ORIGA™ 2 High Temperature

Original Product Authentication and Brand Protection Solution

Features

- Asymmetric authentication based on Elliptic Curve Cryptographic (ECC)
- ORIGA™ Digital Certificate (ODC) with device personalization
- Large NVM for storage of device behavior and logistic information
- High accuracy temperature sensor
- Small Outline Non-leaded package – RoHS compliant
- MIPI BIF (Battery Interface) standardized single-wire interface for communication between mobile device and battery

Applications

- Battery authentication for mobile phones, computing devices, digital imaging, power tools, drones etc.
- Power supply units and (fast) AC adaptors
- Power cables

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™ 2 in small USON 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™ 2 features the market leading strong asymmetric cryptography engine and 3.5 kbits of user non-volatile lockable memory and a temperature sensor. The incorporated power management unit reduces power consumption and has over-under voltage protection up to ±20 V. The MIPI BIF compliant single wire host interface 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' novel ORIGA™ ORIGinal product Authentication chip assists OEMs and system manufacturers to ensure the authenticity and safety of their ORIGinal products. It offers a robust cryptographic solution designed to protect against unauthorized aftermarket replacements and clones.

In it's second generation ORIGA™ 2 incarnation, it is especially suited for the Authentication of batteries, but can be used for the authentication of any other accessory, consumable or original spare part as well as long as three contacts can be attached to the chip to power it and communicate with it.

1.1 General Description

ORIGA™ 2 is an integrated Battery Authentication IC. It features a built-in strong asymmetric cryptography engine and 3.5 kbits of user non-volatile memory with a well defined data map covering all functions. The device has a built-in power management unit to reduce power consumption and is tolerant to over-voltages. Furthermore, it also contains an integrated junction temperature sensor which can be set to interrupt the external host controller through the MIPI Battery (digital) Interface. Figure 1 shows the ORIGA™ 2 device Battery Authentication IC function overview.

