Cybersecurity rooted in people and devices

Iluminada Baturone
Full Professor. University of Seville. lumi@us.es
Senior Researcher. Microelectronics Institute of Seville (IMSE-CNM)

November, 17th 2022

IMSE -cnm Instituto de Microelectrónica de Sevilla

CSIC Consejo Superior de Investigaciones Científicas

Universidad de Sevilla

Outline

Our research group: Cybersecurity rooted in people and devices

1. Secure digital identities
2. Post-quantum cryptography (PQC)
3. Non-Fungible Tokens (NFTs)
4. Design and use of secure and trusted hardware

Our research group: Cybersecurity rooted in people and devices

We are researchers at Microelectronics Institute of Seville (IMSE-CNM)

An R+D+i joint center of the University of Seville and the Spanish National Research Council (CSIC).

Our research interests are: cybersecurity, post-quantum cryptography, biometrics, hardware security, soft-computing (neural networks and fuzzy logic).

Our group is composed of:

- Professors of Computer Science Engineering School and Physics Faculty of University of Seville
- Ph.D. students
- Master students

Our current Research Projects

- Mas+Cara:

Proof of concept of a decentralized and private facial recognition scheme with post-quantum security
(PDC2021 – Next Generation European Union)

Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

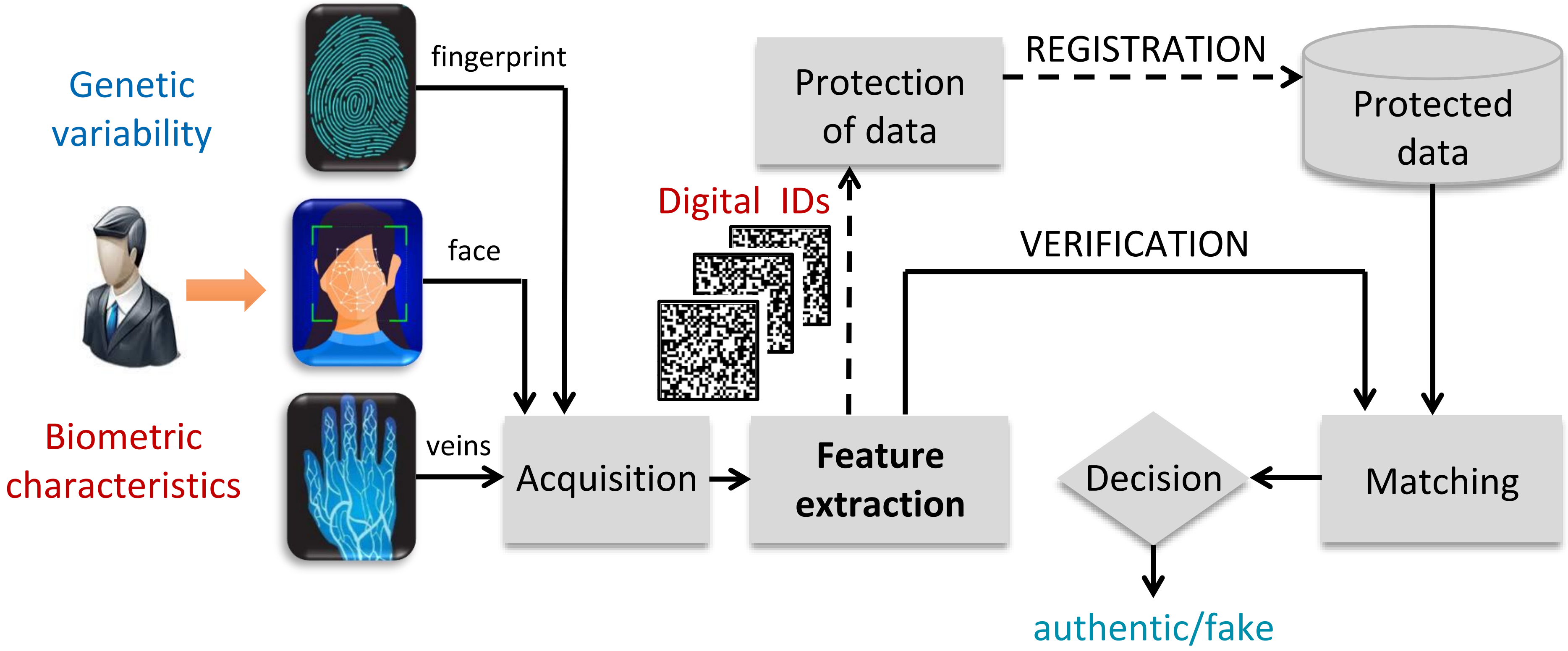
- HardWallet:

