preventing additional writes. This bit can only be programmed once.



(1) 16-Bit address is sent with lower 8-bit address followed by higher 8-bit address with least significant bit first.

Figure 8. Status OTP Write/Read Flows

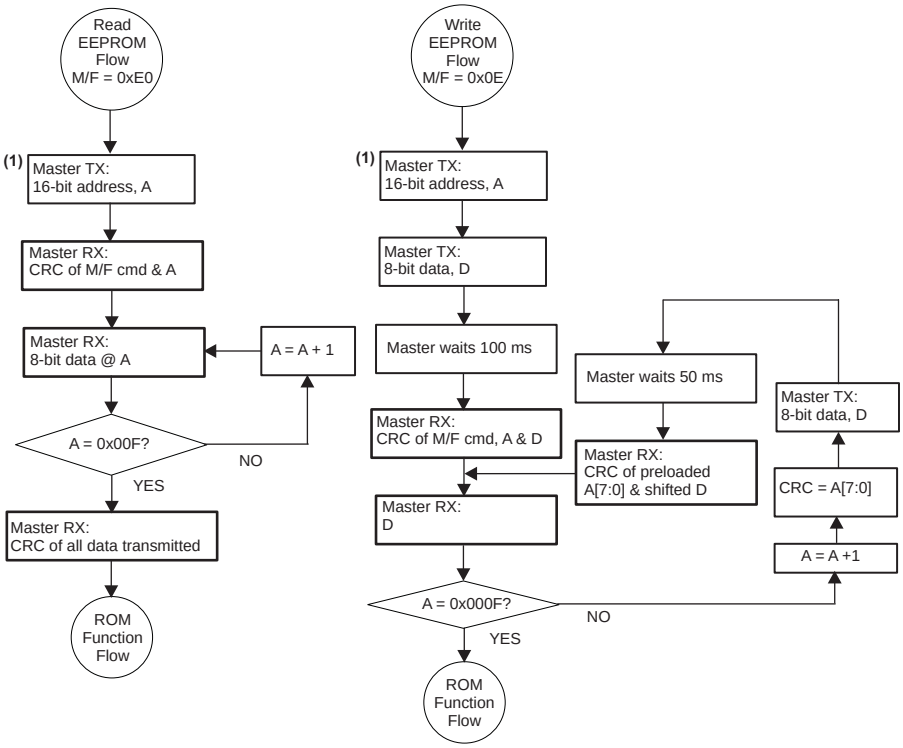
Non-Volatile EEPROM Memory

The EEPROM memory is intended for in-field programming. Programming the EEPROM is no different than writing to RAM or registers, but the timing between the write and read back is different. A bit can be written to **1** or cleared to **0** multiple times and the value is retained when power to the device is removed.

General Use – Memory Function Commands 0xE0 (Read) and 0x0E (Write)

Table 4. General Memory Space Addressing

ADDRESSES	FUNCTION
0x000F – 0x0000	16 Bytes general use



(1) 16-Bit address is sent with lower 8-bit address followed by higher 8-bit address with least significant bit first.

Figure 9. EEPROM Write/Read Flows

Control and Version Registers – Memory Function Command 0x88 (Read) and 0x77 (Write)

The control register starts authentication, clears the message/digest values, and flags when the authentication process has completed. The version register is used to determine the silicon revision.

Table 6. General Memory Space Addressing

ADDRESSES	FUNCTION
0x0001	Silicon Revision Number
0x0000	Control Register

The bits of the Control register are as follows:

	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
NAME	PROGK1	PROGK0	RSVD	CLEAR	RSVD	POR	DONE	AUTH
POR STATUS	0	0	0	0	0	1	0	0

PROGK1 If LOCKK1 is **1** (see Status Register), writing this bit to **1** enables the programming of Device Key 1. Further information about the programming of the keys is found in the SHA-1 section.

PROGK0 If the LOCKK0 bit is **1** (see Status Register), writing this bit to **1** enables the programming of Device Key 0. Further information about the programming of the keys is found in the SHA-1 section.