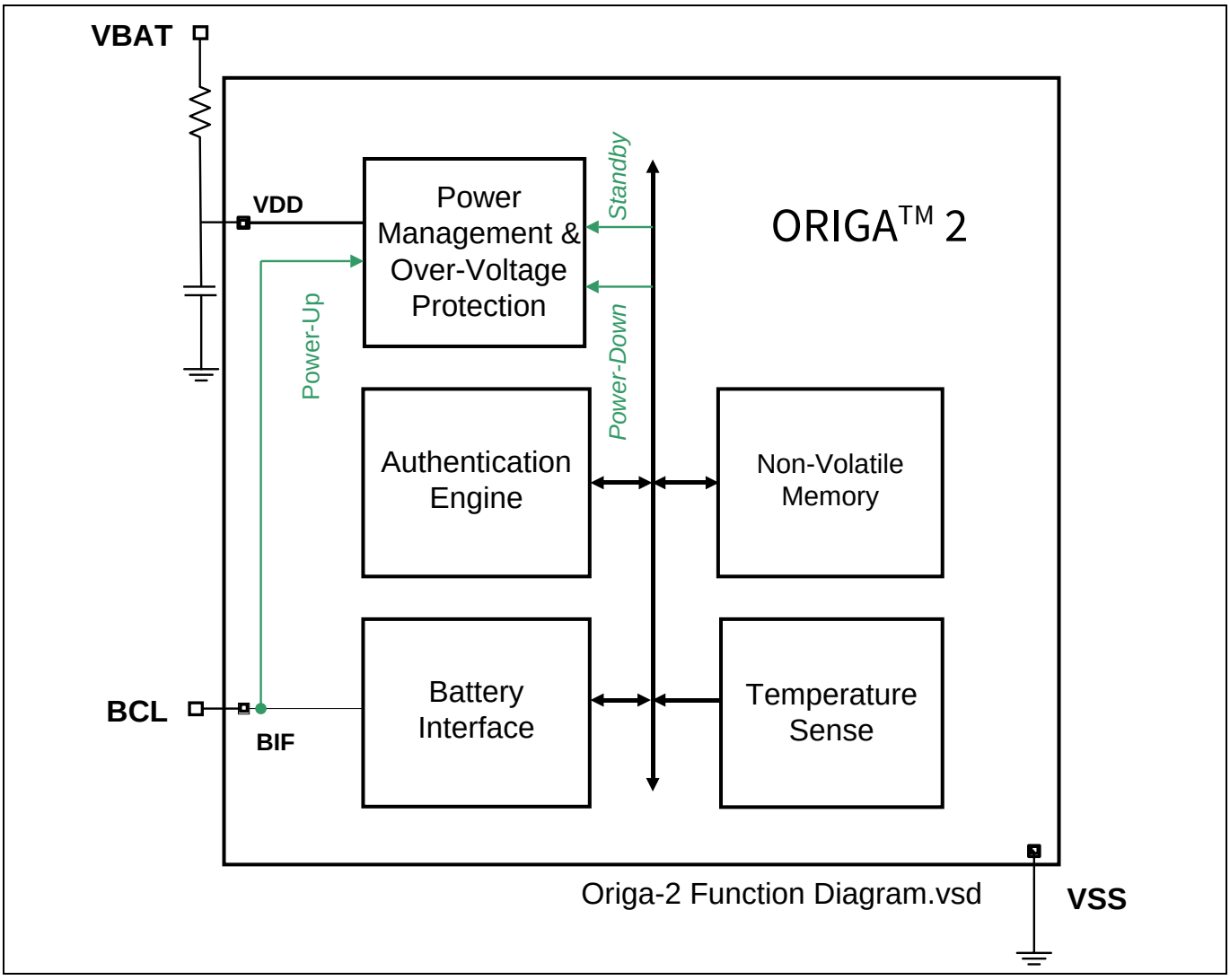

Figure 1 Function Overview

1.2 Application Domain

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).

