ORIGA™ High Temperature

Original Product Authentication and Brand Protection Solution

Features

- Asymmetric authentication based on Elliptic Curve Cryptographic (ECC)
- Large NVM for storage of device behavior and logistic information
- Quad Flat Non Leaded package(WQFN) – RoHS compliant
- Infineon Single Wire Interface (SWI) for communication between host and accessory

Applications

- Batteries
- Printer Cartridges
- Accessories such as earphones, Speakers, Docking Stations, Game Controller, Chargers
- Medical Equipment and Diagonistic Supplies.
- Authentication of system services, functionalities and networking systems

Description

The Infineon ORIGA™ ORIGinal product Authentication chip helps OEMs and system manufacturers to ensure the authenticity and safety of their original products. It offers a robust cryptographic solution to protect against unauthorized aftermarket replacements and copies. With more than 0.5 Billion ORIGAs deployed at major OEM customers, the ORIGA™ in small WQFN package is particularly suited for applications with very stringent space requirements. The product reduces cost by eliminating the need for additional secure key storage ICs in the host system. ORIGA™ features the market leading strong asymmetric cryptography engine and large user non-volatile memory. The Infineonsingle wire host interface (SWI) allows operation using a single dedicated contact which reduces size and, in turn, improves reliability, robustness, performance, and system cost.

Table of Contents

1 Overview

Infineon Technologies' ORIGA™ SLE95050H is an authentication chip that offers a robust cryptographic solution, designed to assist system manufacturers to ensure the authenticity and safety of their original products, and protection of their investments against after-market replacements.

It leverages Infineon's market leading security knowhow into the battery and accessory authentication markets. With its innovative asymmetric cryptography approach, it significantly reduces system cost whilst making a leap up in security.

1.1 Advantages

Infineon Technologies' ORIGA™ SLE95050H family offers the following advantages:

- Improved security using unique asymmetrical public/private key cryptography with two different keys for encryption and decryption
- Improved total system cost by allowing a host-side software implementation without compromising security and reducing maintenance or support efforts created by wrong accessories
- Improved safety of the system by ensuring system integrity and control
- Large Non-Volatile Memory (NVM) of 576bit (standard customer NVM of 512bit + 64 bits protected NVM) for storage of device behavior or logistic information (e.g. store number of usage cycles, store data for logistic chain traceability)

1.2 Application Domains

The main area of application is authentication leading to increased safety, functionality and reliability of the accessories, replacement parts and disposables.

The Infineon Technologies' ORIGA™ family lends itself for use in multiple application domains which use its safety and highly reliable authentication features. These protect the systems from unauthorized accessories, replacement parts and disposables. Such unauthorized accessories will be easily and immediately detected, allowing the systems decide a suitable next execution step.

Application Domain Examples

- Batteries
  - Computing Devices, Digital Imaging, Mobile Phones
- Printer Cartridges
- Accessories
  - Earphones, Speakers, Docking Stations, Game Controller, Chargers
- Other Peripherals
- Original Replacement Parts
- Medical Equipment & Diagnostic Supplies
- Authentication of system services, functionalities and parts in networked systems

1.3 Personalization and Key Management

Authentication Chips are produced in a standard version. For different customers and different applications these chips have to be individualized / personalized.
This is done by configuring chips with customer specific information (keys, etc).

