Release, Version 1.01, Feb 2013

ORIGA™ SLE95051

Original Product Authentication and Brand Protection Solution

Short Product Information

www.infineon.com/ORIGA

Power Management & Multimarket

SLE95051
All characteristics described in this document might change without further notice.

Rev 1.00	First release
Rev 1.01	Update electrical characteristics based on the latest datasheet (v1.05)

Published by Infineon Technologies AG
Am Campeon 1-12
85579 Neubiberg, Germany

Attention please!

The information herein is given to describe certain components and shall not be considered as a guarantee of characteristics.

Terms of delivery and rights to technical change reserved.

We hereby disclaim any and all warranties, including but not limited to warranties of non-infringement, regarding circuits, descriptions and charts stated herein.

Infineon Technologies is an approved CECC manufacturer.

Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office in Germany or our Infineon Technologies Representatives worldwide (see address list).

Warnings

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

Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

1 Overview 4
1.1 Advantages 4
1.2 Application Domains 4

2 System Configuration 5

3 System Features 7
3.1 Strong Asymmetric Cryptography Engine 7
3.2 Non-Volatile Memory 7
3.3 Single-Wire Interface as I/O Interface 7
3.4 Clock 7
3.5 Decrease-only counter / Lifespan indicator 7
3.6 Others 8

4 Electrical Characteristics 9
4.1 Absolute Maximum Ratings 9
4.2 Input/Output Signals 9
4.3 Operating Characteristics 10
4.4 Device Configuration and Electrical Schematics 11

5 Single-Wire Interface 13
5.1 Single-Wire Transaction 13

6 Packaging 15
6.1 Pin Configuration 15
6.2 Pin Out 15
6.3 Package Dimensions of WLP-5 16

7 Authentication Implementation & Cryptographic Details 17

8 Personalization and Key Management 19

9 Summary 20

1 Overview

Infineon Technologies' ORIGA™ SLE95051 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™ SLE95051 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:

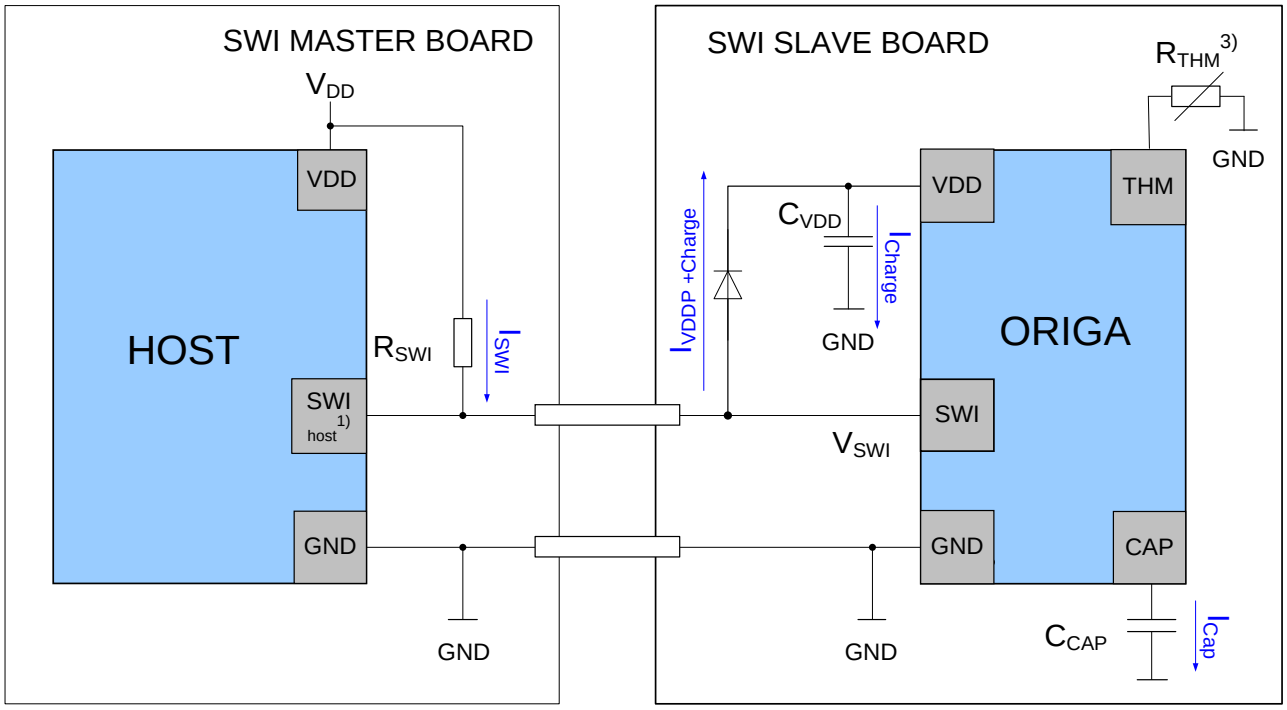
- Batteries
  - Computing Devices, Digital Imaging, Mobile Phones
- Printer Cartridges
- Accessories
  - Earphones, Speakers, Docking Stations, Game Controller, Chargers
- Other Peripherals
- Original Replacement Parts
- Medical Equipment & Diagnostic Supplies
- Authentication of system services, functionalities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