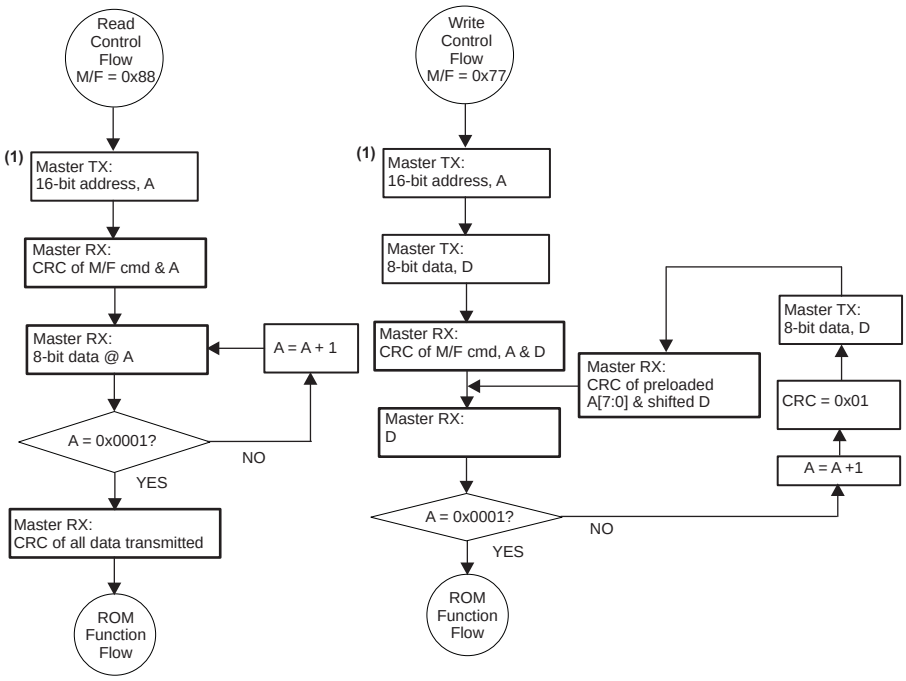
RSVD These bits are reserved for future use. They should always be written to **0**.

CLEAR Writing this bit to **1** clears the message/digest registers. This can be done before the message is written to ensure that all data values are known or after the digest is read to clear the HMAC calculation output. The bq26100 resets the bit back to 0.

POR This bit is set when the device comes out of a POR condition. The bit can be written to **0** to clear the flag. Writing the bit to **1** has no effect on device operation.

DONE This bit is set when the device completes the HMAC calculation. The host should poll for this bit to determine when the digest is available for reading. This bit is automatically cleared when the AUTH bit is written to **1**. This bit is also cleared at POR.

AUTH This bit is set to initiate the HMAC calculation. This bit is automatically cleared when the DONE bit is written to **1**.



(1) 16-Bit address is sent with lower 8-bit address followed by higher 8-bit address with least significant bit first.

Figure 11. Control Register Write/Read Flows

Profile Command

Pack manufacturers can use the profile command to determine how the device should be programmed.

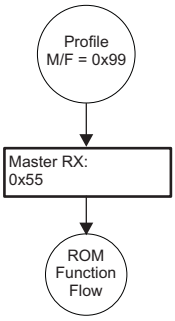


Figure 12. Profile Command Flow

SLEEP MODE DESCRIPTION

The bq26100 enters sleep mode when the SDQ enters a stop state or when SDQ encounters an invalid ID.

SHA-1 DESCRIPTION

The SHA-1 is known as a one-way hash function, meaning there is no known mathematical method of computing the input given only the output. The specification of the SHA-1, as defined by FIPS 180-2, states that the input consists of 512 bit blocks with a total input length less than 2^{64} bits. Inputs which do not conform to integer multiples of 512 bit blocks are padded before any block is input to the hash function. The SHA-1 algorithm outputs 160 bits, commonly referred to as the digest.

The full SHA-1 specification and algorithm can be found at http://csrc.nist.gov/publications/fips under FIPS 180. (As of April 23, 2004 the latest revision is FIPS 180-2).

The bq26100 generates an SHA-1 input block of 288 bits (total input = 160 bit message + 128 bit key). To complete the 512 bit block size requirement of the SHA-1, the bq26100 pads the key and message with a 1, followed by 159 0's, followed by the 64 bit value for 288 (000…00100100000), which conforms to the pad requirements specified by FIPS 180-2:

HMAC DESCRIPTION

The SHA-1 engine is used to calculate a modified HMAC value. Using a public message and a secret key, the HMAC output is considered to be a secure *fingerprint* that authenticates the device used to generate the HMAC.

To compute the HMAC let *H* designate the SHA-1 hash function, *M* designate the message transmitted to the bq26100, and K_D designate the unique 128 bit device key of the bq26100. HMAC(M) is defined as:

$H[K_D \,||\, H(K_D \,||\, M)]$, where || symbolizes an append operation

The message, *M*, is appended to the device key, K_D, and padded to become the input to the SHA-1 hash. The output of this first calculation is then appended to the device key, K_D, padded again, and cycled through the SHA-1 hash a second time. The output is the HMAC digest value.

KEY PROGRAMMING DESCRIPTION

The 128-bit key used in the HMAC calculation is built from two 64-bit key spaces on the bq26100. Each key can be programmed independently, allowing multiple parties to program part of the full 128-bit key without the knowledge necessary to reproduce the full 128-bit key. To further protect the 128-bit key, the value written to each 64-bit non-volatile key space is the output of a SHA-1 calculation on a 160-bit input. Figure 13 provides a flow for the programming of the 128-bit device key. Once KEYx has been programmed, the LOCKKx bit should be programmed to 0 in the status register, preventing another value from overwriting that key space.