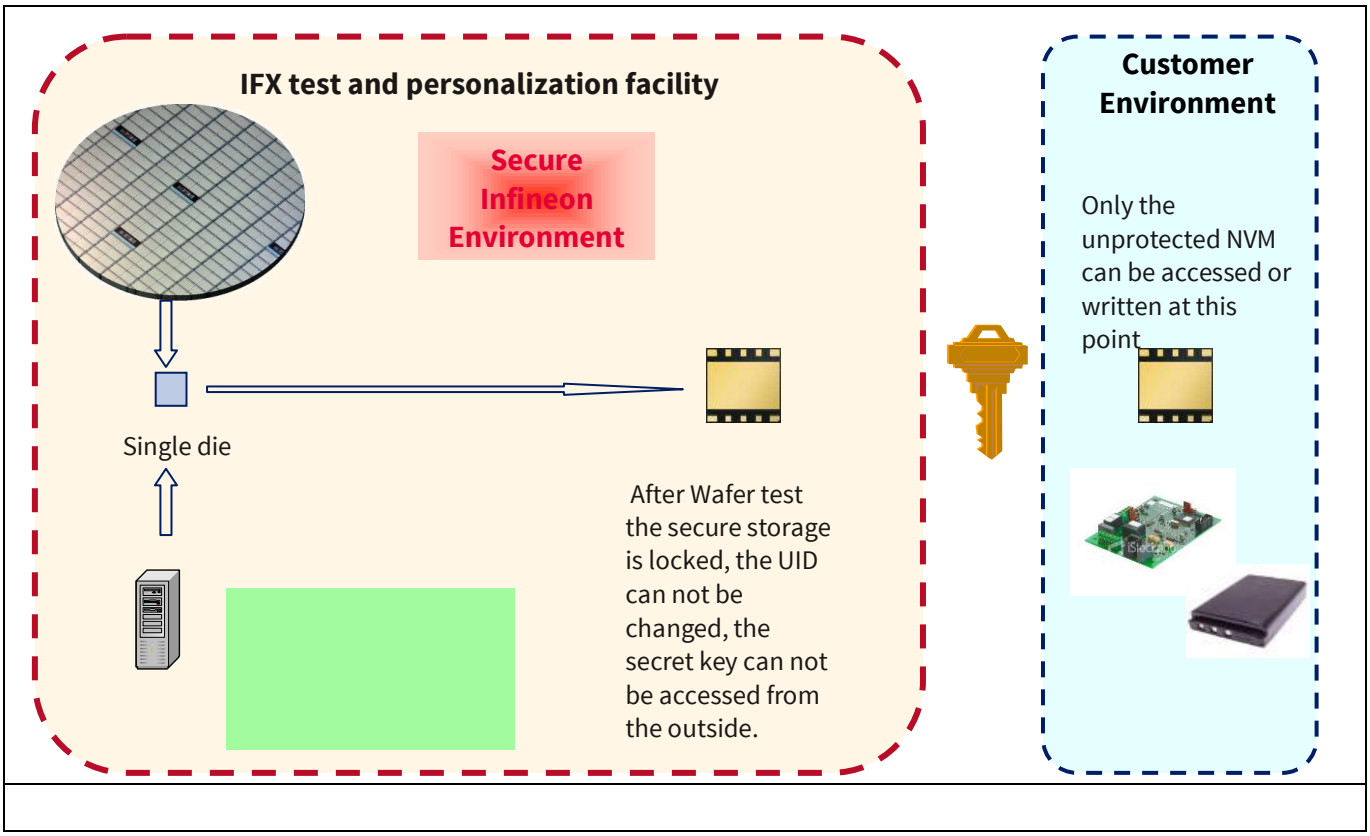

Figure 1 Personalization

Personalization must be performed in a controlled, trusted and protected environment, to prevent any misuse or illegal use of chips. Customer parameters must be protected against unauthorized knowledge or use.

Infineon‘s security chip manufacturing and testing facility is security certified and evaluated by a third party authority, and it meets the requirements for performing the critical personalization flow.

ORIGATM SLE95050H customers (or their approved contracted manufacturers) receive unique sets of key pairs associated with customers’ products.

The secret key should be the same for one accessory product type (e.g. headset) or across a range of products (battery, headset, docking station) to assure interoperability. The corresponding host side public key will be provided to the customer with the host side personalization package.

2 System Configuration

The ORIGA™ devices are a compact design which encompasses the authentication function and analog function in a single solution.

The entire functionality of the SLE95050H ORIGA™ devices is supported via Infineon's proprietary smart Single-Wire Interface protocol which supports three communication modes: Uni-cast, Multi-cast and Broadcast communication. Unicast mode allows commands to be sent, written and read to a single device, while Multicast mode allows commands for multiple devices, and Broadcast for all devices.

The authentication system (Figure 1) consists of a host device serving as the master communicating through the Single Wire Interface (SWI) to the accessory(ies) containing the SLE95050H.

