OPTIGA™ Trust – SLS 10ERE

Your Authentication Solution for Increased Security and Lower System Costs

July 2014

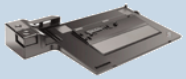
Why device authentication?

PROFIT
Toner & printer cartridges

PRIVACY
Data encryption and secure storage

LIABILITY
AC adapter

QUALITY
Projector



RELIABILITY
Docking station

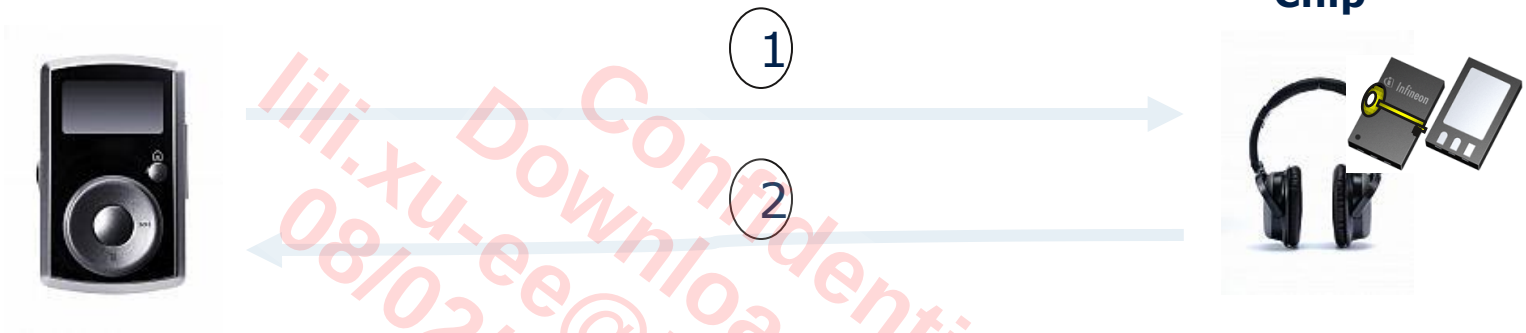
SAFETY
Medical devices

IMAGE
Company Brand

How does authentication work

HOST DEVICE
SW authentication Module

ACCESSORY:
Authentication Chip



1. The embedded device is turned on and its Authentication Module sends a challenge to the accessory to check if it is an authorized accessory
2. The Authentication Chip in the accessory responds to the challenge
3. The Authentication Module compares challenge & response and authenticates the accessory
4. The embedded device software can then decide what action to take depending on the result of accessory authentication (i.e., show a message that a fake accessory is used and advise on purchase of original accessory 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

Product counterfeiting inflicts billions of dollars in damages to businesses

IACC (int'l anti-counterfeiting coalition)

- It is estimated that counterfeiting is a **$600 billion a year** problem
- It's a problem that has grown over **10,000 percent** in the past two decades
- **~5% to 7%** of the world trade is in counterfeit goods

Daily more news

The possible applications for OPTIGA™ Trust authentication products are endless

Electronic accessory authentication
(e.g. MP3 players)

ICT Infrastructure authentication
(e.g. routers)

Gaming authentication
(e.g. slot machines)

Industrial

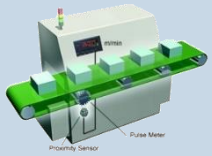
Printer cartridge authentication

Medical equipment authentication

Cloud computing authentication

Software/ IP authentication

Internet of Things
- Connected Home
- M2M Communication

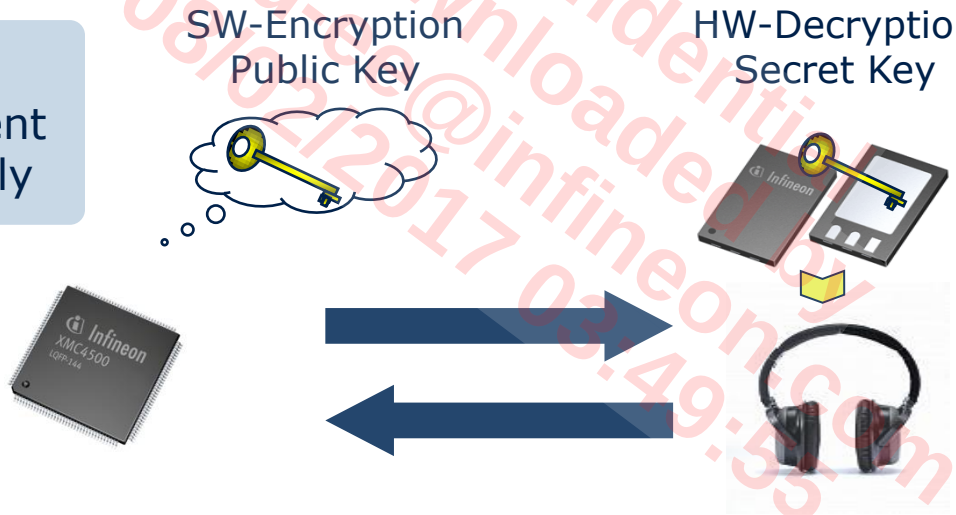


Why OPTIGA™ Trust SLS 10ERE?
Asymmetric Elliptic Curve Cryptography

Symmetrical Algorithms can not afford SW implementations: They pose a high risk of "Break-once, Publish-everywhere"

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

Non-Secure SW environment Public Key Only



Private Key is protected in Hardware

OPTIGA™ Trust SLS 10ERE

Product

- Unique key pair per device
- 163 bit ECC
- 3.5kbit user NVM
- SWI interface

Eval Kit

- Windows based GUI
- USB format

OPTIGA™ Trust

Host side

- C-library for host side support
- Download from myinfineon.com

Documentation

- Databook
- Application notes on ECC authentication, NVM usage, SWI interface

Why OPTIGA™ Trust?

Improved security
- Chip individual, unique magic number, 10 byte unique ID
- State of the art asymmetric elliptic curve cryptography
- Uniqueness provided by chip individual key pair

Optimized system costs with 1 chip solution

Easy integration due to full turn key solution

Lean and easy connectivity with Single Wire Interface

Smallest foot print using USON-3 package

OPTIGA™ Trust Evaluation Board

For Demo

- USB: Simulated Host
- Windows based GUI

For Evaluation

- Based on IFX XMC4500
- Built-in JTAG interface for debugging
- IDE with free license (HiTOP)

Infineon is the partner of choice for the key trends in the device authentication market

Increased security at lower system costs

With advanced hardware based security and asymmetric algorithms

Turn-Key solutions for fast and easy designs

OPTIGA™ Trust products consist of a chip and all necessary software

ENERGY EFFICIENCY
MOBILITY
SECURITY

Innovative semiconductor solutions for energy efficiency, mobility and security.