Trusted and post-quantum secure hardware for wallets of decentralized identities using bio and device metrics
(PID2020 – Spanish Research Agency)

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN
AGENCIA ESTATAL DE INVESTIGACIÓN

Secure digital identities

People: Digital IDs from biometric traits



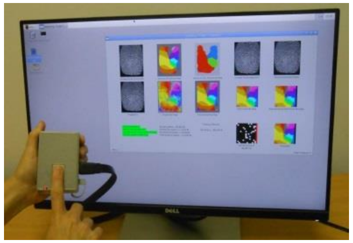
In order to avoid spoofing:

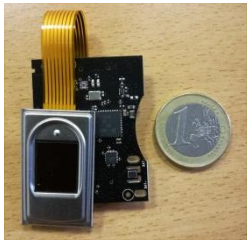
- Multi-modal instead of uni-modal biometrics
- Behavioral instead of only physical biometrics

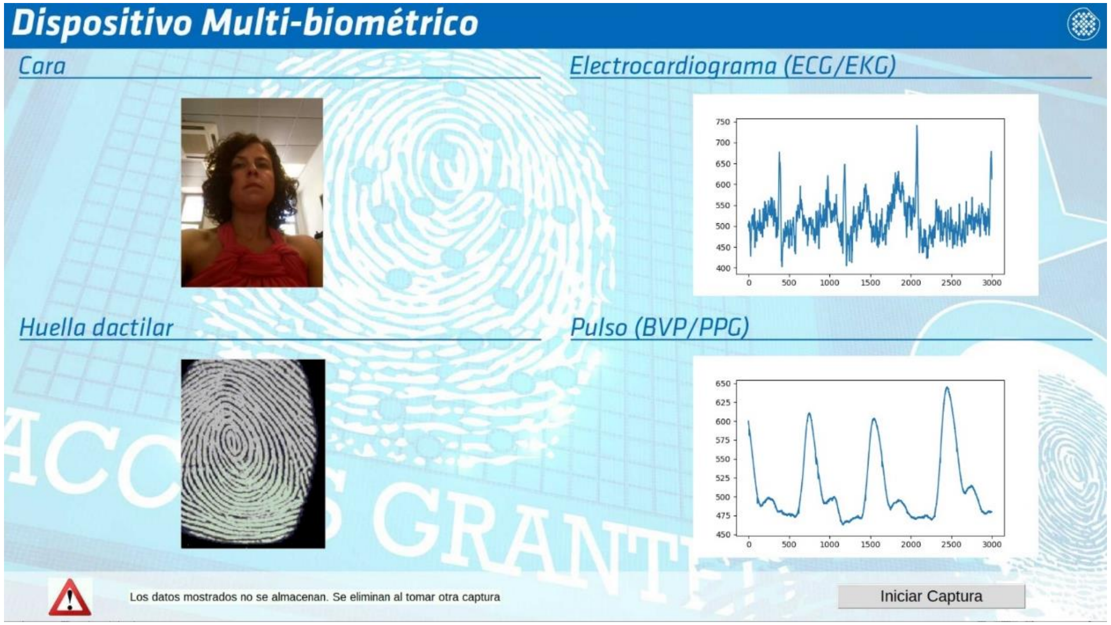
Secure digital identities

People: Digital IDs from biometric traits

- We have proposed a fingerprint recognition solution for wearables
- We have explored recognition by physiological traits