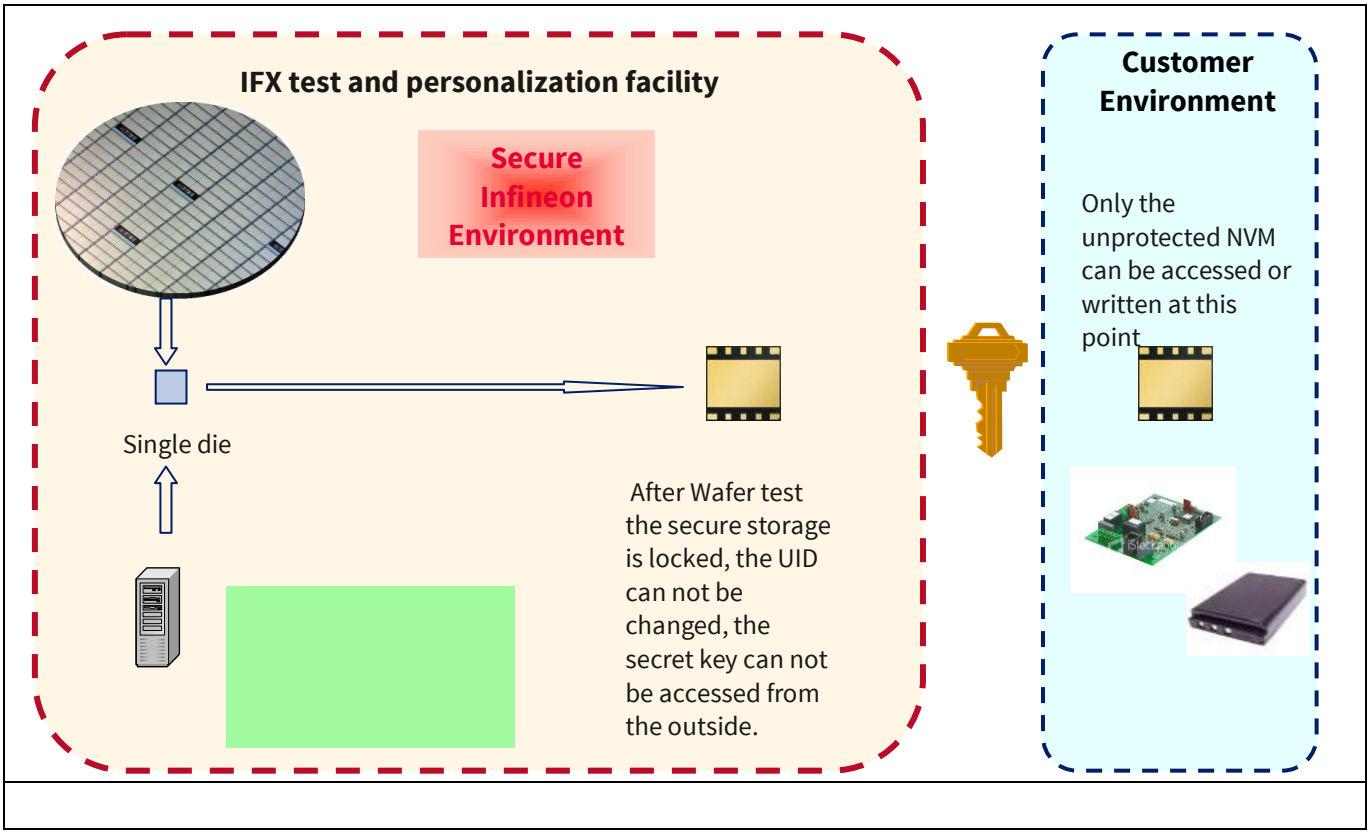

Figure 2 Personalization

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™ 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

Figure 3 shows how the ORIGA™ 2 device Battery Authentication IC can be used in a single Lithium Ion cell battery pack application as a digital single wire Primary Class II slave to a master controller. It can be supplied from the battery pack cell with BIF pin connected to BCL, as shown. A Lithium Ion cell battery pack always contains protection circuit, called Safety Function in the diagram. (This is not included in SLE95200H). The MIPI Battery Interface specification mentions about the host battery insertion/removal Presence Detector which is useful for creating interrupts to the Host IC SW layer.