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 SLE95051 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 SLE95051.



1) GPIO configured as open drain output with drive capability of >1mA – 10mA
3) Thermistor only needed for external temperatur measurement, if not needed THM stays n.c.

Figure 1 System Building Blocks of SLE95051 – Indirect Powered via Single-Wire-Interface.

3 System Features

Main Features:

- Strong Asymmetric Cryptography Engine
- Non-volatile Memory
- Infineon Technologies Single Wire Interface (SWI) as I/O interface
- Power Management – Low Power Consumption
- 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)
- Library Concept for easy host side integration available

3.2 Non-Volatile Memory

- 512-bits unprotected NVM for user mode area
- 64-bits NVM read-only space for customer specified information which cannot be modified by the end user. Programming of this information shall be done before chip packaging.

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
- Unique Chip ID of 96bits (16bit vendor, 16bit product, 64bit unique chip ID)
- Communication library concept for easy to use integration on host side available

3.4 Clock

- Digital system operating frequency of 4 MHz ±10%

3.5 Decrease-only counter / Lifespan indicator

- 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

3.6 Others

- ESD –
  - HBM = 2kV
  - CDM = 500V
- EEPROM updating (erase and program) time @ 4ms per page (64 bits)
- EEPROM endurance 10^5 write/erase cycles @ 25°C
- Data retention for minimum of 10 years @ 25°C
- Lifetime: 5 years / 100% duty cycle = 438000h

4 Electrical Characteristics

4.1 Absolute Maximum Ratings

Table 1 Absolute Max Ratings

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
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.

4.2 Input/Output Signals

Table 2 I/O & Power Signals.

Pin No.	Pin Name/ Pad Inst	Pin Type	Buffer Type	Function
4	VDD	PWR	-	2V to 5.5V power supply. I/O / V_{DDP} 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.

4.3 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}	2.0		5.5	V
Active Supply Current	I_{VDDP}	0.6	1.3	2.5	mA_{rms}
SWI Drain Current[1]	I_{OD}			10	mA_{rms}
Inactive Supply Current[2]	$I_{core(Inactive)}$		1.0	5.0	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 V_{OL} = 0.4V
2. Host powers down SLE95051

Table 4 Thermal Characteristics.

Parameter	Symbol	Values			Unit
		Min	Typ	Max	
Ambient Temperature	T_A	-20	25	85	°C

Table 5 I/O Characteristics.

