Release, Version 1.00, February 2012

ORIGA™ SLE95200

Original Product Authentication and Brand Protection Solution

Short Product Information

www.infineon.com/ORIGA

Power Management & Multimarket

Never stop thinking

Published by
Infineon Technologies AG
81726 Munich, Germany

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, 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.

Information

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

Warnings

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

Infineon Technologies components may be used in life-support devices or systems only 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.

Preface

This document is the Product Brief of SLE95200 (ORIGA™2).

This version of the Battery Authentication and Protection Product Overview is an advanced release, issued to selected customers previous to the full product release in order to provide early product information and enable review and feedback to Infineon. Features and spec values may be changed without notice.

Textual Convention

This document uses the following textual conventions:

- Functional units of subsystems are given in plain UPPER CASE. For example: “The SSC can be used to communicate with shift registers.”.
- Pins using negative logic are indicated by a N postfix. For example: “A reset input pin, RESETN, is provided for the hardware reset.”.
- The default radix is decimal. Hexadecimal constants have a suffix with the subscript letter “H”, as in 100_H. Binary constants have a suffix with the subscript letter “B”, as in: 111_B.

Units are abbreviated as follows:

- KByte = 1024 bytes of memory
- MHz = Megahertz
- Byte = 8-bit quantity
- MByte = 1,048,576 bytes of memory
- kBaud, kBit = 1000 characters/bits per second
- MBaud, MBit = 1,000,000 characters/bits per second
- µs = Microsecond

1 Overview

Infineon Technologies' ORIGA™ SLE95200 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 aftermarket 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.

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.

11 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
- MIPI **[1]** BIF compliant single wire Battery Interface

2 General Description

ORIGA™2 is an integrated Battery Authentication IC. It features a built-in strong asymmetric cryptography engine and up to 4 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 **[1]** Battery (digital) Interface. **Figure 2.0** shows the ORIGA™2 device Battery Authentication IC function overview.