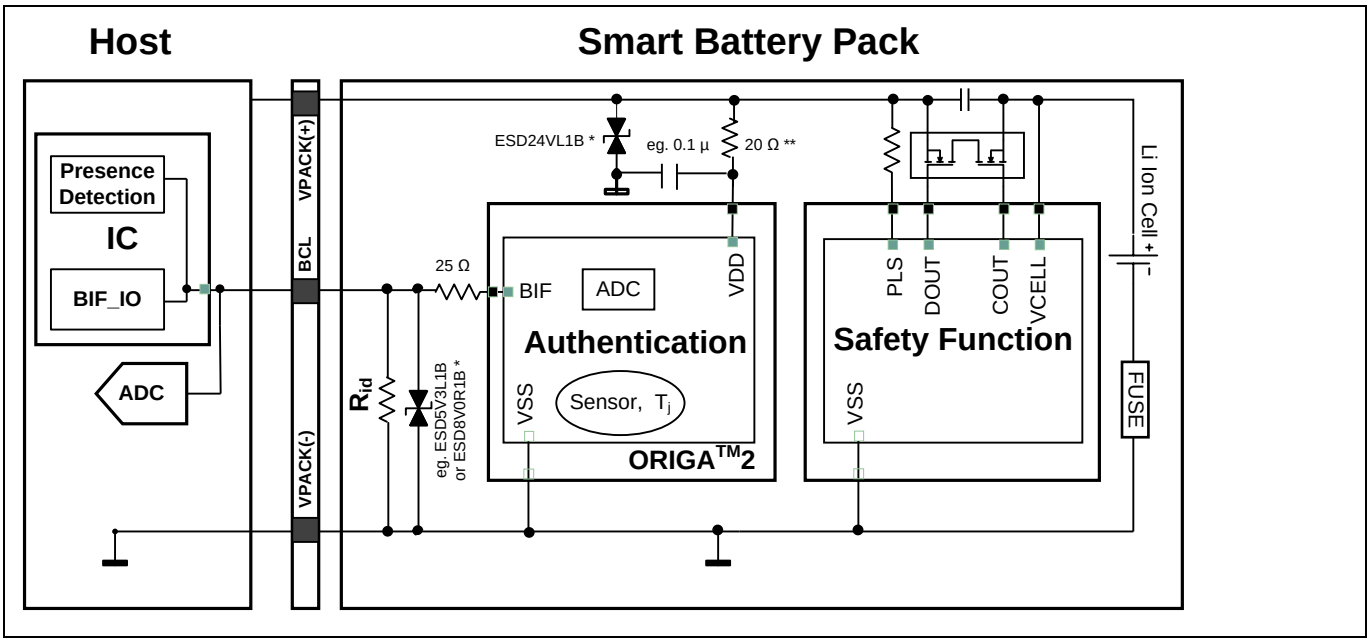

Figure 3 Rechargable Smart Battery Pack Application.

Attention: * External ESD components depend on system ESD requirement.

Attention: A 4.7K Ohm pull-up resistor at the host controller GPIO is recommended. For bigger pull-up values, please ensure the signal rise and fall time meet BIF specification and requirement.

2.1 Advantages

Infineon Technologies' ORIGA™ 2 family offers the following advantages:

- Advanced security using unique asymmetrical public/private key cryptography with two different keys for encryption and decryption
- Improved total system cost by allowing robust host-side implementation in software without compromising security
- 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) for storage of device behavior or logistic information (e.g. storage of number of usage cycles, user data and logistic chain traceability)
- The NVM is large enough for ORIGA™ Digital Certificate (ODC) security upgrade allowing unique key pairs for each device (optionally available)
- Convenient Temperature Monitoring and fast battery presence detection
- MIPI BIF compliant single wire Battery Interface

3 System Features

3.1 Asymmetric Cryptography Engine

- Elliptic Curve Cryptography (ECC) – 163-bit key authentication
- ORIGA™ Digital Certification
- Integrated Random Number Generator
- Unique challenge/response used in each authentication
- Software library available for easy host integration

3.2 Non-Volatile Memory (NVM)

- 3.5 kbits of user space with minimum of 10 years storage
- User programmable Write Lock
- Fast NVM access via Brust read/write mode

3.3 Temperature Sensor

- Integrated Precision Junction Temperature Sensor measurement from -30°C to 110°C
- ± 2°C accuracy from -10°C to 70°C
- ± 3°C accuracy from -30°C to -10°C and 70°C to 85°C.
- ± 6°C accuracy from 85°C to 110°C.

3.4 BIF Interface

- Please refer to Standardization Specification for digital protocol and interface

3.5 Power Management

- On-chip over voltage protection (OVP) against faulty power supply
- Power Up and Down Control via Digital Interface
- Power Standby and Sleep Modes

3.6 Package

- USON-3 package of width of 2mm is suitable for slim battery pack
- Package Size: 3.3mm ± 0.1mm X 2.0mm ± 0.1mm
- Pitch: 0.5mm ± 0.1mm
- Height: 0.6mm (Max)
- The packages comply with RoHS standard
- Operating ambient temperature of -30°C to 110°C

3.7 Others

- ESD
    - HBM = 2kV
    - CDM = 500V

4 Electrical Characteristics

Stresses above the max. values listed here may cause permanent damage to the device. Maximum ratings are absolute ratings; exceeding only one of these values may cause irreversible damage to the integrated circuit.

