



Never stop thinking

Infineon ORIGA™ -- Original Product Authentication and Brand Protection Solution -- SLE 95050

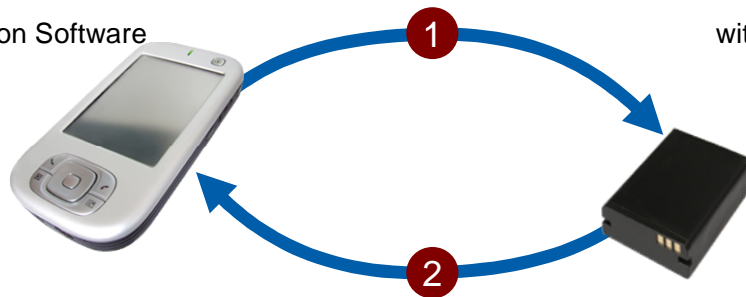
ORIGA™ SLE95050

Industry's first Low Cost Brand Protection device, featuring Authentication with Asymmetric Cryptography and Temperature Sensing.

How does it work?

Example: Battery Brand Protection & Authentication

Mobile Device:
with Authentication Software
Module inside



Accessory:
with Authentication
Chip inside

Mobile Device is turned on and its Authentication Module sends a challenge to the battery to check if it is an authorized battery

- n ORIGA™ in the battery responds to the challenge
- n Authentication Module compares challenge & response and authenticates the Battery
- n Mobile Device software can then decide what action to take depending on the result of Battery authentication (i. e., show a message that a fake battery has been detected, advise on purchase of original battery and that it will only operate in a reduced power mode to ensure safety and good results, or any other action).

APPLICABLE TO ANY ACCESSORY CONCEPT

Key Features

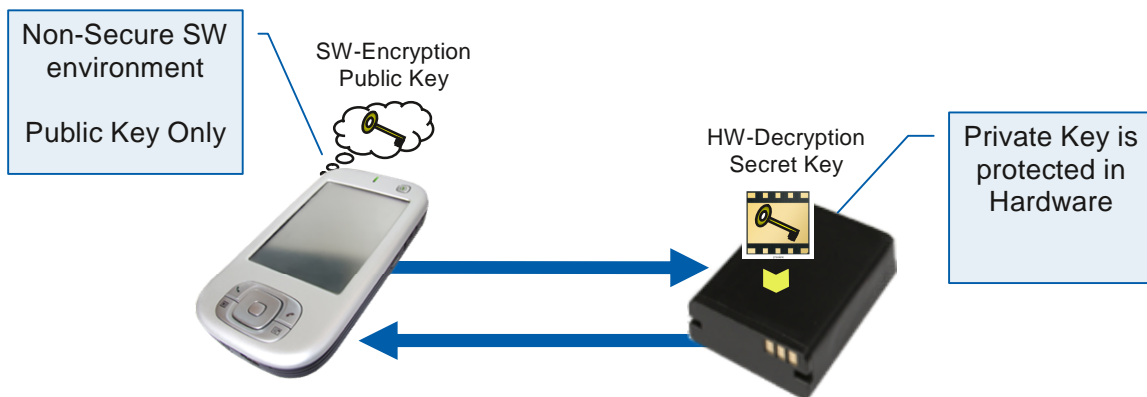
- n Asymmetric cryptography allows robust host side software implementation with public key; even without a costly master device, there is no compromise to security
- n Built-in ADC for convenient temperature monitoring by sending a command and reading the temperature value (or other sensor data)
- n Easy to implement Single-Wire host interface
- n Remote power from host possible
- n Low power device
- n NVM: Personalization of accessory, host immediately knows which accessories are attached
- n Life-span indicator

Applications

- n Brand Protection & Clone prevention
- n Authentication of Accessories, Disposables and Replacement Parts like
 - o Batteries
 - o Headsets, Speakers and Docking Stations
 - o Chargers
 - o Diagnostic Supplies and Medical Equipment
 - o Printer Cartridges
 - o Other Accessories like Game Controllers
- n Accessories pairing
 - o Theft deterrent
 - o Brand Partner Program
 - o End-to-end system integrity
- n Authentication of system services, functionalities and parts in networked systems
 - o Online operation monitoring
 - o Product warranty program