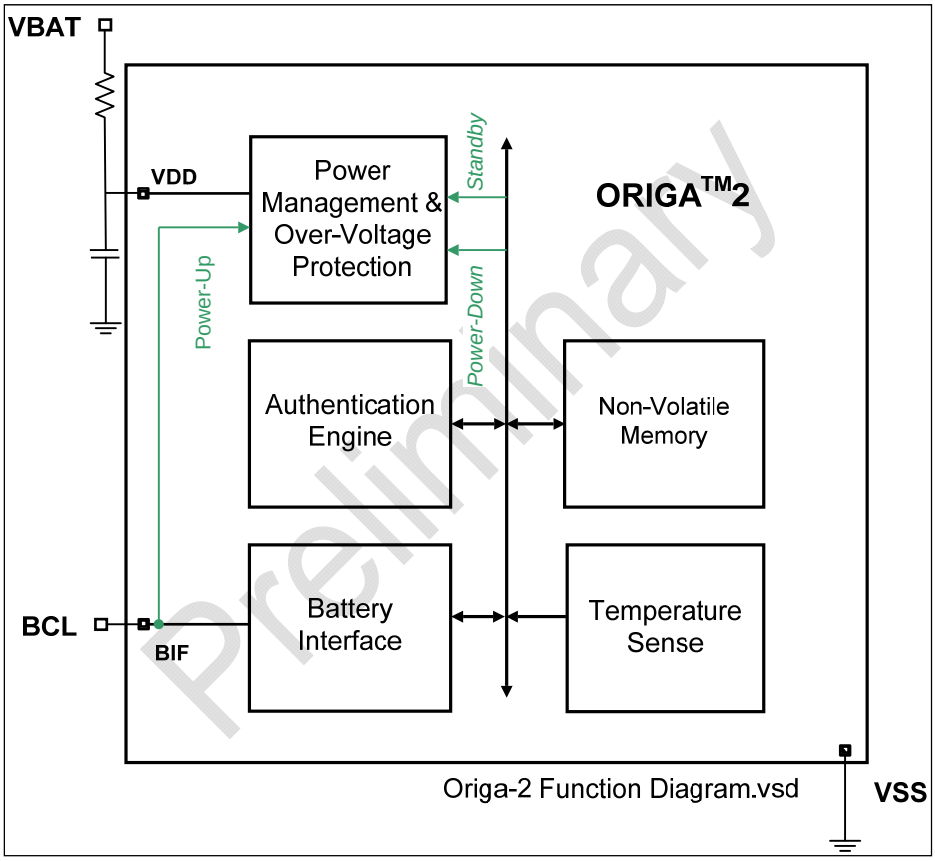

Figure 2.0 Function Overview

2.1 Applications

The main area of application is authentication leading to increased safety, functionality and reliability of the accessories, replacement parts and disposables with a special focus on batteries.

The 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 the suitable next steps. Also the re-use of the chip as well as unauthorized re-use or re-provisioning of the original part can be avoided using the data authentication feature.

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

2.2 Typical Circuit

Figure 2.1 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(Battery Communication Line), as shown. A Lithium Ion cell battery pack always contain protection circuit, called Safety Function in the diagram. (This is not included in SLE95200). The MIPI Battery Interface **[1]** specification mentions about the host battery insertion/removal Presence Detector which is useful for creating interrupt to the Host IC SW layer.

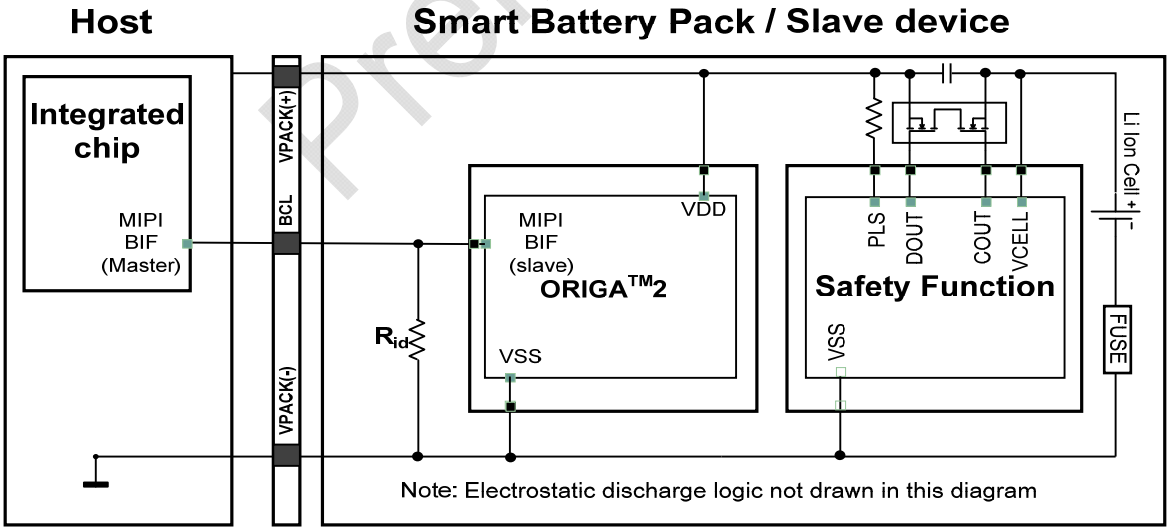

Figure 2.1 Rechargeable Smart Battery Pack Application

2.3 Features

The features are listed as follows:

- Strong Asymmetric Cryptography Engine
  - Elliptic Curve Cryptography
  - ORIGA™ Digital Certification
  - 163 bit standard Key Length
  - Integrated hardware security measures
  - MAC Function for User Data Authentication
  - Processing of complete challenge/response
  - Library Concept for easy host side integration available
- Battery Interface (BIF) **[1]**
  - Low Power and Low Voltage Signalling using Time Distance Coding
  - Unified access to all functions to enable generic SW driver usage in the systems
  - Allow vendor specific functions in addition to MIPI BIF- defined basic functions that enable slave device differentiation in the market
  - The BIF interface was also defined to be compliant with other required battery standards for mobile devices
  - Non-Volatile Memory User Space of 3.5Kbits with Minimum of 10 Years Storage
  - Non-Volatile Memory User Space with User Programmable Write Lock Page granularity (64 bits per page)
  - Non-Volatile Memory Protected Space which cannot be modified by the end user
  - Non-Volatile Memory endurance of 10^5 erase/write cycles