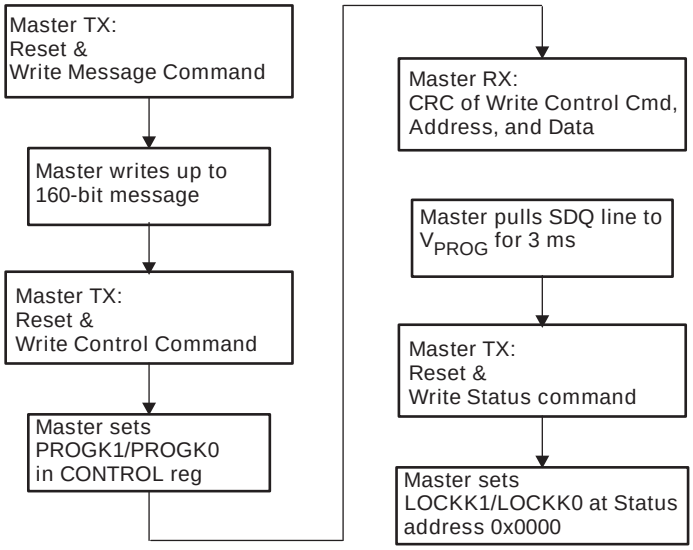


Figure 13. Key Programming Flow

This flow is run twice, for KEY0 and KEY1. An external power source is required on the PWR pin during key programming. Figure 14 shows a typical connection for the external power source.

Since there is no key pre-appended to the message, the key message is padded with a 1, followed by 287 0's, followed by the 64-bit value for 160 (00..01010000):

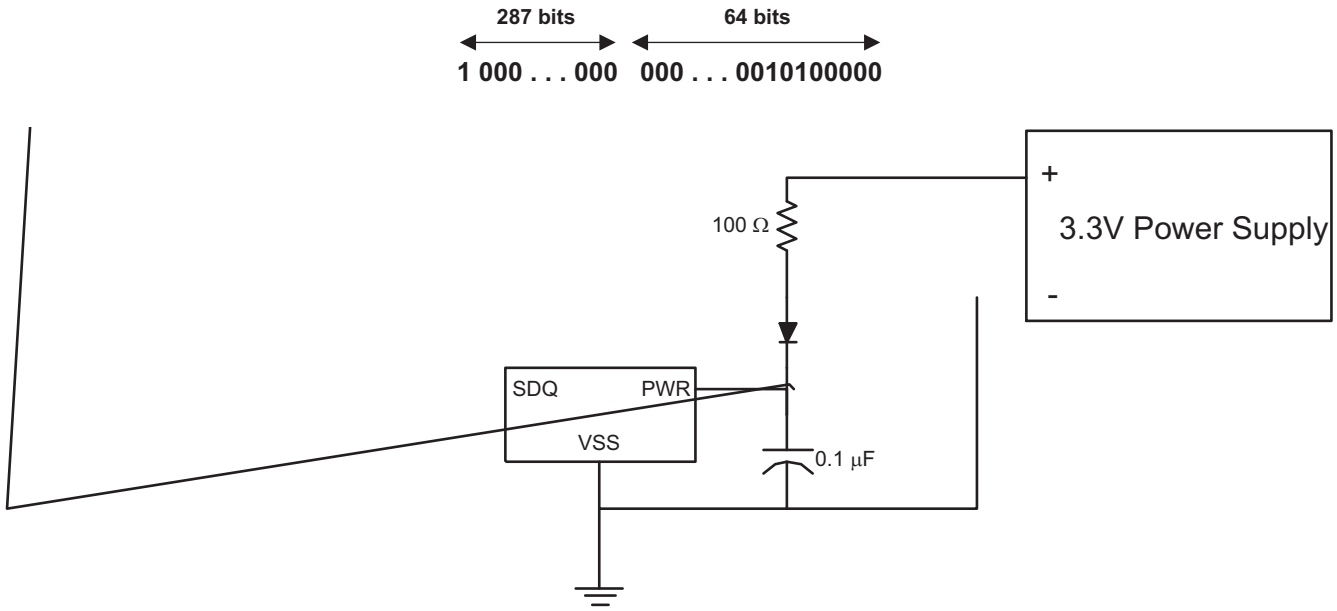


Figure 14. External Power Source Connection

PACKAGING INFORMATION

Orderable Device	Status

DRP (S–PVSON–N6) PLASTIC SMALL OUTLINE NO–LEAD

4205935/E 06/11

NOTES:

= Y14.5M–1994.

D. The package thermal pad must be soldered to the board for th

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2013, Texas Instruments Incorporated