ProductID

Strong and secure Identity of Things solution.

ProductID is the ultimate solution to the demands of products, batch, or goods identification.

Using a combination of highly reliable tools it provides the same security standards as the digital signature of documents and certified emails.

How it works:
To grant the secure identification of a generic object ProductID creates its digital twin. The digital identity is granted by a cryptographic NFC tag that owns a unique ID. Tag is able to sign a dataset using an RSA 1024 private key verifiable with a simple smartphone: a web page opens automatically scanning the tag and If the signature check is positive, the browser is redirected to the object' specific web page.

Solution components:
- Security element/tag: crypto smartcard with NFC wireless interface. Available in two formats: standard ISO 7816-1 and round disk, 2.5 cm diameters with 3M™ adhesive.
- Card initialization tool: PC application (Linux or Windows) and allows the product owner to initialize the tag.
- ProductID front-end service: public or custom card verification page. Normally invisible, it advises the user if card verification fails, or open the product specific description page.
- ProductID back-end service: public or custom server that trace the card usage on IOTA public ledger.
- Private IOTA node: allow to grant access to the ledger and write data with reliable performance.

Key features:

- Identity of things
- anti counterfeit
- object tracking
- Proof of onwership
- Proof of presence

Things Lab

www.thingslab.technology

ProductID

Technical specification:

- Security element/tag:
  - Memory: 23KB EEPROM, 3 KB RAM
  - Operating system: Java Card 3.0.4, GlobalPlatform 2.1.1
  - RSA up to 2048 bits key length encryption and signature algorithm
  - Communication Protocol:
    - ISO14443 Part1-4 (NFC)
    - Contactless interface supports Type A
  - Available form factors:
    - Standard ISO 7816-1
    - Round disk, 2.5 cm diameters with 3M™ adhesive.

- Digital ID:
  - One-time signed ID is generated and encoded in an NDEF message as URL. RSA signature is based on:
    - ProductID page web address or custom page web address
    - 81 characters long unique ID assigned to the security element during the initialization phase.
    - Usage counter, automatically increased ad each tag scan

- Front end (ProductID web page):
  - One-Time signature verification process:
    - Card public key is retrieved from the IOTA ledger (card's dedicated MAM channel)
    - Last recorded usage counter is retrieved from IOTA legder (card's dedicated MAM channel)

- Back end (ProductID web platform):
  - Manage the card initialization process:
    - Card public key is stored on the IOTA ledger (MAM channel)
    - Last recorded usage counter is retrieved from IOTA ledger (card's dedicated MAM channel)

Overall security features:
Secure elements (tags) can't be cloned and signature verification process can't be tampered with. Public key is stored in IOTA public ledger so it can't be modified and are accessible over thousand of nodes.

Key features:

- Identity of things
- anti counterfeit
- object tracking
- Proof of onwership
- Proof of presence

Things Lab

www.thingslab.technology