  Please refer to Standardization Specification for digital protocol and interface
- Temperature Sensor
  - Integrated Precision Junction Temperature Sensor measurement from -25 °C to 85 °C
  - ± 2 °C accuracy from -10 °C to 70 °C
  - ± 3 °C accuracy from -25°C to -10 °C and 70 °C to 85 °C.
  - Temperature alarm feature
- Power Management
  - On-chip over voltage protection (OVP) against faulty charger
  - Single Supply Voltage for Authentication Function
  - Power Up and Down Control via Digital Interface
  - Power Standby and Sleep Modes
- Packages (Preliminary information)
  - ORIGA™2 device available in USON-8 sample package, final package tbd
  - The packages comply with RoHS standard
  - Operating ambient temperature of -25 °C to 85 °C – Refer to **Operating Specification** for detail

3. MIPI BIF Explanation

Compared to ORIGA™1 the ORIGA™2 device not only employs the Infineon single wire interface it now is also extended with 4-bit error detection and all other extended features that make it MIPI Battery Interface (BIF) standard compliant.

The MIPI Battery Interface (BIF) is the first comprehensive battery communication interface standard for mobile devices. BIF is a robust, scalable and cost-effective single-wire communication interface between the mobile terminal and smart or low cost batteries. BIF improves mobile terminal safety and performance by providing comprehensive battery monitoring data and functions in a structured, software-friendly manner. The BIF specification is designed to replace all existing proprietary battery interface solutions.

Main advantages are:

- Smart Battery Support coexisting with Low Cost Battery Support
- Fast Battery Pack Presence Detection
- Single Wire Interface
- Support for Battery Authentication Function as well as Battery Temperature Monitoring
- Slave Interrupt support & Multi-slave support
- Manufacturer specific Function support
- Unified SW access to all functions and data
- Unified, scalable data structures and scalable function content in a Slave device based on need.

For more information please see, where you can also download the whitepaper on MIPI-BIF Interface.

http://www.mipi.org/working-groups/battery-interface

The BIF transceiver implements the BIF physical logic **[1]**. The digital transceiver operates in half-duplex as a BIF slave device. It detects parity error using 4-bit-Hamming-15 coding. It also distinguishes Broadcast Word and Unicast Word. The data payload is extracted for the Programmable Controller to further process. The Programmable Controller implements the DDB according to the MIPI Data Map **[1]**.Therefore the features of the device qualify it as a MIPI **[1]** Class 2 Smart Battery Primary Slave device

3.1 Non-Volatile Memory

The Authentication Engine and temperature sensing function use it as non-volatile storage in protected region. Battery Pack Management function can use upto 4 Kbits (standard 3.25 Kbits) provided in the user area which is lockable, according to the MIPI Battery Interface Specification **[1]**.

4 Authentication

The Infineon ORIGA™2 is an asymmetric key authentication device using Elliptic Curve Cryptography **[3]**

4.1 Introduction to Authentication & Cryptography

The Infineon ORIGA™2 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 Pay-TV 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.

Figure 4.1 shows how multiple ORIGA™2 devices can be connected to a single Host. In this lowest system cost configuration (software-to-hardware authentication), the host side can be done with a small piece of code library and only a very small Data RAM need in a 16-bit micro-controllers. The host-side implementation runs on the host processor in Software without compromising the security of the system, unlike in symmetric cryptography systems (e.g. SHA/DES/TDES/AES).
The reference code can be licensed by Infineon for use in conjunction with the ORIGA™2 device.