Parameter	Symbol	Values			Unit	Conditions/ Remarks
		Min	Typ	Max		
Input High Voltage	V_{IH}	2		5.5	V	LVTTL
Input Low Voltage	V_{IL}			0.8	V	LVTTL
Input High Current	I_{IH}			6	uA	
Input Low Current	I_{IL}			1	uA	
Output Low Current	I_{OL}			10	mA	

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

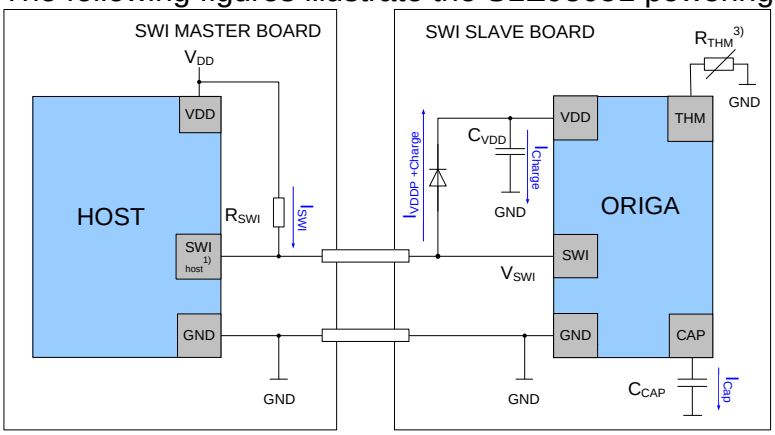
Output High Voltage and Current depend on external pull-up circuitry

4.4 Device Configuration and Electrical Schematics

The SLE95051 ORIGA™ supports multiple configuration options:
1) Host Software to single SLE95051.
2) Host Software to multiple SLE95051.

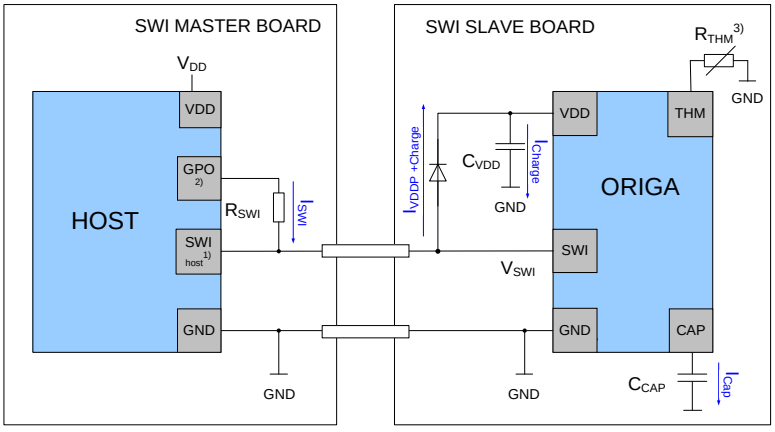
Once initialized the host system may trigger a search ID sequence to identify ORIGA™ devices. After identification of such devices, the host can execute a challenge, verify the response and then determine the success of the authentication.

The following figures illustrate the SLE95051 powering options.



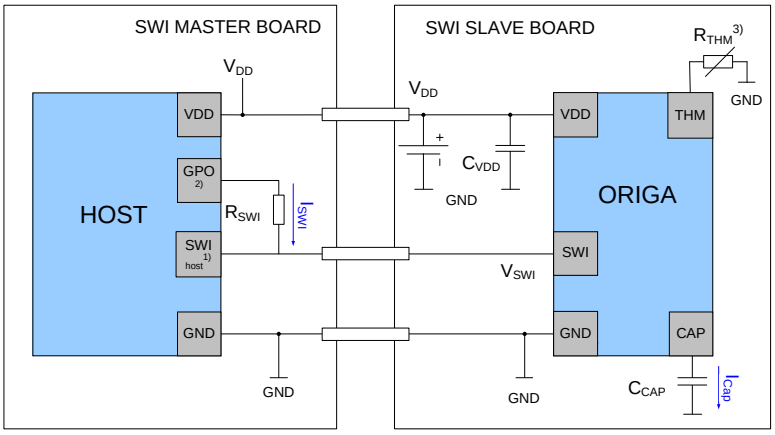
1) GPIO configured as open drain output with drive capability of >1mA – 10mA
3) Thermistor only needed for external temperatur measurement, if not needed THM stays n.c.