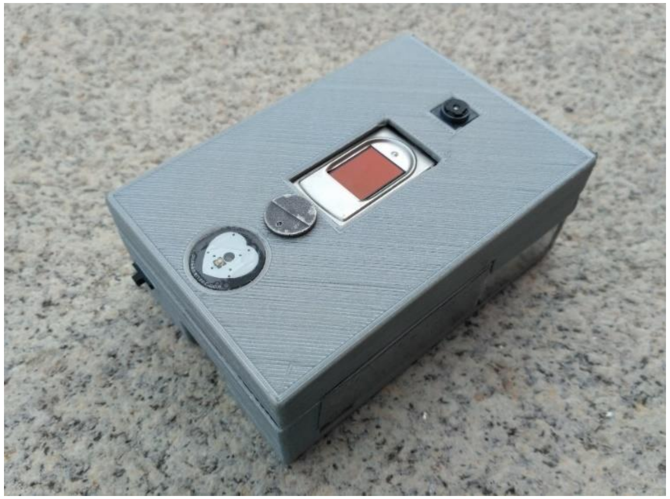




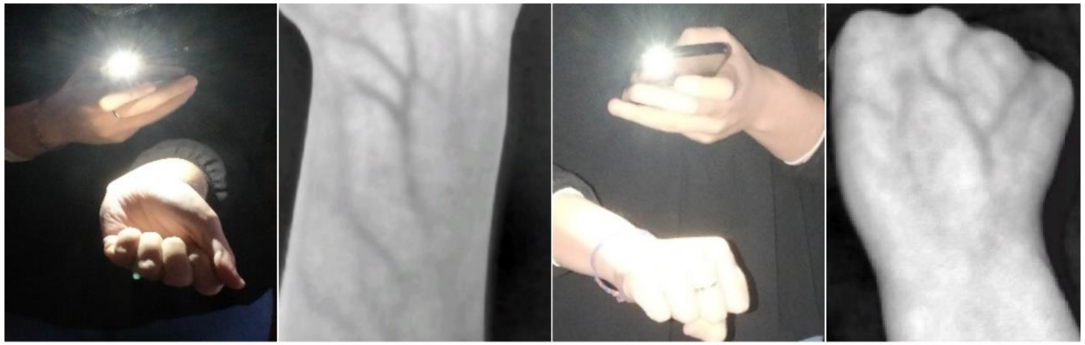


Dispositivo Multi-biométrico

Los datos mostrados no se almacenan. Se eliminan al tomar otra captura

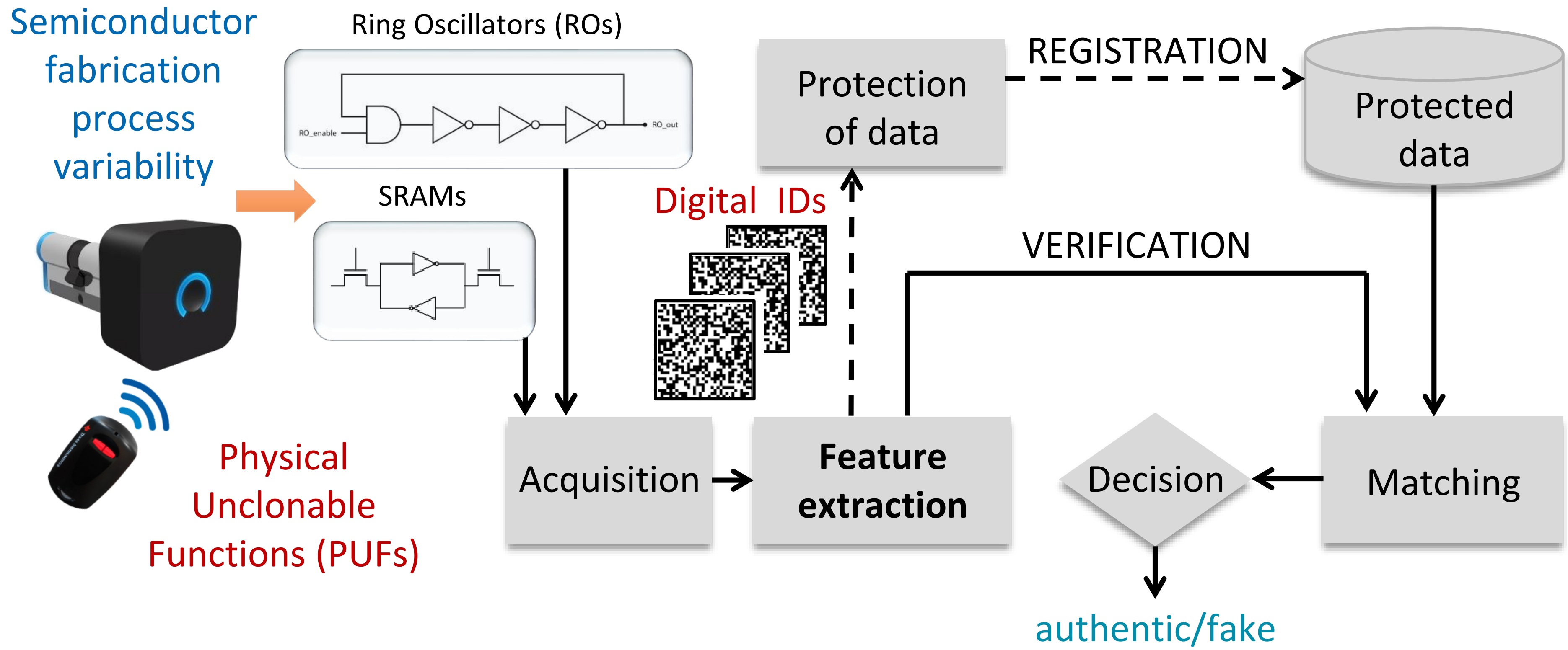


- We have developed facial and vein biometric recognition systems in ordinary smartphones