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 read out. Typically, symmetric algorithms are used in situations where a secure surrounding environment can be established, like in banking and data transmission.

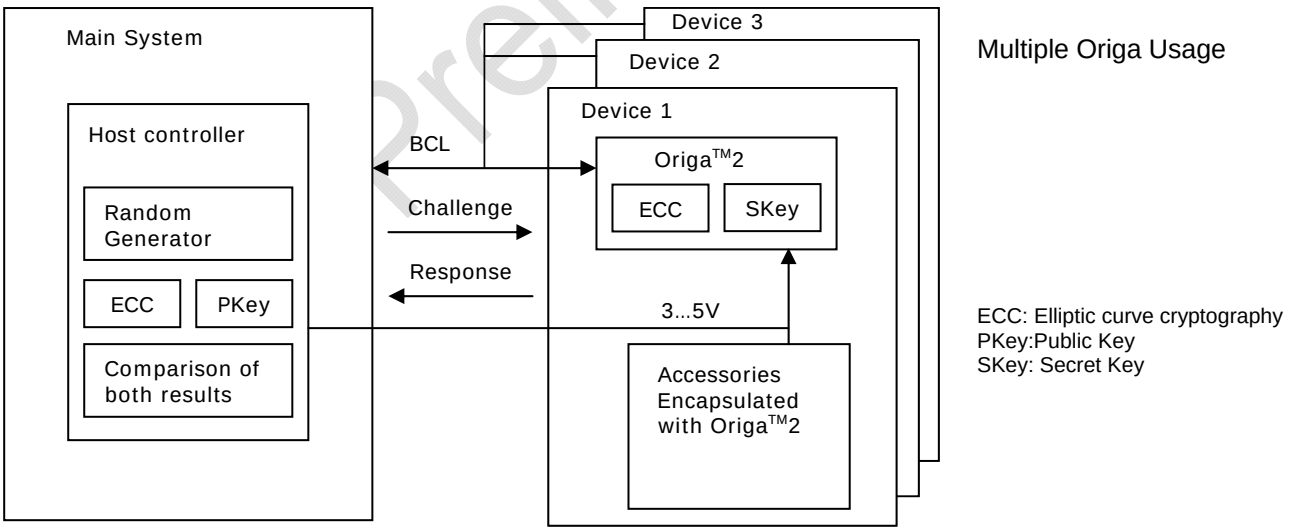

Figure 4.1 Software-Hardware Authentication System

On the other hand asymmetric cryptography uses two different keys for encryption and decryption. One key, the so called public key (P-Key), can be made public (and therefore used in the Software implementation), as long as the other key, the secret key (S-Key, 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 asymmetric cryptography algorithm and the one most suitable for embedded applications.

The ORIGA™2 device from Infineon uses a specific elliptic curve cryptography (ECC) algorithm 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.

Additionally, the Infineon ORIGA™2 devices offer unprotected and freely usable NVM up to 4 Kbits 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.

4.2 Personalization

Personalization must be performed in a controlled, trusted and protected environment, to prevent any misuse or illegal use of chips and especially secure generation and injection of key material. Also customer parameters must be protected against unauthorized knowledge or use. Infineon provides a secured environment for the process, as shown in **Figure 4.2**.