Table 1 Absolute Max Ratings

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Supply	V_{DD}	-20		+20	V	max 1A, indefinite time. Test condition: BIF pin unconnected.
Cell	V_{cell}			4.8	V	
I/O	V_{BIF}	-0.5		7	V	
ESD robustness HBM	$V_{ESD,HBM}$			2000	V	JESD22-A114-B
ESD robustness CDM	$V_{ESD,CDM}$			500	V	JESD22-C101-A
Storage Temperature	T_{store}	-65		125	°C	High temperature incurs NVM retention time penalty

Attention: Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

4.1 Operating Characteristics

Table 2 Operating Specification

Parameter	Symbol	Values			Unit	Note/Test Condition
		Min	**Typ**	**Max**		
Ambient Temperature	T_{Amb}	-30		110	°C	
Powered Time	P_{oH}			6×10^4	Hr.	At 85°C Junction Temperature
On-Off Cycles	$N_{on/off}$			5×10^4		
NVM Endurance	N_{cyc}		10^5			25°C
NVM Retention	T_{retent}		10		years	At 85°C. NVM operates up to 85°C.
NVM Failure Rate	T_{undet}		10		fit	Undetected during manufacturing.
Battery Supply	V_{DD}	2.2		4.8	V	Measurement at VDD pin.
Current Consumption, Active Mode	$I_{VDD, Active}$		0.5		mA	No activity
Current Consumption, Active Mode	$I_{VDD,Active-ECC}$		3.1		mA	During Authentication Response Computation
Authentication Function Current Consumption, Standby Mode	$I_{VDD,STB}$		0.1		mA	
Authentication Function Current Consumption, Power-Down Mode	$I_{VDD,OFFT}$		1.0		uA	

Table 3 BIF I/O Characteristics

Parameter	Symbol	Values			Unit	Conditions/Remarks
		Min	**Typ**	**Max**		
Protocol Input High Voltage	V_{IH}	0.9		3.0	V	
Protocol Input Low Voltage	V_{IL}	-0.5		0.3	V	
Open-Drain Output	V_{OL}			0.1	V	I_{BIF}=1mA
Input Hysteresis	V_{Hyst}	50			mV	
Wake-up Input Threshold	$V_{ITH,wake}$	0.3		0.9	V	

Parameter	Symbol	Values			Unit	Conditions/Remarks
Wake-up Glitch Suppressor Pulse Width	t_{sup}			30	us	A sequence of small pulses that adds up to the tsup also triggers wake-up. It does not reject low pulse longer than 30 ms.
Bus Power Up Delay				10	ms	MIPI Aliiance Specification
Pull-Up Current	I_{PU}			0	uA	No weak internal pull-up as it causes leakage current
Pull-Down Current	I_{PD}			0	uA	No weak internal pull-down as it interferes with R_{BSI} measurement
Leakage Current	$I_{leakage}$			700	nA	Measurement is done not immediately after an ESD event.
BIF Protocol Timing						Refer to MIPI BIF Specification
Powering Down Low Time	t_{BIF_LOW}		1.5		ms	

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.

Table 4 Authentication Response Computation Time

Parameter	Symbol	Values			Unit
		Min	Typ	Max	
Response Computation Time, ECC-131	T_{ECC131}		67		ms
Response Computation Time ECC-163	T_{ECC163}		100		ms
Response Computation Time ECC-193	T_{ECC193}		135		ms

5 Packaging

The SLE95200H comes in a PG-USON-3-1 type package.