Secure digital identities

Devices: Digital IDs from its hardware



Semiconductor fabrication process variability

Ring Oscillators (ROs)

SRAMs

Physical Unclonable Functions (PUFs)

Acquisition

Feature extraction

Digital IDs

Protection of data

REGISTRATION

Protected data

VERIFICATION

Matching

Decision

authentic/fake

In order to avoid spoofing:

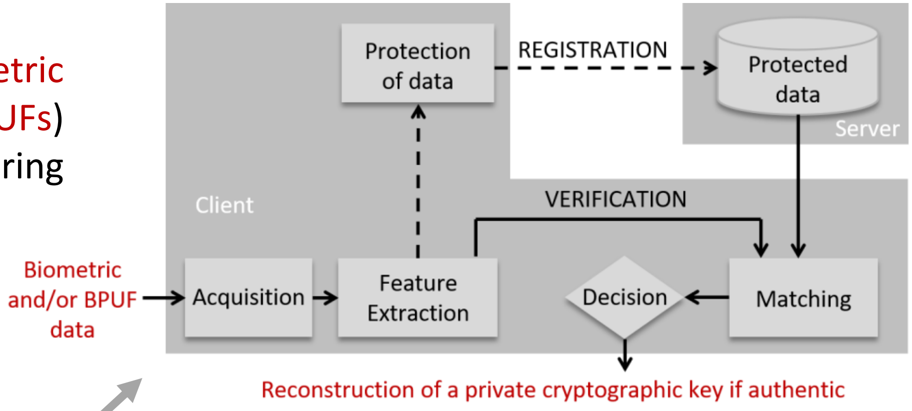
- Multi-modal instead of uni-modal PUFs
- Behavioral instead of only Physical Unclonable Functions: BPUFs

European Patent Application submitted in July of 2019 with application number EP 19382623.7

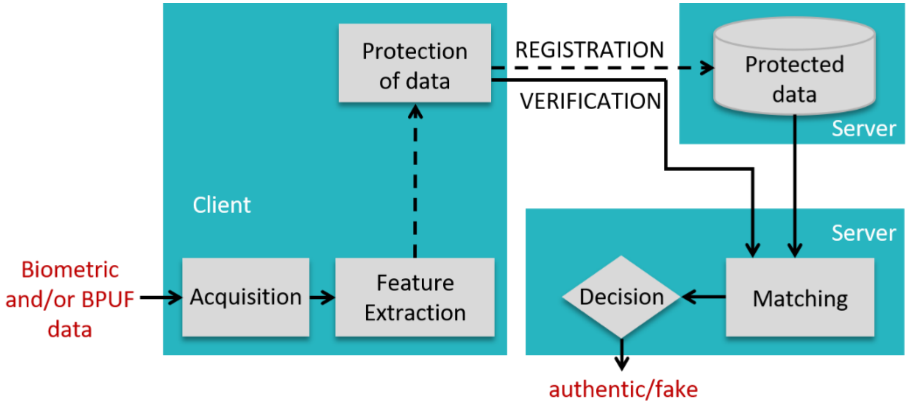
Post-quantum cryptography methods for protection and matching of noisy or approximated information

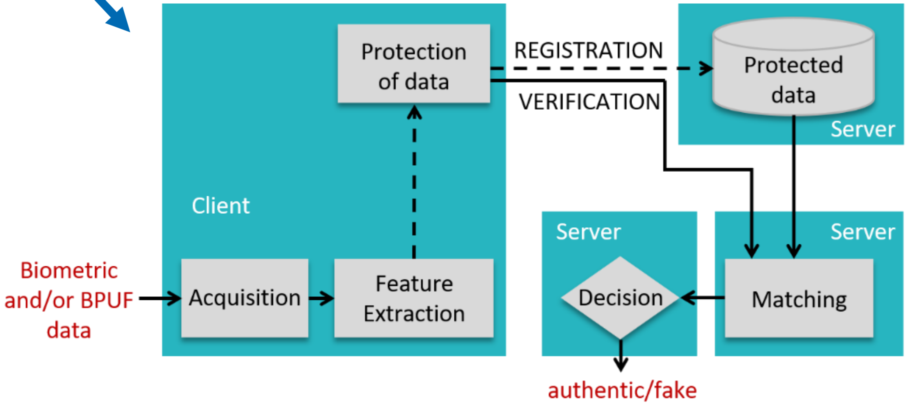
- A client acquiring authentic but noisy information like biometric and/or Behavioral and Physical Unclonable Functions (BPUFs) data can perform secure electronic transactions, without storing cryptographic keys but reconstructing them.