Figure 2 Single Wire Interface (SWI) Powered (Indirect Power) using one GPIO



1) GPIO configured as open drain output with drive capability of >1mA – 10mA
2) General purpose Output with drive capability of >1mA – 10mA, needed for low power mode
3) Thermistor only needed for external temperatur measurement, if not needed THM stays n.c.

Figure 3 Single Wire Interface (SWI) Powered (Indirect Power) using two GPIOs



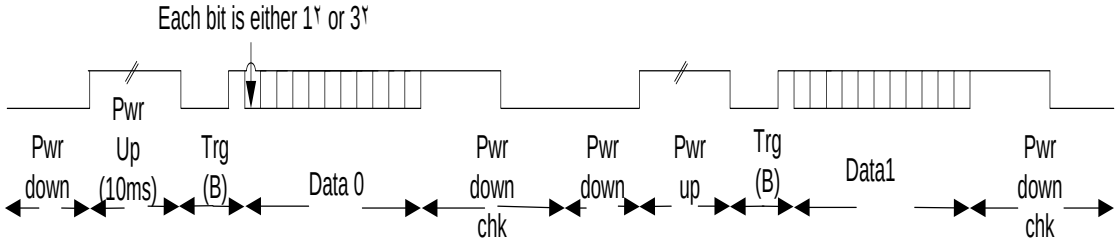
1) GPIO configured as open drain output with drive capability of 1mA – 10mA
2) General purpose Output with drive capability of 1mA – 10mA, needed for low power mode
3) Thermistor only needed for external temperatur measurement, if not needed THM stays n.c.

Figure 4 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.



τ (tau) = 0.5 *(1/Data baud rate). The baud rate of SWI is represented by toggling of state of logic “1” voltage level and logic “0” voltage level per second transferred.

Figure 5 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.

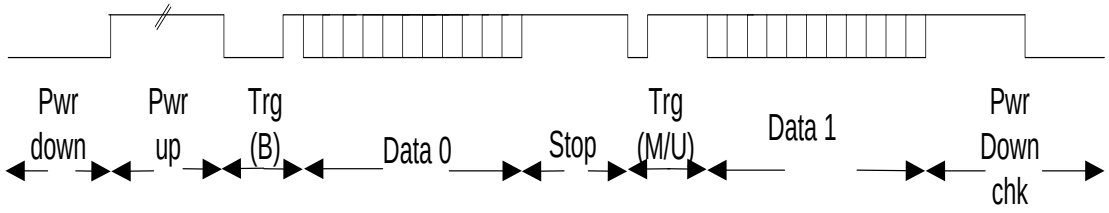


Figure 6 Power-Up Single Packet Transaction.

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

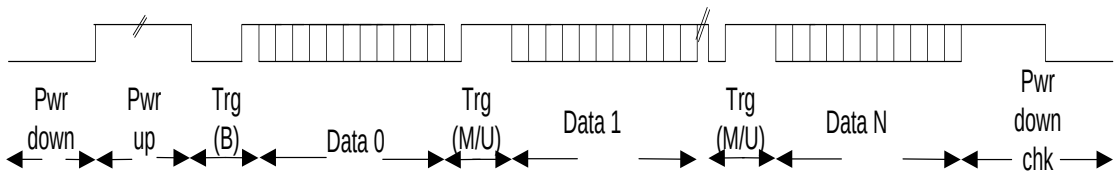


Figure 7 Back-to-Back Data Packet Transaction.

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.