5.1 Pin Configuration

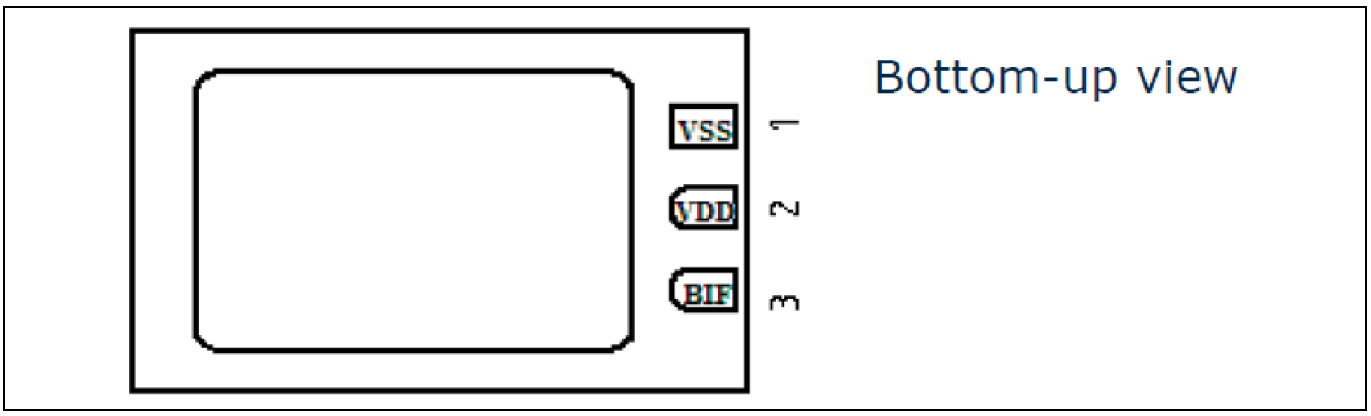

Figure 4 Pin Configuration (PG-USON-3-1 package)

5.2 Pin Out

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

Pin No.	Pin Name/ Pad Inst	Pad	Function
1	VSS	VSS_PAD	Ground
2	VDD	VDD_PAD	Power supply
3	BIF	BIF_PAD	Open drain pull output driver