- Our solution exploits homomorphic encryption based on proven post-quantum public-key algorithms, NIST approved for standardization and 4-round finalists.



- Our solution is valid for keyless and passwordless contexts in centralized and new decentralized architectures





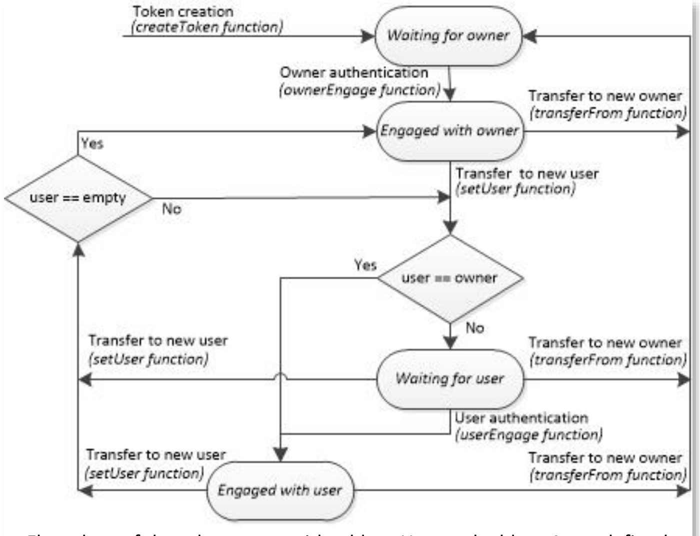
European Patent Application submitted in April of 2022 with application number EP 22382418.6

https://videos.us.es/media/MasCara_Demo1/1_lqidpel4

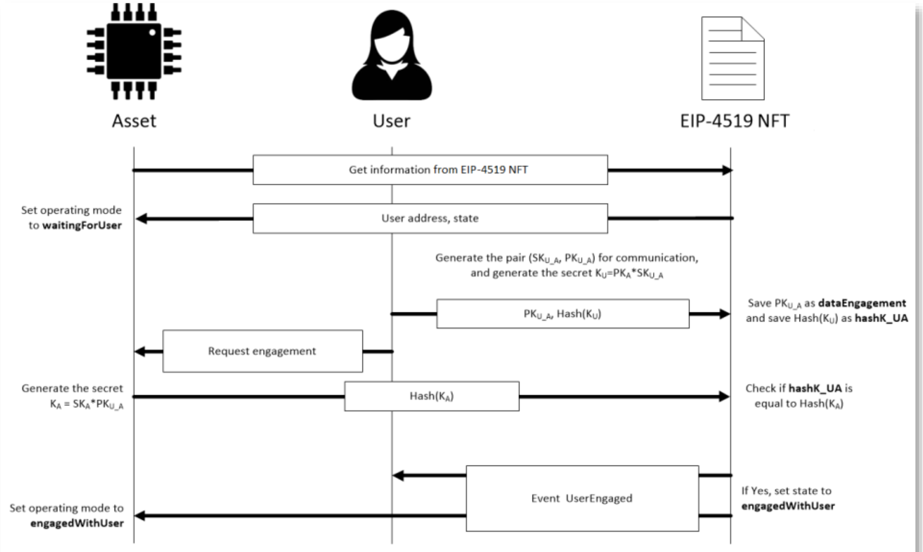
Non-Fungible Tokens (NFTs): Secure combination of the physical world and Blockchain

- We have proposed EIP-4519: NFTs Tied to Physical Assets
  https://eips.ethereum.org/EIPS/eip-4519

Standard interface for NFTs representing physical assets that can reconstruct their blockchain accounts, obey users and owners, and establish secure communication channels with them