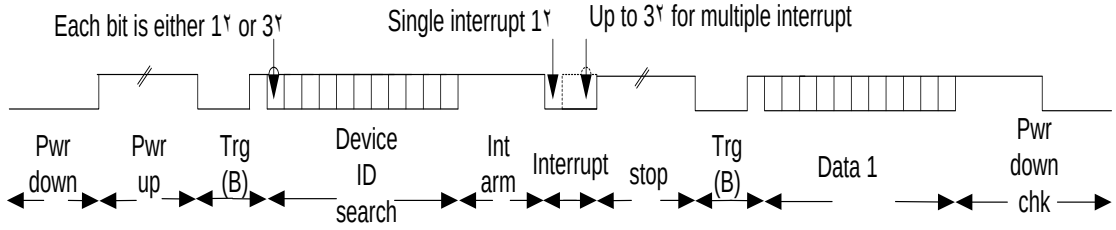


Figure 8 Device-ID Search Data Packet Transaction.

6 Packaging

The SLE95051 comes in a WLP-5 type package.

6.1 Pin Configuration

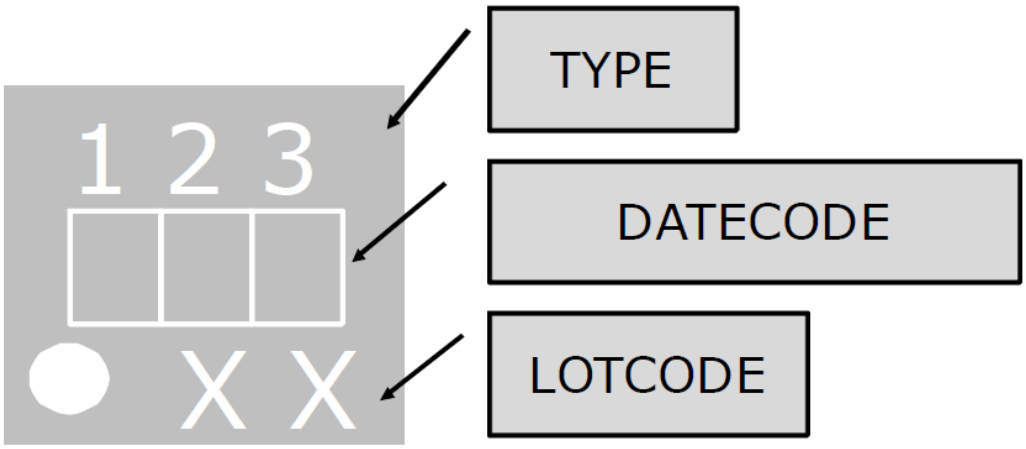


Figure 9 Pin Configuration (WLP-5 package)

6.2 Pin Out

Pin No.	Pin Name/ Pad Inst	Pin Type	Pad Description	Domain
A1	CAP	O	1.5V supply pad	VCAP
A2	VSS	GND	Digital ground	VDD
B2	SWI	IO	Bi-dir pad with input and open-drain pull output driver	VDD
C1	NC		NC	
C2	VDD	Supply	Power supply	VDD

Table 5 Pin Assignment and Pin Description. Non mentioned pins are not connected.