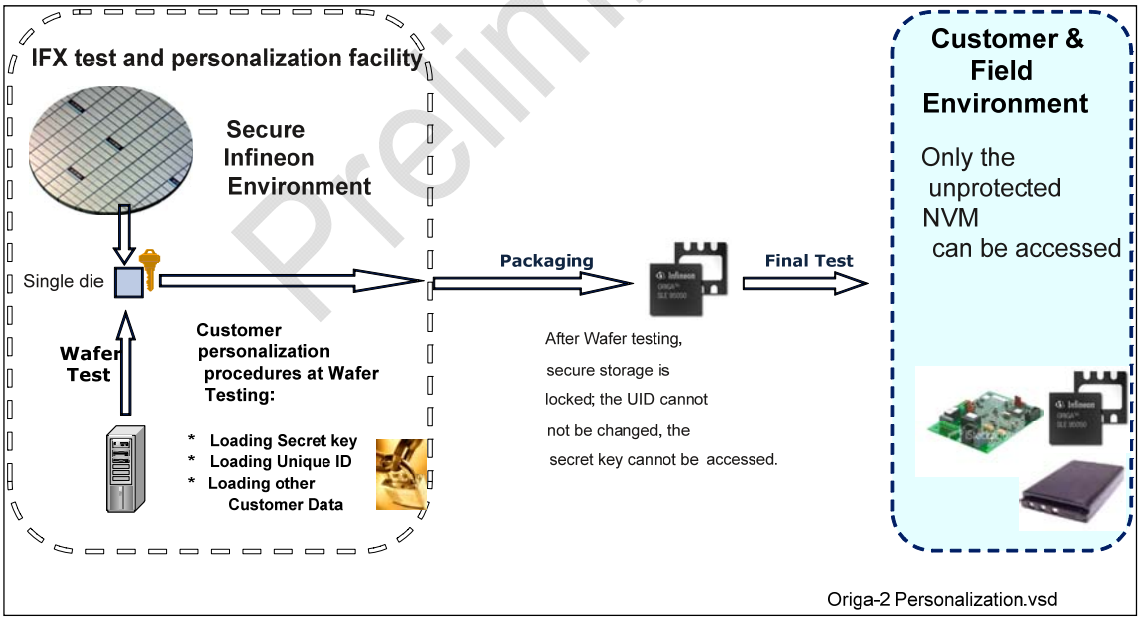

Figure 4.2 Personalization Process

The following steps are the Chip & Customer Personalization procedures at the Infineon Wafer Testing site: The followings are the Customer Personalization procedures at Wafer Testing site:

- Generating & Provisioning Secret key
- Generating & Provisioning Unique ID
- Loading other Customer Data
- Optionally securely generating and provisioning the ORIGA Digital Certificate

After Wafer Testing, the secure storage is locked, the Unique ID cannot be changed and the secret key cannot be accessed from the outside.

Only the unprotected region of the non-volatile memory can be accessed after the lock is applied.

Infineon's security chip manufacturing and testing facility is security certified and evaluated by a third partyauthority, and it meets the requirements for performing the critical personalization flow. ORIGA™2 customers (or their approved contracted manufacturers) receive unique sets of key pairs associated with customers' products.

4.3 ORIGA™2 Authentication Functions

ORIGA™2 performs these:

- Elliptic Curve computation **[3]** working hand-in-hand with the Host side provided C-library
- Message Authentication Code (MAC) computation
  – a new session key pair is generated in each authentication performed
  – this Session key is used subsequently for authentication of user data
- Storage of ORIGA™2 Digital Certificate
- Various hardware protection measures against the most common attacks and improved measures to protect the private key in the chip

4.4 ORIGA™2 Authentication System

The authentication process in the device works hand-in-hand with the Host side ECC process as shown in **Figure 4.3**. Please refer to (host) software programmer's guide and application notes for system integration. The authentication process works as in the following steps:

Step1 (Generate Challenge): After the Host is switched on, its Authentication Module sends a Challenge to the accessory (where ORIGA™2 resides), to check if it is an authorized accessory.

Step2 (ORIGA™2 Authentication Computation): ORIGA™2 in the accessory Responds to the Challenge.

Step3 (Generate check Value): The Host computes the expected Response while the accessory computes the Response.

Step4 (Verify Response): The Host compares the Response from the accessory with its calculated expected Response. It can then decide what action to take depending on the result of the comparison. For example, in a battery these actions can range from just recording the failed authentication, to showing messages that an unsafe is used to only charging with a safe reduced rate or even not charging at all.