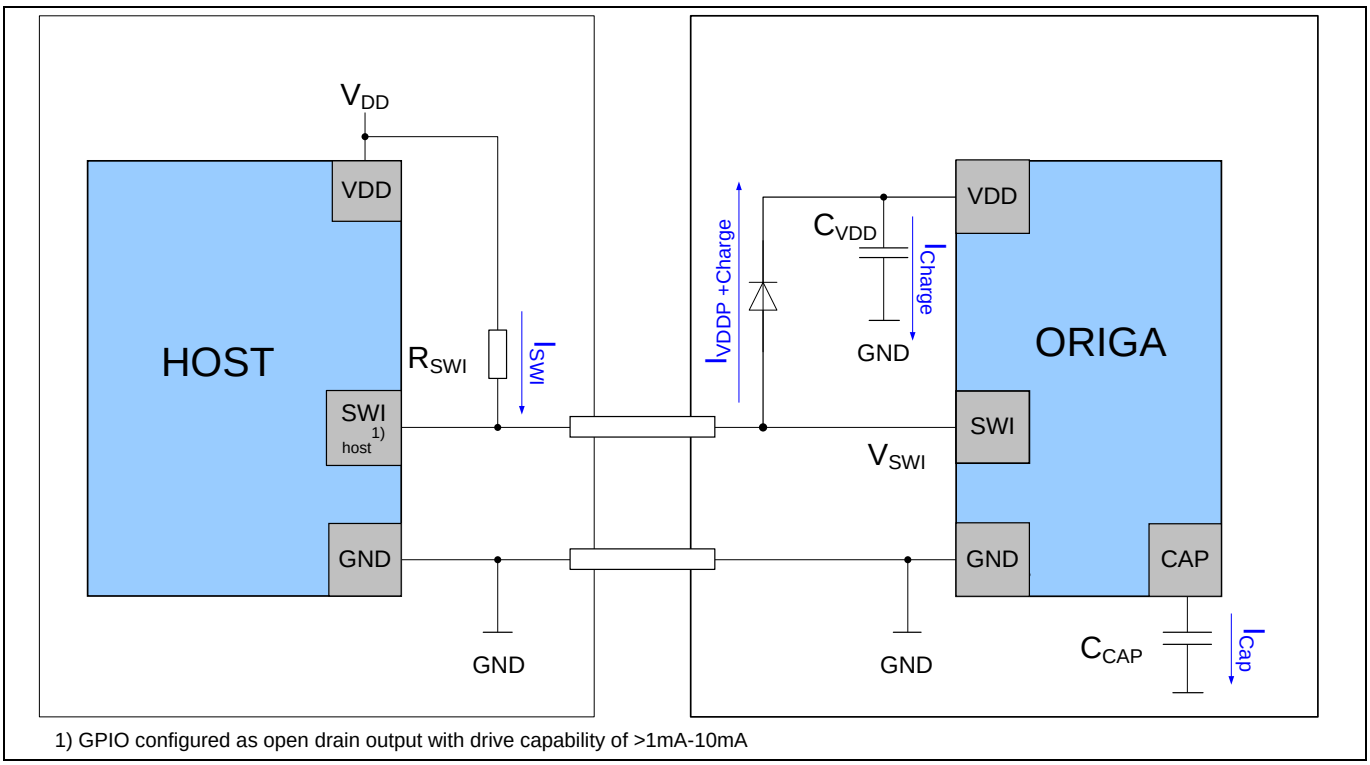

Figure 2 System Building Blocks of SLE95050H – Indirect Powered via Single Wire Interface.

3 System Features

- Strong Asymmetric Cryptography Engine
- Non-volatile Memory
- Infineon Technologies Single Wire Interface (SWI) as I/O interface
- Power Supply – Single Wire Interface powered or Battery powered solution.

3.1 Strong Asymmetric Cryptography Engine

- Elliptic Curve Cryptography (ECC) – based authentication
- Host challenge by software (master – slave)
- Processing time of less than 60ms for authentication on ORIGA
- Processing time of complete challenge/response: Less than 200ms (w/o pre-computing of ECC challenge/response, depending on host microcontroller)
- Software library is available for host integration

3.2 Non-Volatile Memory

- 512-bits unprotected NVM for user mode area
- Up to 192 bits protected NVM read-only space for customer specified information which cannot be modified by the end user
- Counter can be decremented on command by the system host, in conjunction with certain events, such as expired time, dispensed units, charging cycles etc
- The counter value can only be read by the host, it cannot be reprogrammed

3.3 Single-Wire Interface as I/O Interface

- Up to 500kbit/s transmission speed and programmable
- Supports adaptive learning mode
- Powered directly (e.g. from Battery) or indirect via Single-Wire interface (SWI)
- Multiple device capabilities in direct powered mode
- Device ID search scheme and address manage for multiple device capabilities

3.4 Power Supply – Low Power

- Typical usage of 0.8mA$_{rms}$ – 1.3mA$_{rms}$@2V$_{DD}$
- Wide operating conditions: 2.2 to 4.8V at V$_{DDP}$ Pin
- For Single-Wire-Interface powered mode (indirect power) the communication line has to be connected via pull-up to at least 3V (see V$_{DD}$ in figure 2)
- Less than 12uA in power-down/sleep mode.
- Power-up: 10ms for full system power up
- Power-down: after continuous logic 0 for >196µs on SWI

3.5 Others

- ESD –
  - HBM = 2kV
  - CDM = 500V

4 Electrical Characteristics

Table 1 Absolute Max Ratings

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Junction Temperature range	T_j	-20		110	°C	
IO / VDD power supply	V_{DDP}	1.85		6	V	
Digital supply.	V_{DIG}	1.25		1.85	V	
Signal voltage level	V_{SWI}			6	V	

Note: Stresses above the maximum values listed here may cause permanent damage to the device. Exposure to absolute maximum rating conditions for extended periods may affect device reliability. Maximum ratings are absolute ratings; exceeding anyone of these values may cause irreversible damage to the integrated circuit.

4.1 Input/Output Signals

Table 2 I/O and Power Signals

Pin No.	Pin Name/ Pad Inst	Pin Type	Buffer Type	Function
4	VDD	PWR	-	2.2V to 4.8V power supply. I/O / VDDP power supply.
5	SWIO	I/O	OD	Open-drain input and pull-down wired-AND. Supports single-wire interface protoccol.
6	VSS	GND	-	SWIO / VDD ground.
1	CAP	PWR	-	Digital power supply.

4.2 Operating Characteristics

Table 3 Power Supply

Parameter	Symbol	Values			Unit
		Min	Typ	Max	
Digital Supply (internal)	V_{DIG}	1.4	1.55	1.7	V
I/O / VDD Power Supply	V_{DDP}	2.2		4.8	V
Active Supply Current	I_{VDDP}	0.6	1.3	3.5	mA_{rms}
SWI Drain Current[1]	I_{OD}			8	mA_{rms}
Inactive Supply Current[2]	$I_{core(Inactive)}$		1.0	12.0	uA

All Min, Typ and Max values contained in this table are preliminary. Final values are to be confirmed.

1. Prolong drain current exceeding 10mA may damage the device. Tested at VOL = 0.4V
2. Host powers down SLE95050H

Table 4 Thermal Characteristics

Parameter	Symbol	Values			Unit
		Min	Typ	Max	
Ambient Temperature	T_A	-20	25	110	°C

Table 5 I/O Characteristics

Parameter	Symbol	Values			Unit	Conditions/Remarks
		Min	Typ	Max		
Input High Voltage	V_{IH}	2.2		4.8	V	LVTTL
Input Low Voltage	V_{IL}			0.8	V	LVTTL
Input High Current	I_{IH}			10	uA	
Input Low Current	I_{IL}			1	uA	
Output Low Current	I_{OL}			8	mA	

All Min, Typ and Max values contained in this table are preliminary. Final values are to be confirmed.

