

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



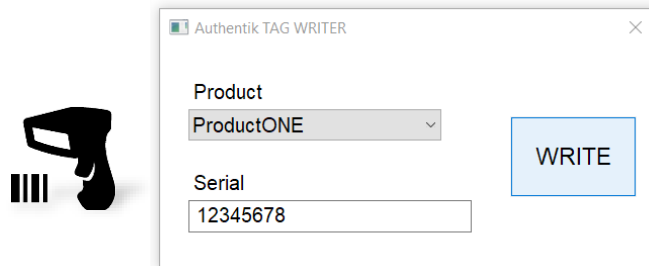
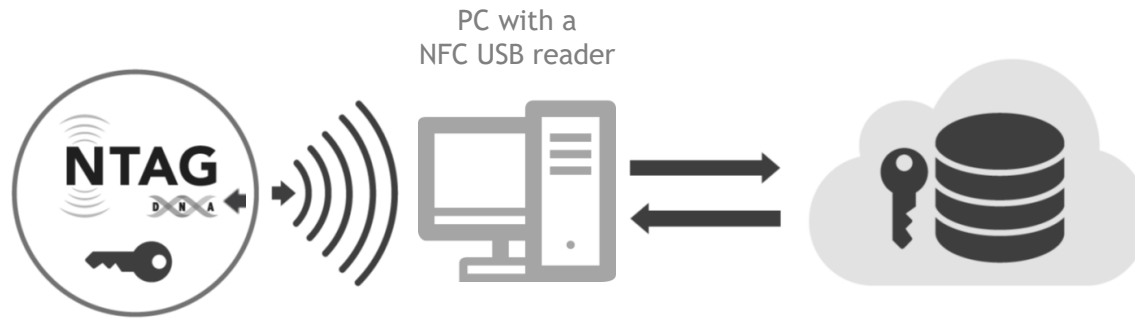
Modern tags

The NFC *DNA* 4 tag in details

- ▶ AES-128 + Leakage Resilient Primitive (attack resistant)
- ▶ Counter incremented at each reading of the message
- ▶ Dynamic message signature
 - ▶ Signature with message authentication code LRP(AES)-CMAC
 - ▶ Standard : AES-CMAC / OMAC1 : NIST SP 800-38B
 - ▶ strengthened by LRP
- ▶ 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