6.3 Package Dimensions of WLP-5

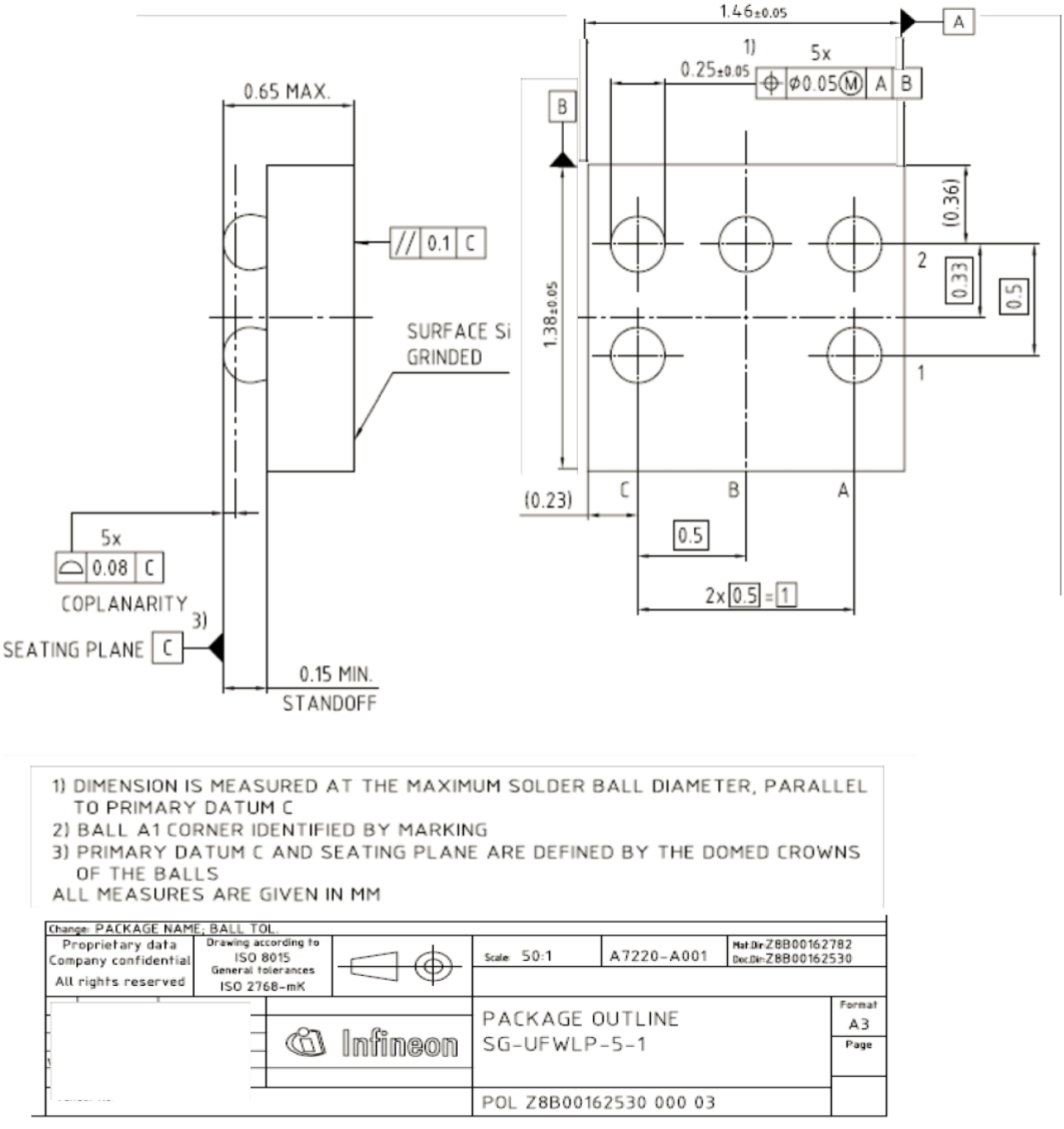


Figure 10 WLP-5 (bottom view)

7 Authentication Implementation & Cryptographic Details

The Infineon ORIGA™ SLE95051 is a novel asymmetric key authentication device offering superior cryptography and functionality at reduced system cost compared to other solutions.

It is based on Infineon's long standing experience and market leadership in security solutions. It offers a cost effective level of physical hardware security, e.g. versus bus probing and memory analysis attacks and shares the same highly secure front-end facilities, logistics & personalization processes as high security application devices, such as banking and PayTV smart cards.

Due to its unique asymmetric cryptography implementation the Infineon authentication chip can be used in a software-to-hardware authentication configuration - No hardware master device on the host side is needed in this configuration.

In this lowest system cost configuration (software-to-hardware authentication), the implementation on the host side can be done with a small piece of code library (about 3kB of code, needing less than 2kB of RAM for execution on preferably 16bit or 32bit, but also possible with 8bit microcontrollers). The host-side implementation runs on the host processor in Software without compromising the security of the system, unlike in a symmetrical cryptography system (e.g. SHA/DES/TDES/AES).