Output High Voltage and Current depend on external pull-up circuitry

4.3 Device Configuration and Electrical Schematics

The SLE95050H ORIGA™ supports multiple configuration options:

1. Host Software to single SLE95050H.
2. Host Software to multiple SLE95050H.

Once initialized the host system may trigger a search ID sequence to identify ORIGA™ devices. After identification of such devices, the host can execute a challenge, verify the response and then determine the success of the authentication.

The following figures illustrate the SLE95050H powering options.

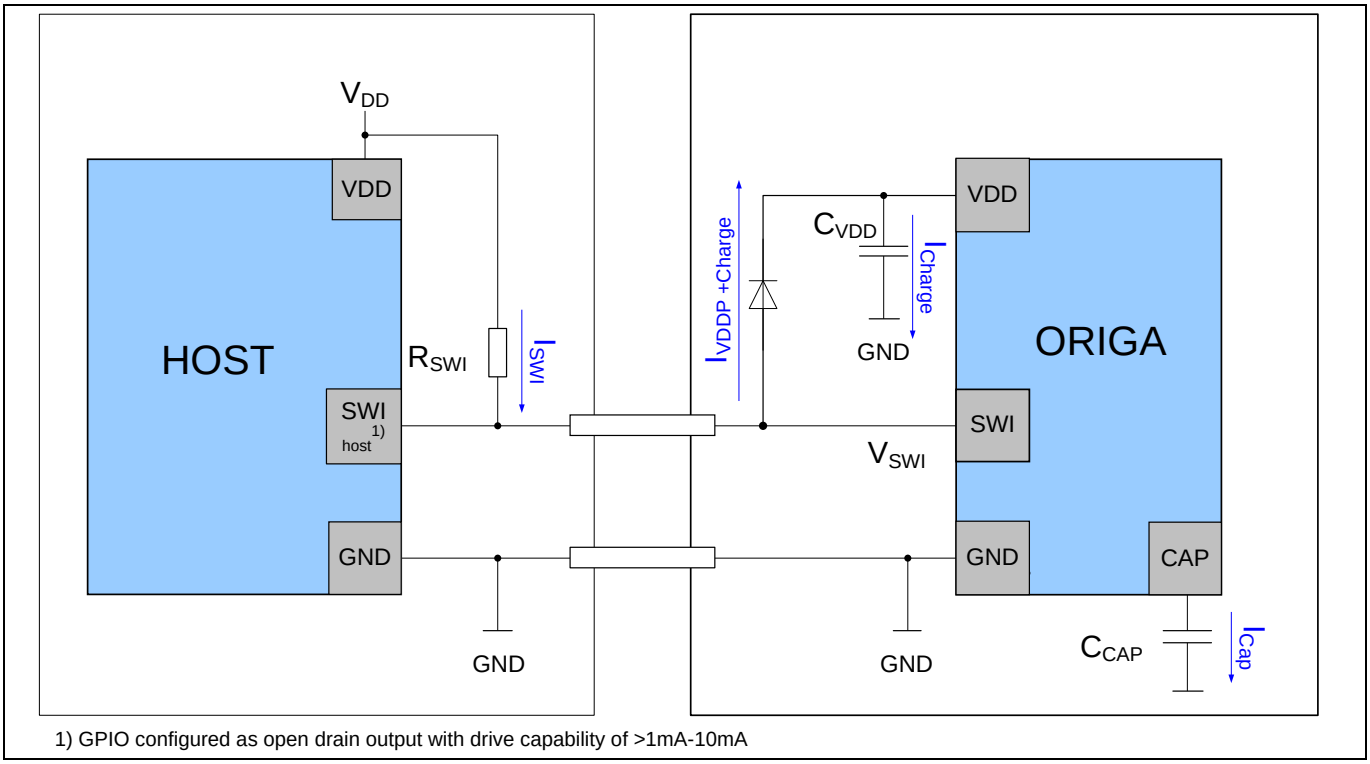

Figure 3 Single Wire Interface Powered using one GPIO

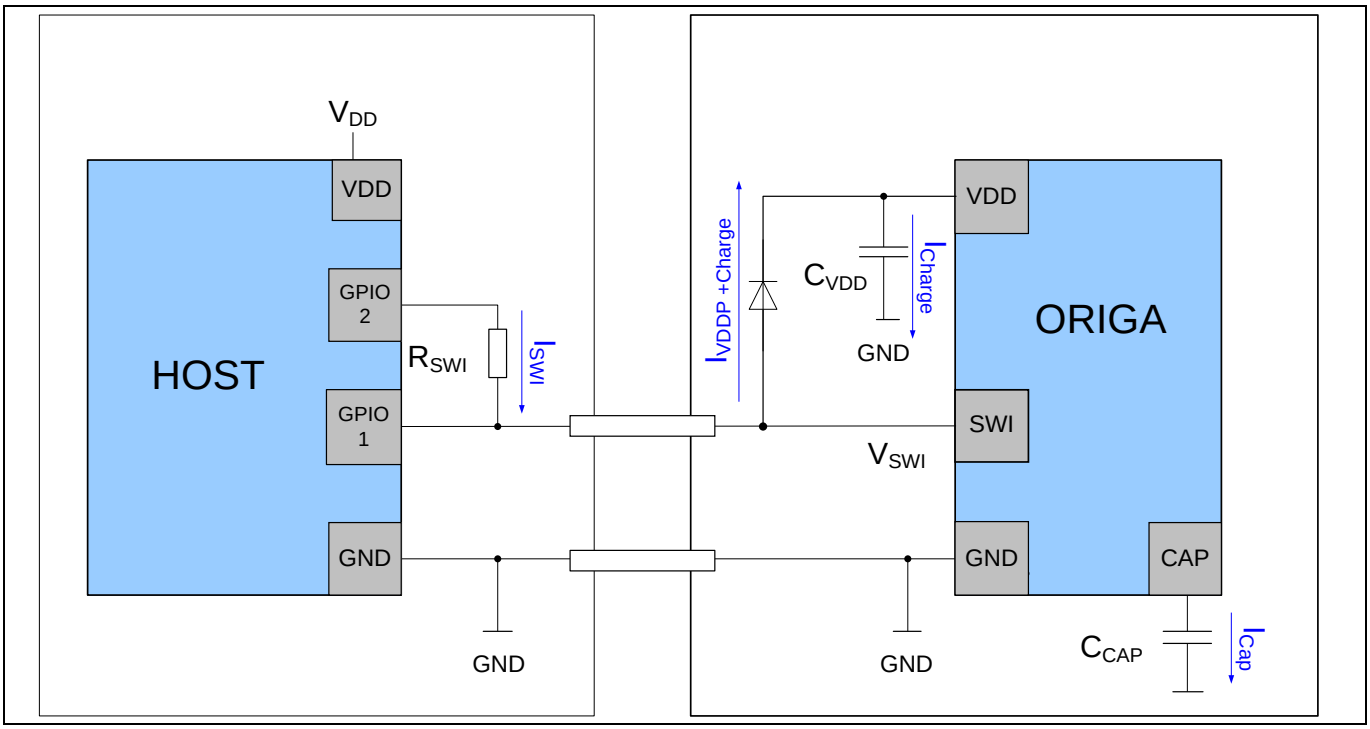

Figure 4 Single Wire Interface Powered using two GPIOs

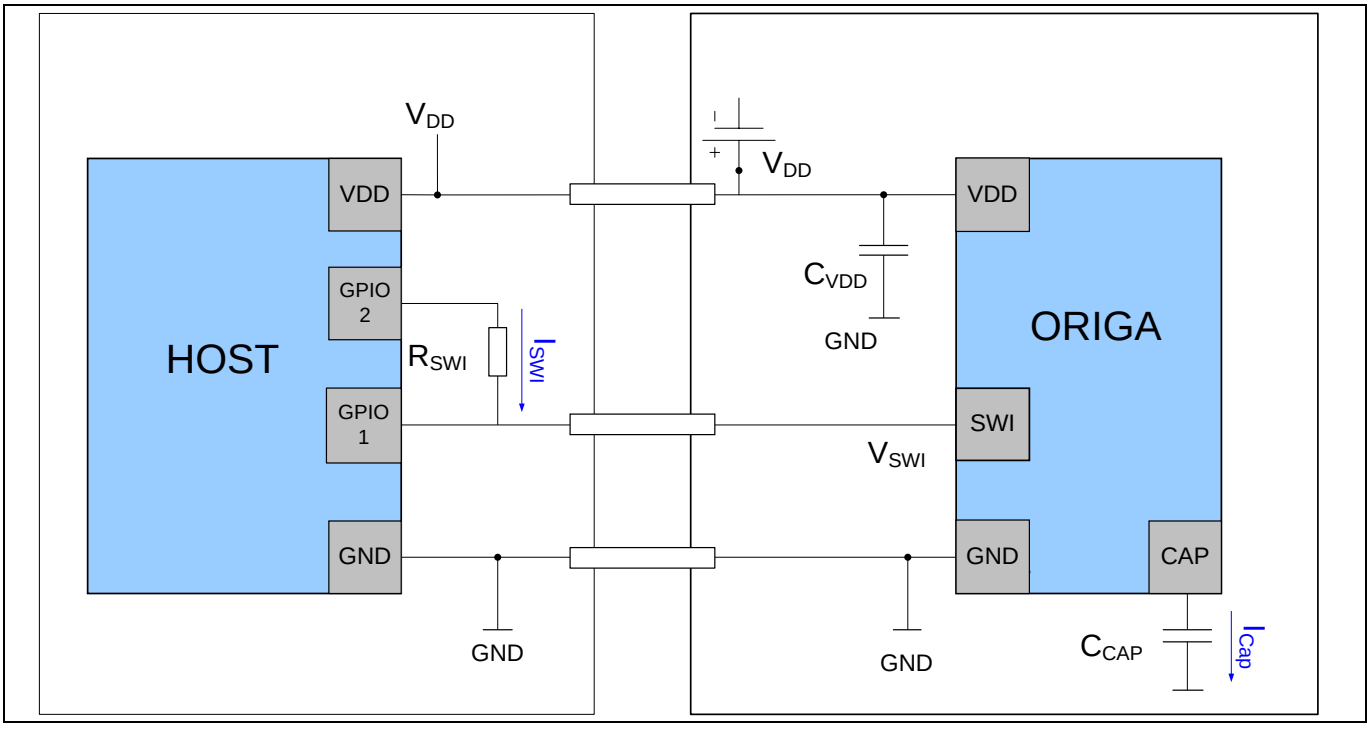

Figure 5 Direct Powered using two GPIOs

5 Single-Wire Interface

5.1 Single-Wire Transaction

Each SWI packet consists of 11 bits (3 command, 8 data bits). When logic 1 on the SWI is seen for a time longer than the power-up time of 10ms, the chip is powered-up and reset.

