AuthentiK

An authenticity certification system

Empower the cryptography to deliver new trust.

A full key-turn system

developed by BitLogiK

Certification

The challenges for authenticity certificates

- Prove the issuance by the manufacturer
- Must be unique
  - Copy resistant
  - Clones detection
- Must be trustworthy for the consumers
  - Integrity
  - Easy and fast to use (check)
  - Trust the second-hand market

Certification

- Present
  - Paper, hologram,…
  - QR Code
  - NFC tag (static content = QR code or paper)

- October 2018 : *NXP DNA 4* tags
  - Active cryptography
  - Easy use with a smartphone, no app required
  - Single-use signatures
  - Private keys internally protected
  - Controlled costs : < 0,60$ per tag

Modern tags

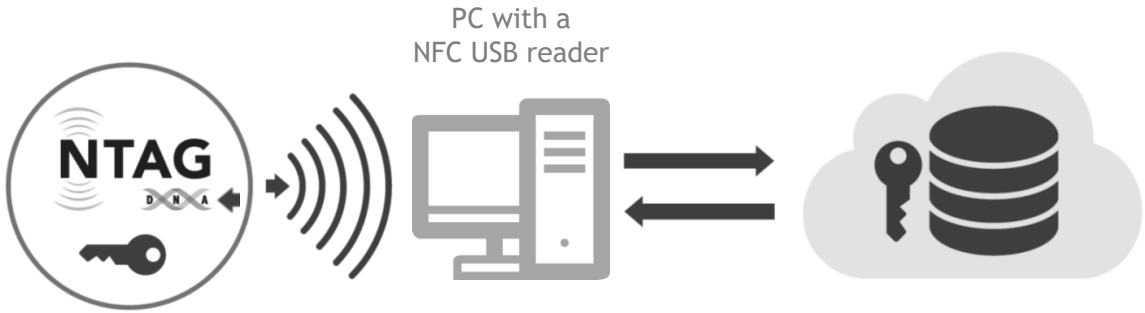
Generate a unique and secure authentication code whenever the tag is read.

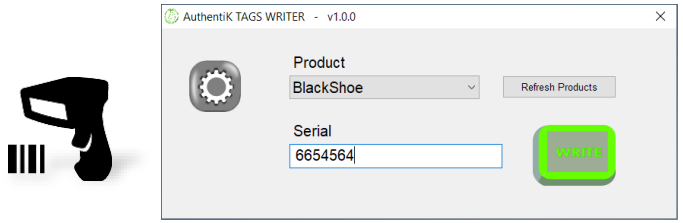
The NFC *DNA* 4 tag in details

- AES-128 protection
- Counter incremented at each reading of the message
- Secure unique dynamic messages authentication
  - Signature with message authentication code LRP(AES)-CMAC
  - Standard : AES-CMAC / OMAC1 : NIST SP 800-38B
  - strengthened by Leakage Resistant Primitive
- Attack-resistant certified silicon
  - Certification Common Criteria EAL4 hardware & software
  - Hard to extract private keys from product
- Native URL NFC reading on mobiles
  - 848kbps : short programming and reading times
  - NFC type 4 ISO14443-4
  - Open the browser right away after “tap”
  - Android and iOS compatible

BitLogiK

The *AuthentiK* system : production





Software
AuthentiK Tags Writer
Windows – Linux – MacOS

At the factory / workshop

- Input the product serial number
- Tag writing and locking
- Secure data registration in the server
  - Tag ID <> Product serial
- Integration in production system as option

Reading possibilities through hand laser or tag

automatic
1-click/1-button

BitLogiK

The *AuthentiK* system : UX

- **For the end-users or resellers** : *tap & check* !