5.3 Package Dimensions of PG-USON-3-1

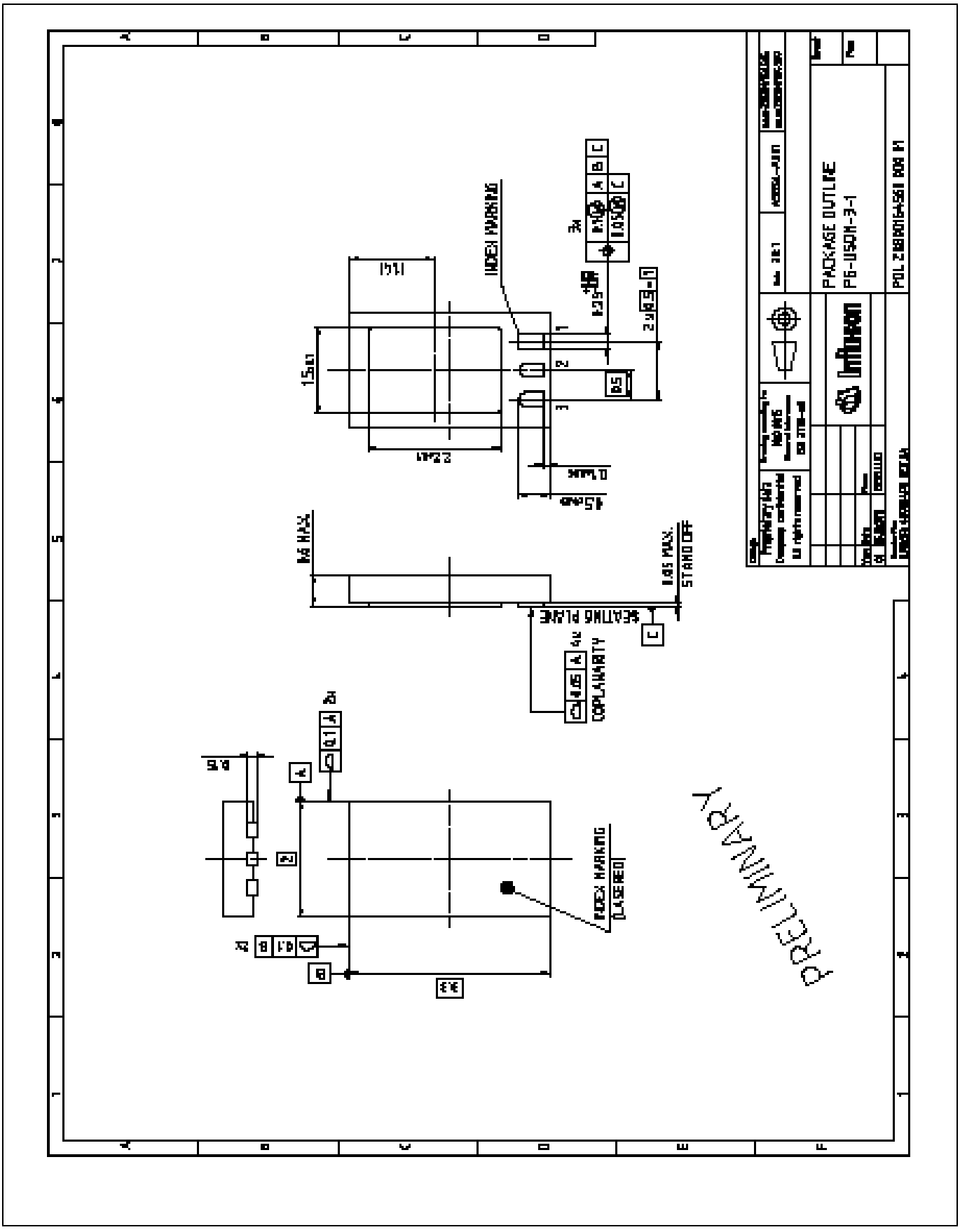

Figure 5 PG-USON-3-1

6 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.