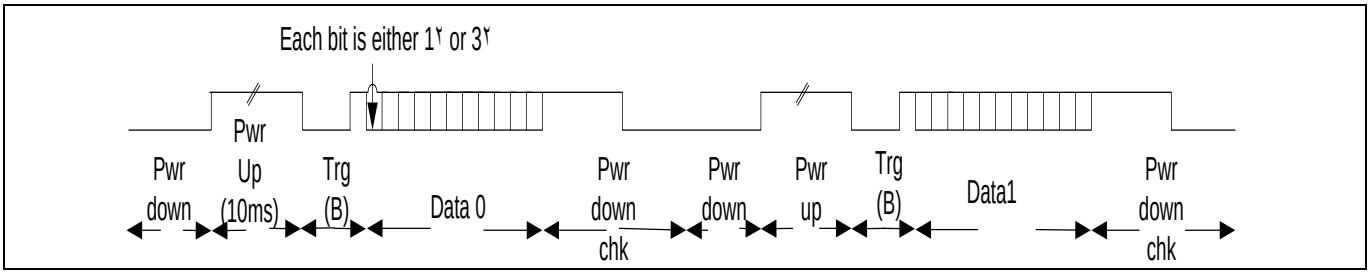

Figure 6 A typical single transaction of the SWI protocol.

In power-up mode, the host can send instructions based on the SWI protocol. When the communication is done, the host can decide to maintain the SWI line at logic 1 or to set it to logic 0 for a time longer than the power-down time of 500µs to power-down the chip to save power.

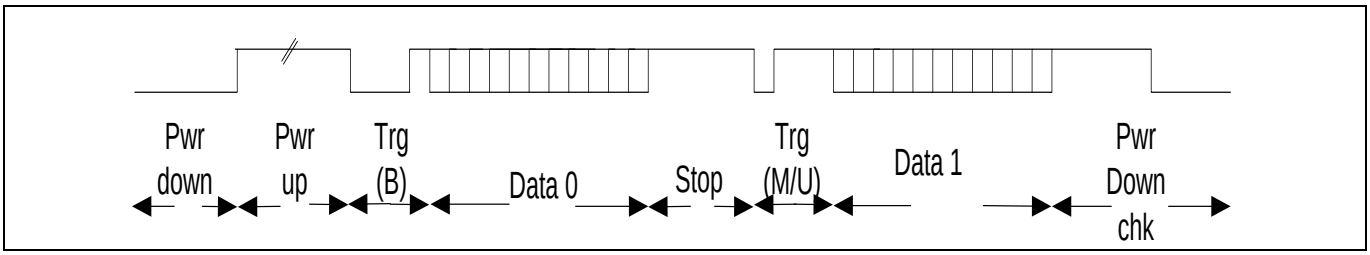

Figure 7 Power-Uo Single Packet Transaction.

In power-down mode, the power sequence and timing is required again before the host can start communication with the chip.

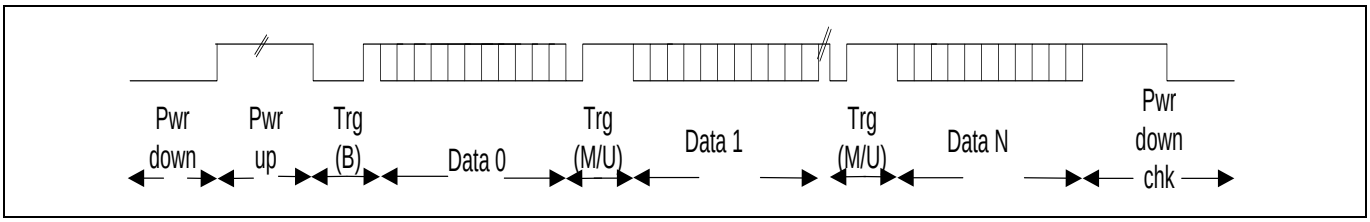

Figure 8 Back-to-Back Data Packet Transaction.

Interrupt can be enabled by the host controller. The host controller must first send an interrupt enable control on the SWI to enable the interrupt on the device(s). Once the device is allowed to interrupt, the host holds the line at logic 1 and if any interrupt- enabled device needs an interrupt, it will pull the line low for a period no greater than the designated interrupt period of 1٢. Once the host detects the logic 0, it interprets that there is an interrupt and will initiate a check on the devices for the interrupt flag.