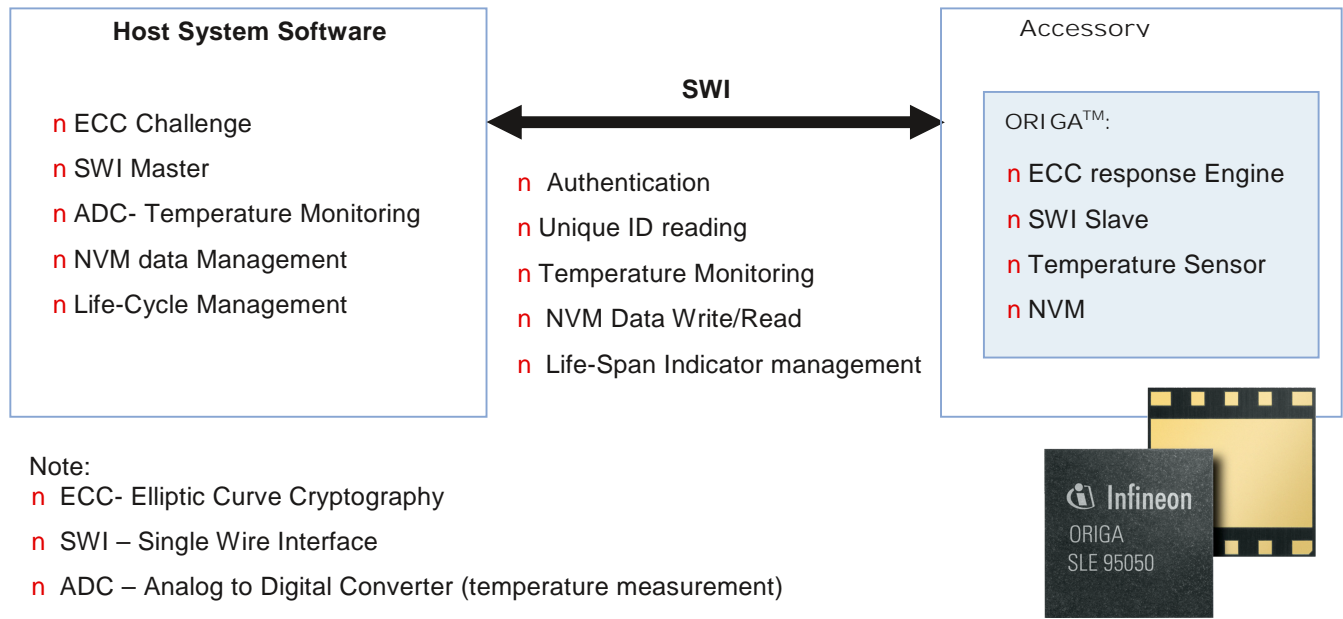
Advantages of asymmetric cryptography

Asymmetric: Two **different** keys for En- and Decryption



ORIGA™ offers Superior Security at Lower System Cost compared to symmetric solutions

System Integration Overview:



Asymmetric Authentication

- n Asymmetric Authentication makes use of two **different** keys for En- and Decryption, a public key and a private key.
 - n The benefit of Asymmetric Authentication is that only one of the keys, the secret key, has to be protected in the silicon while the host side with the public key does not need protecting and can be implemented in software
 - n This is a big advantage over systems which rely on symmetric algorithms: in order to have a robust host side implementation in that case, the host side key has to be protected in a costly master device, as the exact same key is used for encryption/decryption and therefore must not be exposed.
- à **The Infineon SLE95050 uses Asymmetric Authentication which does not require a security device on the host side and still offers a higher security level than symmetric authentication solutions**

“Improved Security at reduced system cost” –
asymmetric cryptography allows secure host side implementation in software