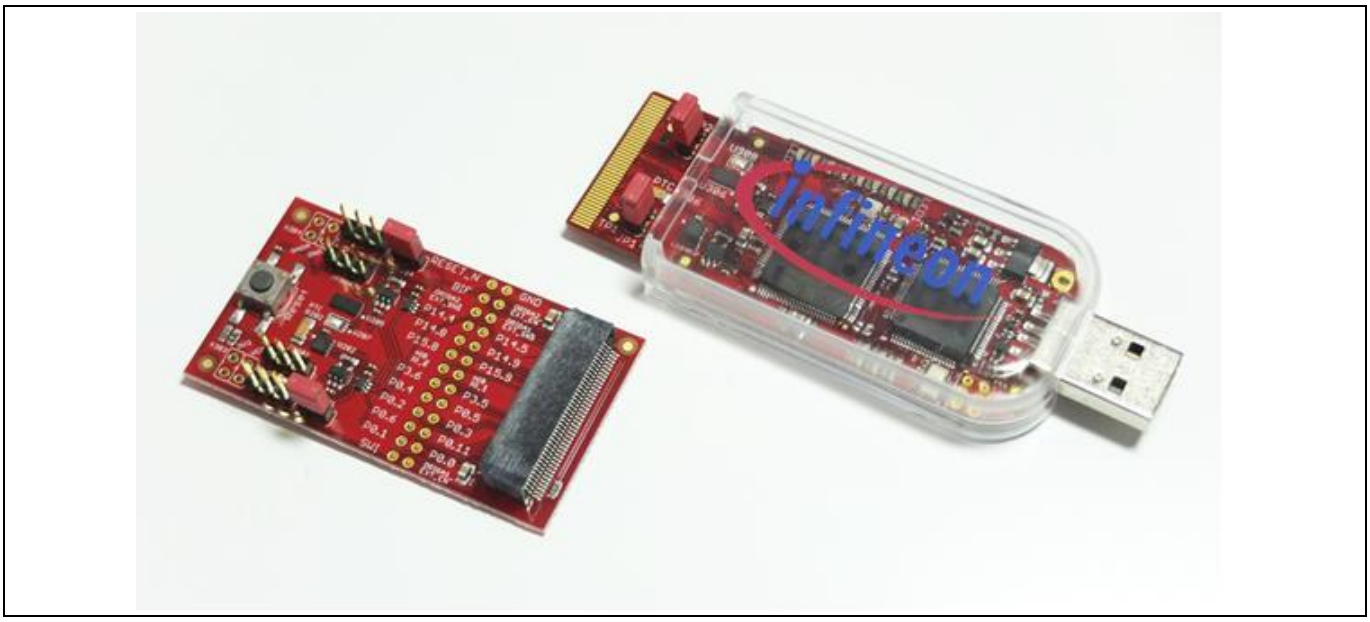

Figure 6 USB Evaluation kit

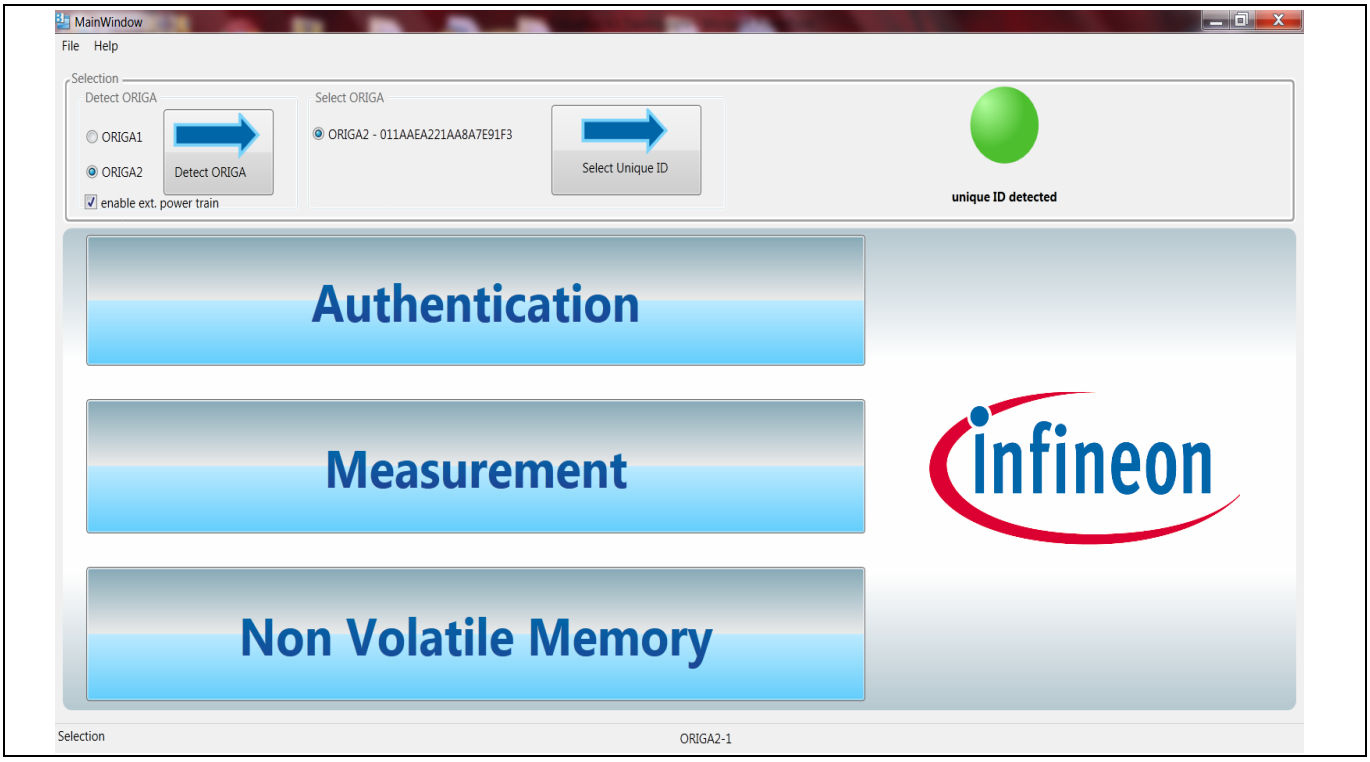

Figure 7 Evaluation kit Software

Revision History

Major changes since the last revision

Page or Reference	Description of change
	ORIGA™ SLE95200H 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

SLE95200H 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.