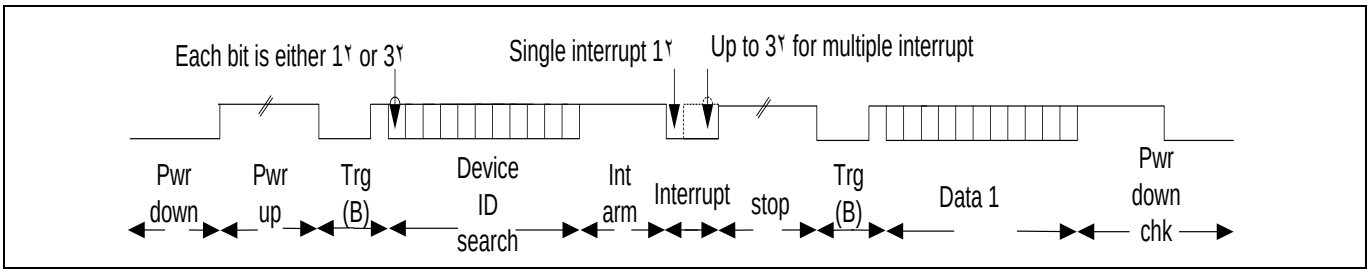

Figure 9 Device-ID Search Data Packet Transaction

6 Packaging

The SLE95050H comes in a WQFN-6 type package.

6.1 Pin Configuration

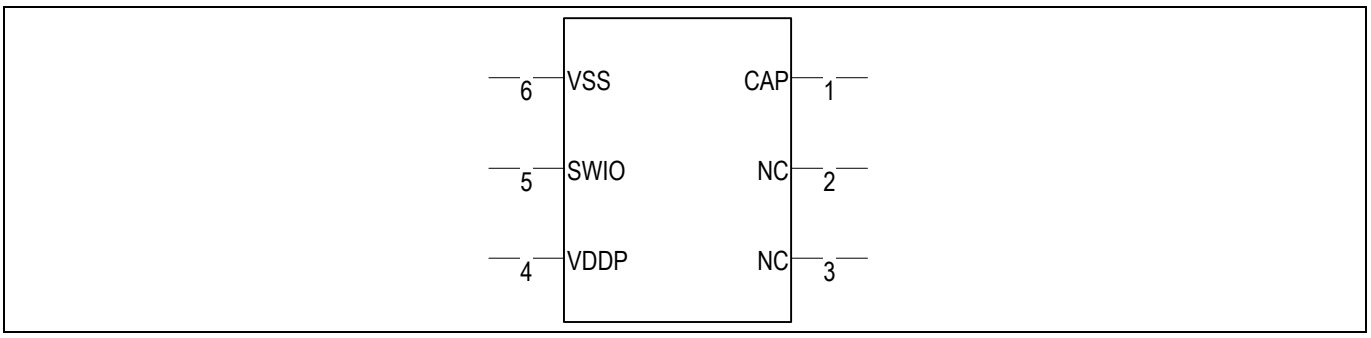

Figure 10 Pin Configuration (WQFN-6 package)

6.2 Pin Out

Table 6 Pin Assignment and description. Non mentioned pins are not connected.

Pin No.	Pin Name/ Pad Inst	Pin Type	Pad Description	Domain
4	VDDP	Supply	2.2V - 4.8V power supply	VDDP
5	SWIO	I/O	Bi-dir pad with input and open-drain pull output driver	VDDP
6	VSS	GND	Digital ground	VDDP
1	CAP	O	1.5V supply pad	VDD