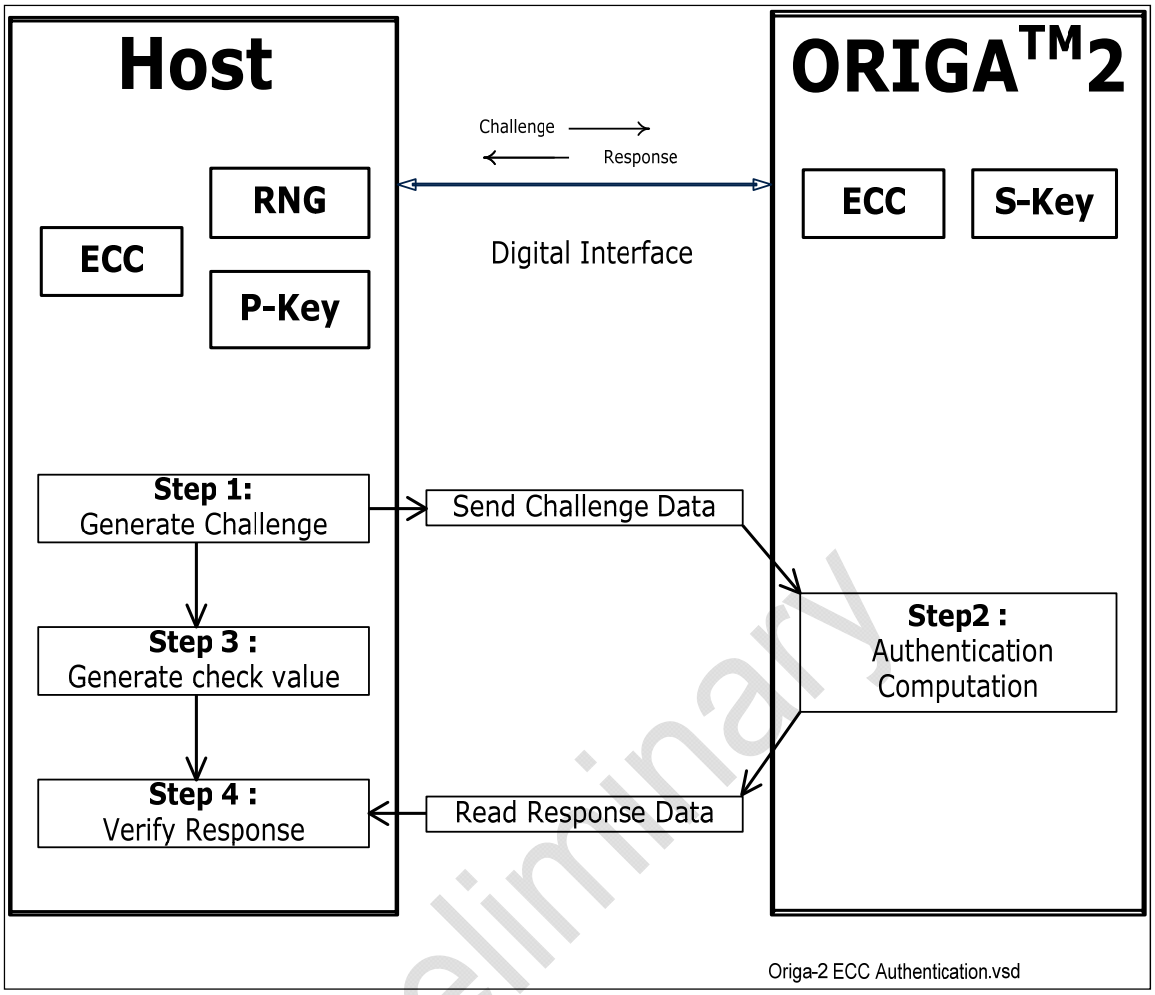

Figure 4.3 ECC Authentication System

5 Pin Assignment

Table 5.0 shows the pin assignment of the package in **Figure 8.0**.