The reference code can be licensed by Infineon for use in conjunction with the ORIGA™ device.

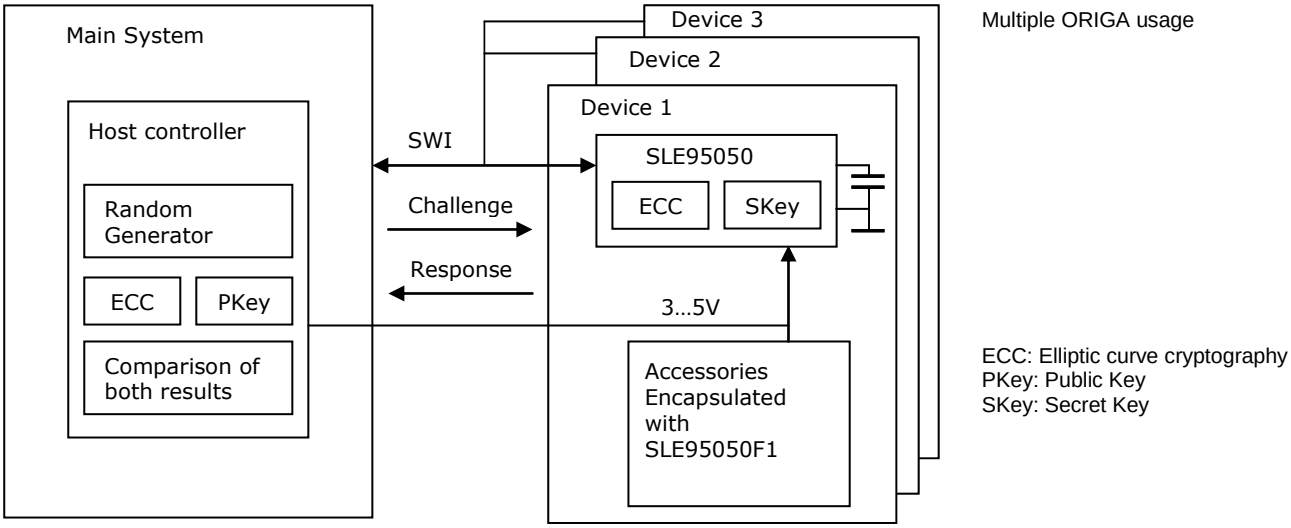


Figure 11 Software-to-Hardware Authentication Implementation

Symmetric vs. Asymmetric Cryptography

In symmetric cryptography the same key is used for encryption and decryption. If one key is hacked, the entire security protection is broken. Software stored keys can be comparably easy to read out. Typically, symmetric algorithms are used in situations where a secure surrounding environment can be established, like in banking and data transmission.

Asymmetric cryptography uses two different keys for encryption and decryption. One key, the so called public key (PKey), can be made public (and therefore used in the Software implementation), as long as the other key, the secret key (SKey, sometimes also called private key), is still in the safe hardware environment of the chip. Asymmetric cryptography is typically used in applications requiring a high level of security in a critical environment like military or government implementations and it is used for identity protection in electronic passports worldwide.

Leveraging the advantages of asymmetric cryptography, Infineon has implemented the most modern and suitable for embedded applications asymmetric cryptography algorithm. The ORIGA™ device from Infineon uses discrete elliptic curve cryptography (ECC) logarithm implementation, a mathematically very complex and highly secure form of ECC. It combines top level operational security with cost efficient implementation. It protects data such as the Private Key, the unique chip ID and other customer information in a protected memory space, which is secured from modification. Also up to 192bit of read only data can be written into this space.

Additionally, the Infineon ORIGA™ SLE95051 devices offer unprotected and freely usable NVM of 512 bit for different purposes such as traceability of manufacturing and logistics

chain, personalization data for the accessory or other end-user behavior like charging cycle documentation.