6.3 Package Dimensions of WQFN-6

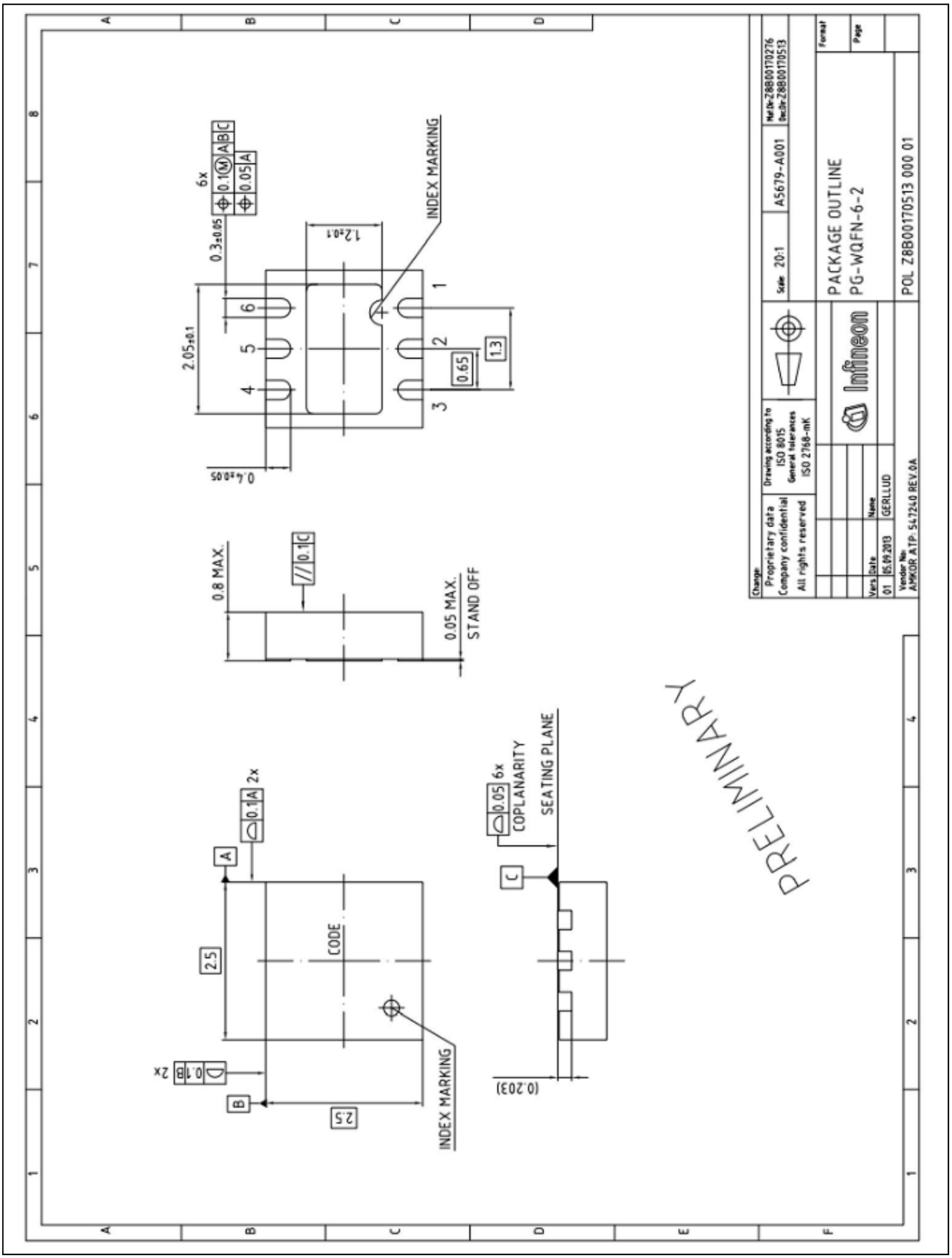

Figure 11 WQFN-6

6.4 Tape & Reel, Marking and Soldering Info

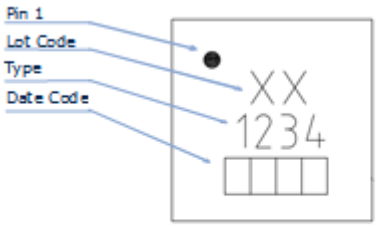

Figure 12 Tape & Reel: 13” with 4” hub, 4x4mm; 6.000 units/reel, reels/box: 1;

7 Evaluation Kit

The ORIGA™ EvalKit USB Stick allows a complete evaluation of all the features of ORIGA™ family. Each Evaluation kit contains dual ORIGA™ SLE95050 and SLE95200. Do note that these are not High Temperature parts and please contact Infineon for High Temperature part evaluation. After installing the demo software from the CD, user will be able to communicate with the on-board ORIGA™ devices.

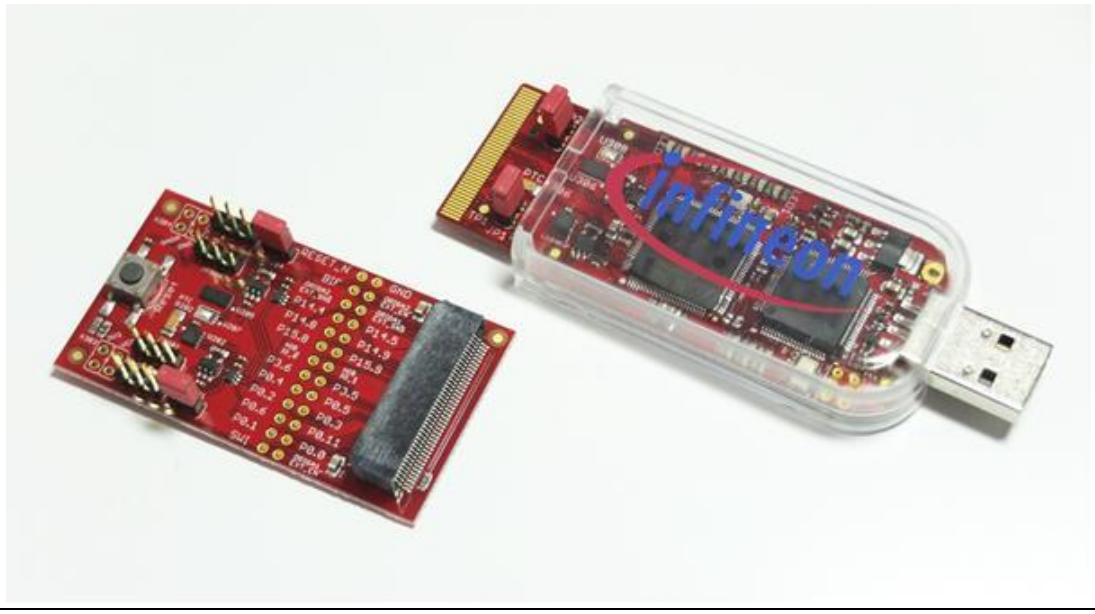

Figure 13 USB Evaluation kit

Revision History

Major changes since the last revision

Page or Reference	Description of change
	ORIGA™ SLE95050H Release.

Edition 2015-10-10

Published by

Infineon Technologies AG

81726 München, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

SLE95050H Product Brief

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”) .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.