The *AuthentiK* system : production



Software
AuthentiK Tag Writer
Windows – Linux – Mac OSX

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

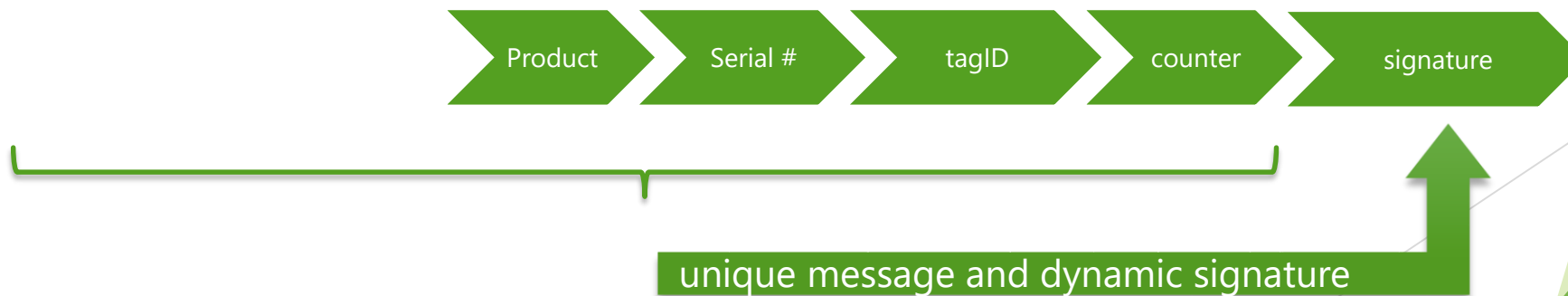
} automatic
1-click/1-button

The *AuthentiK* system : UX

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



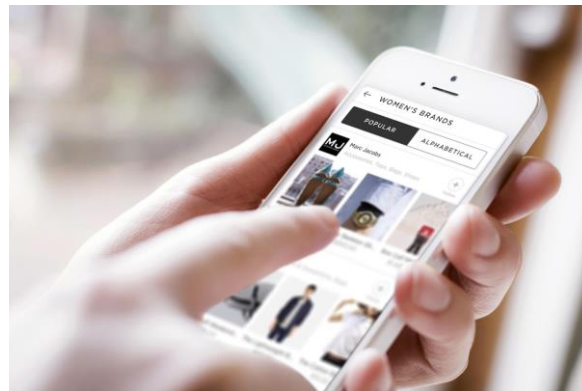
<https://authentik.one/check/ProductONE?sn=12345678&u=045F05222A6380&c=000002&m=D3250A3DF8C258A7>



The *AuthentiK* system : UX+

In-app integration

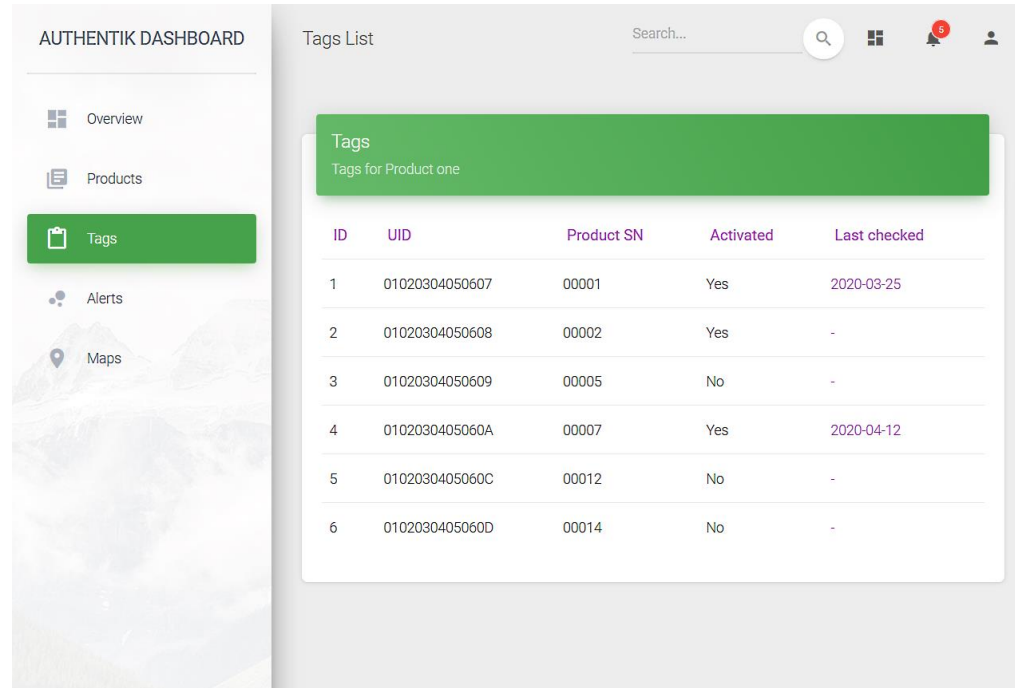
- ▶ Connection to an API
- ▶ Check : tagID read in URL = actual tag's ID
- ▶ Phishing protecting (similar web domain name)
- ▶ Link user <-> product / loyalty
 - ▶ Who owns what ?
 - ▶ Who is interested by what ?
- ▶ Easy tag link sharing
 - ▶ Raise trust for a second-hand buyer



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



The screenshot displays the 'AuthentiK Dashboard' interface. On the left is a navigation sidebar with options: Overview, Products, Tags (highlighted), Alerts, and Maps. The main content area is titled 'Tags List' and features a search bar and user profile icons. Below this is a table titled 'Tags for Product one' with the following data:

ID	UID	Product SN	Activated	Last checked
1	01020304050607	00001	Yes	2020-03-25
2	01020304050608	00002	Yes	-
3	01020304050609	00005	No	-
4	0102030405060A	00007	Yes	2020-04-12
5	0102030405060C	00012	No	-
6	0102030405060D	00014	No	-

An authenticity certification system

Authentik



Further information,
questions, requests ?



info@authentik.one