Table 5.0 Pin Assignment

Pin No.	Name	Pad	Buffer Type	Function
1	VSS	VSS_Pad	Suppy	**ORIGA2 Ground**
2	VDD	VDD_Pad	Supply	**ORIGA2 Supply Voltage**
3	BIF	BIF_Pad	Open Drain	**BIF Single Wire Interface**

6 Absolute Maximum Rating

Warning: 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 6.0 Absolute Maximum Ratings(Preliminary)

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		
I/O	V_{BIF}	-0.5		+7	V	
ESD robustness HBM	$V_{ESD,HBM}$			2000	V	JESD22-A1 14-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

Note: Exceeding maximum rating conditions for extended periods may affect device reliability.

7 Operating Conditions

Table 7.1 Operating Conditions (Preliminary)

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Ambient Temperature	T_{Amb}	-30		85	°C	
NVM Endurance	N_{cyc}		10^5			25°C
NVM Retention	T_{retent}		10		years	At 85 °C
Battery Supply	V_{DD}	2.2		4.8	V	
Current Consumption, Active Mode	$I_{VDD, Active}$		1.0		mA	No activity
Current Consumption, Active Mode	$I_{VDD, Active-ECC}$		3.1		mA	During authentication response calculation
Authentication Function Current Consumption, Standby Mode	$I_{VDD,STB}$		0.2		mA	
Authentication Function Current Consumption, Power-Down Mode	$I_{VDD,OFFT}$		1		µA	

8 Package Outline: PG-USON-3

The package for SLE95200 planned for mass production is PG-USON-3. The package outline are shown below

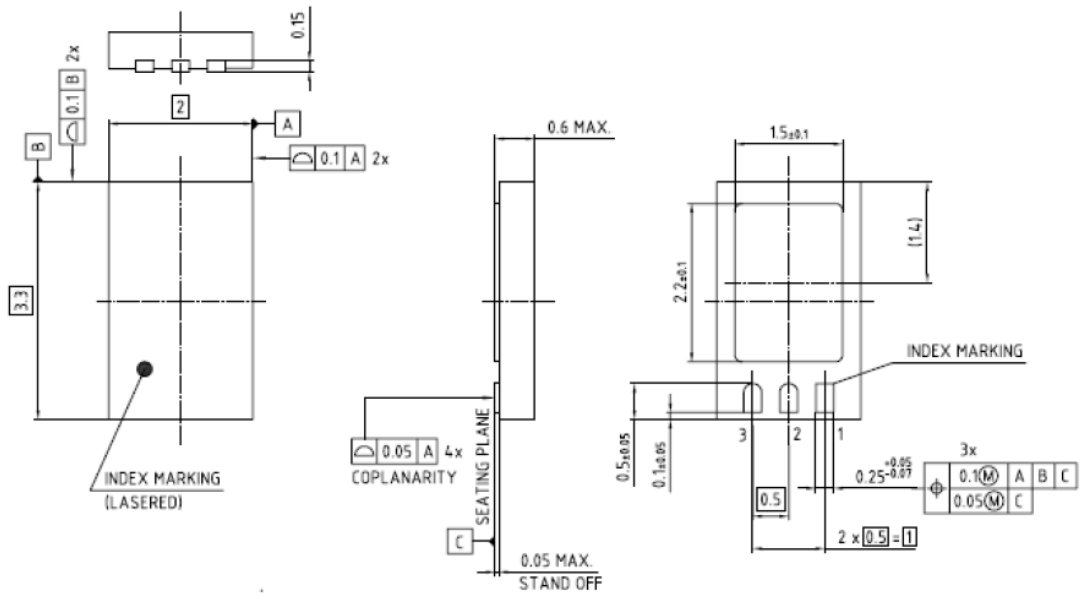

Figure 8.2 PG-USON-3 Package Outline

References

[1] MIPI Alliance Specification for Battery Interface, version 0.9.00, 27 October 2011

[2] MIPI Alliance Battery Interface Working Group, http://www.mipi.org/working-groups/battery-interface

[3] Overview of Elliptic Curve Cryptosystems, http://www.rsa.com/rsalabs/node.asp?id=2013