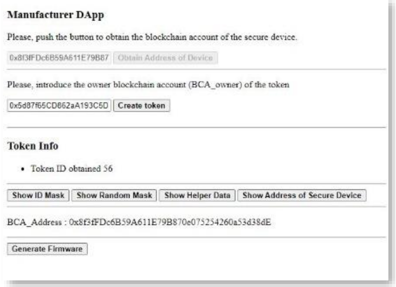


Flow chart of the token states with addressUser and addressAsset defined


Asset
User
EIP-4519 NFT
Get information from EIP-4519 NFT
Set operating mode to waitingForUser
User address, state
Generate the pair (SK_{U_A}, PK_{U_A}) for communication, and generate the secret K_U=PK_A*SK_{U_A}
PK_{U_A}, Hash(K_U)
Save PK_{U_A} as dataEngagement and save Hash(K_U) as hashK_UA
Request engagement
Generate the secret K_A = SK_A*PK_{U_A}
Hash(K_A)
Check if hashK_UA is equal to Hash(K_A)
Event UserEngaged
If Yes, set state to engagedWithUser
Set operating mode to engagedWithUser

Engagement process between user and asset

ethereum


Manufacturer DApp

Please, push the button to obtain the blockchain account of the secure device.

0x8f3fFDc6B59A611E79B87 [Obtain Address of Device]

Please, introduce the owner blockchain account (BCA_owner) of the token

0x5d87f65CD862aA193C5D [Create token]

Token Info

- Token ID obtained 56

[Show ID Mask] [Show Random Mask] [Show Helper Data] [Show Address of Secure Device]

BCA_Address : 0x8f3fFDc6B59A611E79B870e075254260a53d38dE

[Generate Firmware]

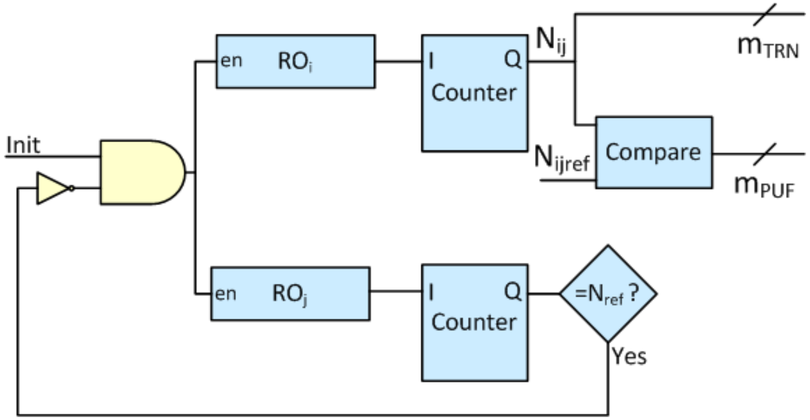
IoT devices, for example, can be tied to EIP-4519

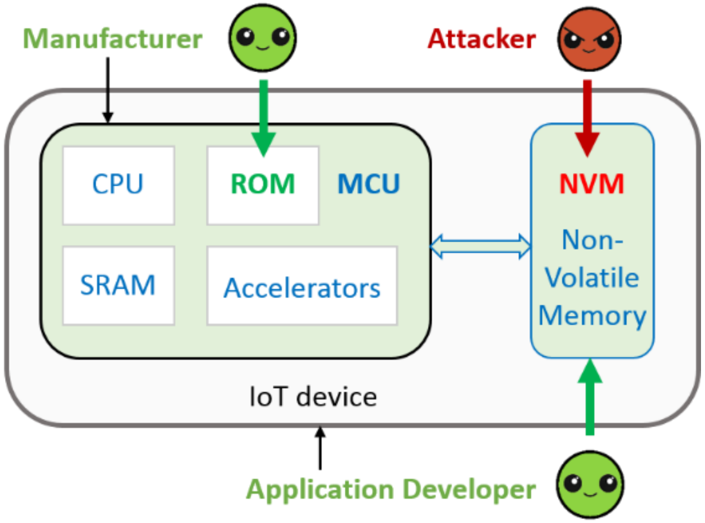
https://videos.us.es/playlist/dedicated/275782623/1_c8xzw42c/1_jqno65ka

Design and use of secure and trusted hardware

- Normally, secret keys are stored in a memory located inside the chip. It is more secure to generate (TRNG) and reconstruct (PUF) them whenever required

We have proposed a unified TRNG/PUF





- For IoT and digital wallets, it is fundamental:
- Secure boot and remote attestation
- Sealed storage of sensitive data

We have proposed solutions based on post-quantum cryptography

Thanks for your attention

…any questions…