8 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).

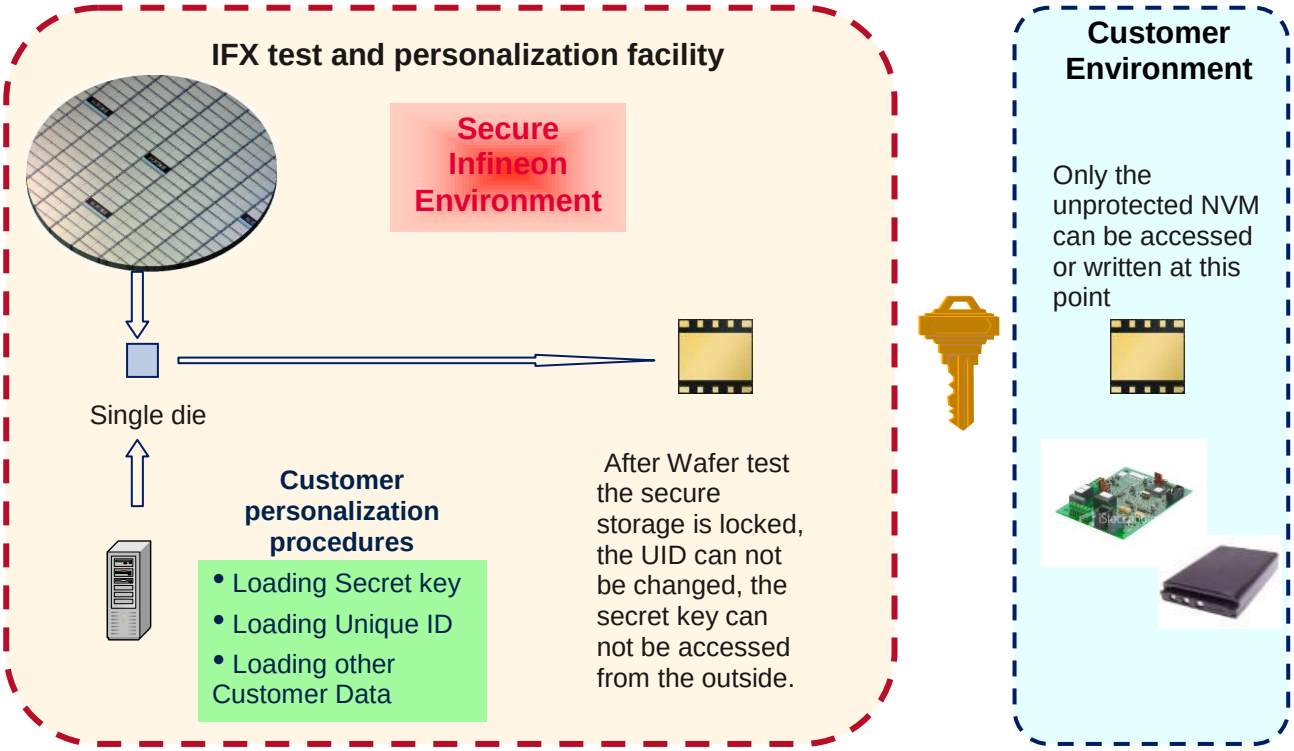


Figure 12 Personalization

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.

ORIGA™ SLE95051 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.

9 Summary

Infineon Technologies ORIGA™ Original Product Authentication and Brand Protection Solution provides superior security at improved system cost compared to other solutions by using unique asymmetrical cryptography with two different keys for encryption and decryption.

With this novel approach it can protect your products and brand, while improving the safety of the overall system.

Its non-volatile memory (NVM) of 512bit can be used for storage of device behavior (e.g. number of usage cycles or data for logistic chain traceability).

The Single Wire Interface is easy to implement without design changes to peripherals or the target accessory interface. The device supports host powered mode via SWI as well as battery powered mode.