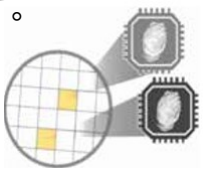
IL005(G1)

VIA PUF Authentificator

H/WによるRoot of Trustを実現します

Introduction

IL005は、VIA PUF技術を用いSHA-256ハッシュアルゴリズムによる暗号化／復号化、認証を実現した世界初のオーセンティケーター（認証機器）です。IL005が実現したハードウェアベースの堅固なセキュリティーソリューションにおいては、複製不可かつ固有のPUFキーが物理的にIC内に生成されます。このPUFキーは、必要に応じて再生成が可能で、メモリ上に保存する必要がないことから、従来のセキュリティーソリューションの限界や脆弱性を根本的に排除することができる革新的なソリューションであると言えます。



Description

IL005はインクカートリッジ、プリンター用トナー、電子タバコの充電池の偽造を防ぐことができます。また、IoT機器のM2M認証やファームウェア保護にも適しています。
IoT機器のファームウェアは、機器の起動時またはファームウェアのアップデート時に、ファームウェアが真正のものであり、且つ、アタッカーによって改変されてないという認証が為されて、初めて保護されていることが証明されます。
ユーザー認証に際しては、ユーザーがIL005デバイス内に正規の暗号化キー持っていることを検証します。
IL005の暗号化特性を利用することにより、IL005にセキュアなストレージ機能を持たせることも可能です。例えば、PUFキーを使用してデータを暗号化することにより、セキュアなストレージ領域を非セキュア領域上に作成することもでき、IL005の内部の鍵が無い限り、暗号化されたデータは機密に保たれます。

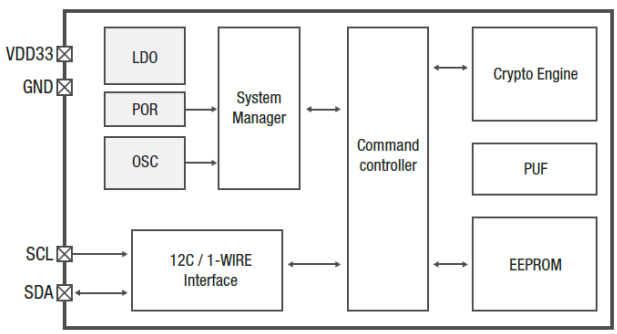
Advantages

- PUF provides the ‘Root of Trust’ on your system
- Unique IDs for each of your devices
- Specificity and competitiveness for your solution
- High-security authentication at the lowest total system cost
- Secure storage on your system
- Low current, compact size and longtime stability for IoT
- Various package options
- Protect firmware and IPs

Key Feature

- PUF value(key) generation
- SHA256/HMAC based symmetric authentication
- Authentication and data encryption / decryption with PUF
- Secure Storage (Encrypted EEPROM data with PUF)
- Store up to 16 keys (256 bit key lengths)
- 5Kbit EEPROM for data and key storage
- Hardware crypto engines : SHA256 / HMAC
- TRNG (True random number generator)
- Operating voltage range : VDD33 : 3.0~3.6 V
- Interface: I2C / 1-Wire (OWI)
- <150nA sleep current
- Security countermeasure: Fault injection & Side channel attack
- Physical attack protection

Block Diagram



Package options

- 8-pin SOIC (SOP)
- 3-pin SOT 23-3L
- 8-pin DFN

Application

IL005 (G1)

Secure ID

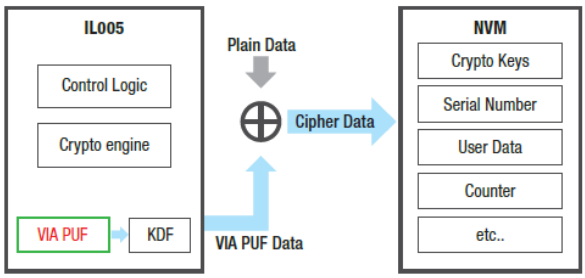
- Direct ID : Use VIA PUF itself as unique ID
- Indirect ID : Inject ID & store by "Secure Memory" concept
- No risk of cloning
- ID card, passport, Driver license, Drone ID etc..

2nd factor authentication

- Secure FINTECH
- Smart door/ Smart card/ IoT sensor & gateway

Secure memory

- Stores data in NVM after encryption by VIA PUF key
- Once use, Do not store VIA PUF Key
- Regenerate the VIA PUF key if necessary

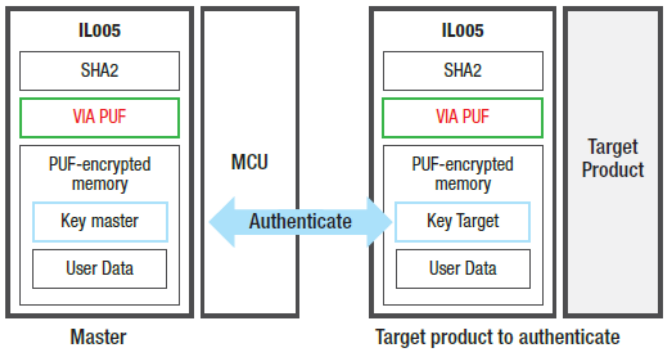


Firmware protection

- Secure boot
- Secure update
- IP protection
- License management

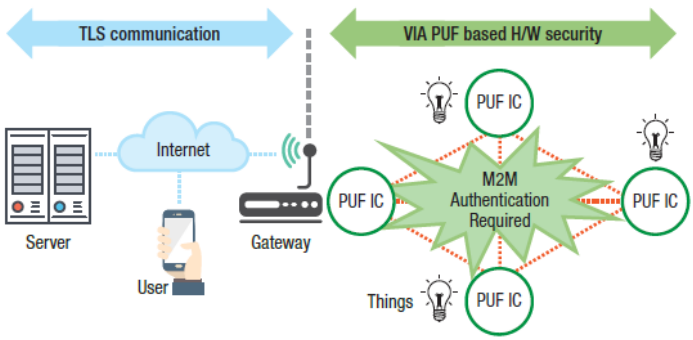
Anti-Counterfeit (off-line)

- Utilize "Secure memory" concept
- Install IL005 in the "Target Product" to authenticate & "Master"
- Enroll "Target Product" before shipping out
- In the field, "Master" and "Target Products" authenticate each other
  - Example : Smart phone accessary, Smart phone battery, Printer ink cartridge, E-Cigarette cartridge, Drone, etc..



IoT security

- Server↔HUB: TLS standards
- HUB↔Thing/ Thing↔Thing : PUF IC security(H/W)



ICTK Holdings本社:
323, Pangyo-ro, Bundang-gu, Seongnam-si,
Gyeonggi-do, Korea
http://www. ictk.com

日本総代理店 ノバテック株式会社:
東京都世田谷区玉川田園調布2-8-5
http://www.novatec.co.jp
Tel 03-6825-8851 Mail iot_security@novatec.co.jp