`https://authentik.one/check/ProductONE?sn=12345678&u=045F05222A6380&c=000002&m=D3250A3DF8C258A7`

Product → Serial # → tagID → counter → signature

single use

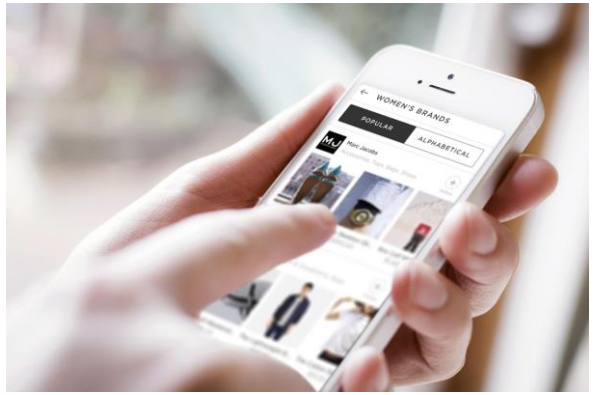
unique message and dynamic signature

BitLogiK

The *AuthentiK* system : UX+

In-app integration

- Connection to an API
- Check : tagID read in URL = actual tag's ID
- Phishing protecting (similar web domain name)
- Link user <-> product / loyalty
  - Who owns what ?
  - Who is interested by what ?
- Easy tag link sharing
  - Raise trust for a second-hand buyer

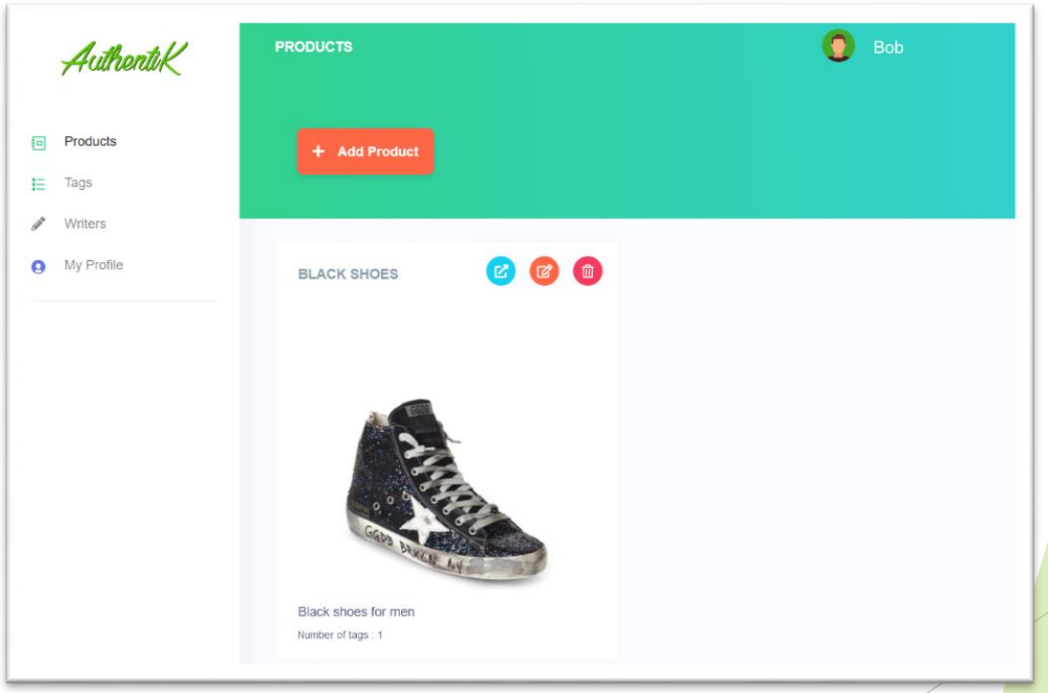


BitLogiK

The AuthentiK system : Dashboard

An interface for administration

- Web
- Tags and products management
  - Follow-up production
  - Follow-up products lifecycle
- Monitor frauds
  - Real-time alerts
    - by email
    - or API requests



BitLogiK

An authenticity certification system

AuthentiK

Further information,
questions, requests ?

info@authentik.one