ARCADIAN-IoT

Multi-factor Authentication

1GLOBAL
formerly TRUPHONE

João Casal (Head of R&D)

15/09/2023

AGENDA

ARCADIAN-IoT

1. Multi-factor authentication: why and how?
2. ARCADIAN-IoT Multi-factor Authentication (MFA)
   - Enable security and trust in the management of objects' identification
   - Enable security and trust in the management of persons' identification
3. Q&A

1. MULTI-FACTOR AUTHENTICATION: WHY AND HOW?

ARCADIAN-IoT

What is Authentication and why its reliability is critical

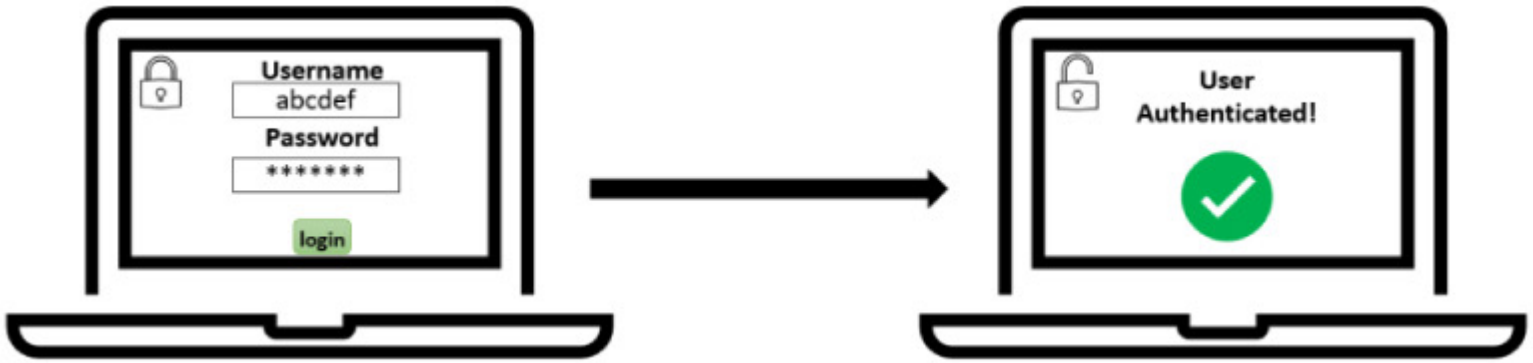
- Process of **validating the identity** of a person or device to allow access to a particular service or data.
- Impersonation is a **critical security threat**. Let's consider why:
  - In the use of bank services, by bank clients or bank employees:
    - access to bank information, ability to do money transfers, …
  - In the control of your laptop and smartphone:
    - access to private data like contacts, photos, emails, private business documents, …
  - In the control of a security camera at home or at the office:
    - access to private habits or to private data in use by employees, …
  - In the access to the data sent by a smart car:
    - access to sensitive information like location or destination, …
  - …

1. MULTI-FACTOR AUTHENTICATION: WHY AND HOW?

ARCADIAN-IoT

Most used authentication method:

Username and password



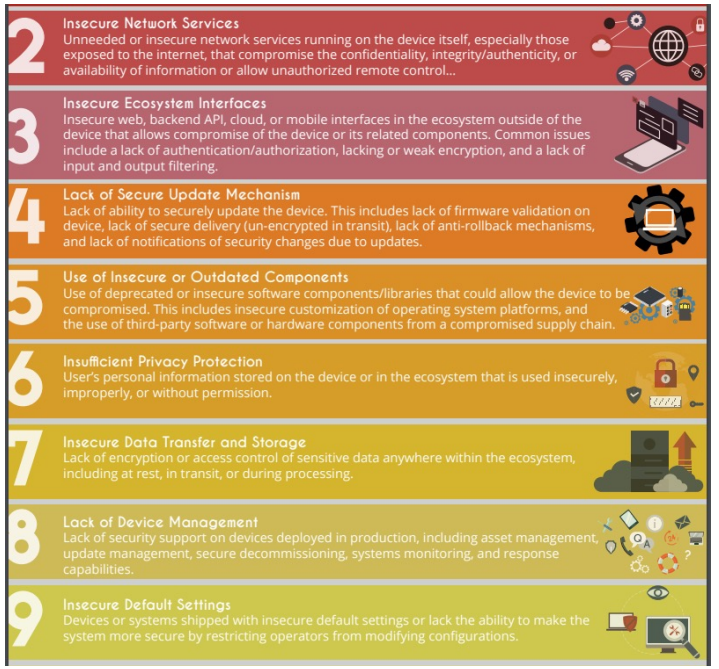
- The user expects Username / Password to authenticate
- Average person owns 25 online accounts
- Only 50% have different passwords for each - passwords are hard to remember
- Use of very simple passwords – name, date of birth, … - is very common
- Brute force attacks (even using freely available tools) has shown to be effective to hack passwords

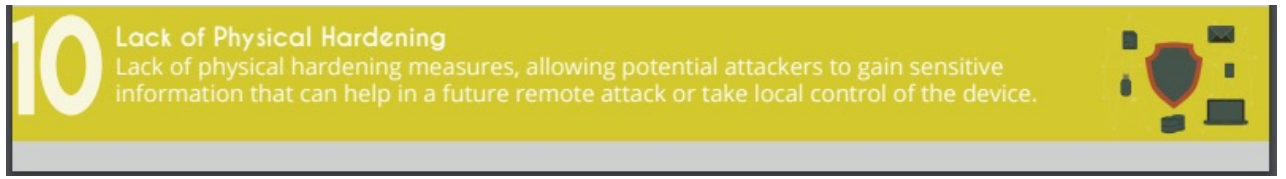
Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology*.

1. MULTI-FACTOR AUTHENTICATION: WHY AND HOW?

ARCADIAN-IoT

Also, in IoT, the **#1 in the most common security risks** is…





https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

1. MULTI-FACTOR AUTHENTICATION: WHY AND HOW?

ARCADIAN-IoT

- “Due to a variety of security concerns, it was found that SFA (single factor authentication) could not offer effective security”

- A 2FA (two factor authentication) increases security by combining:

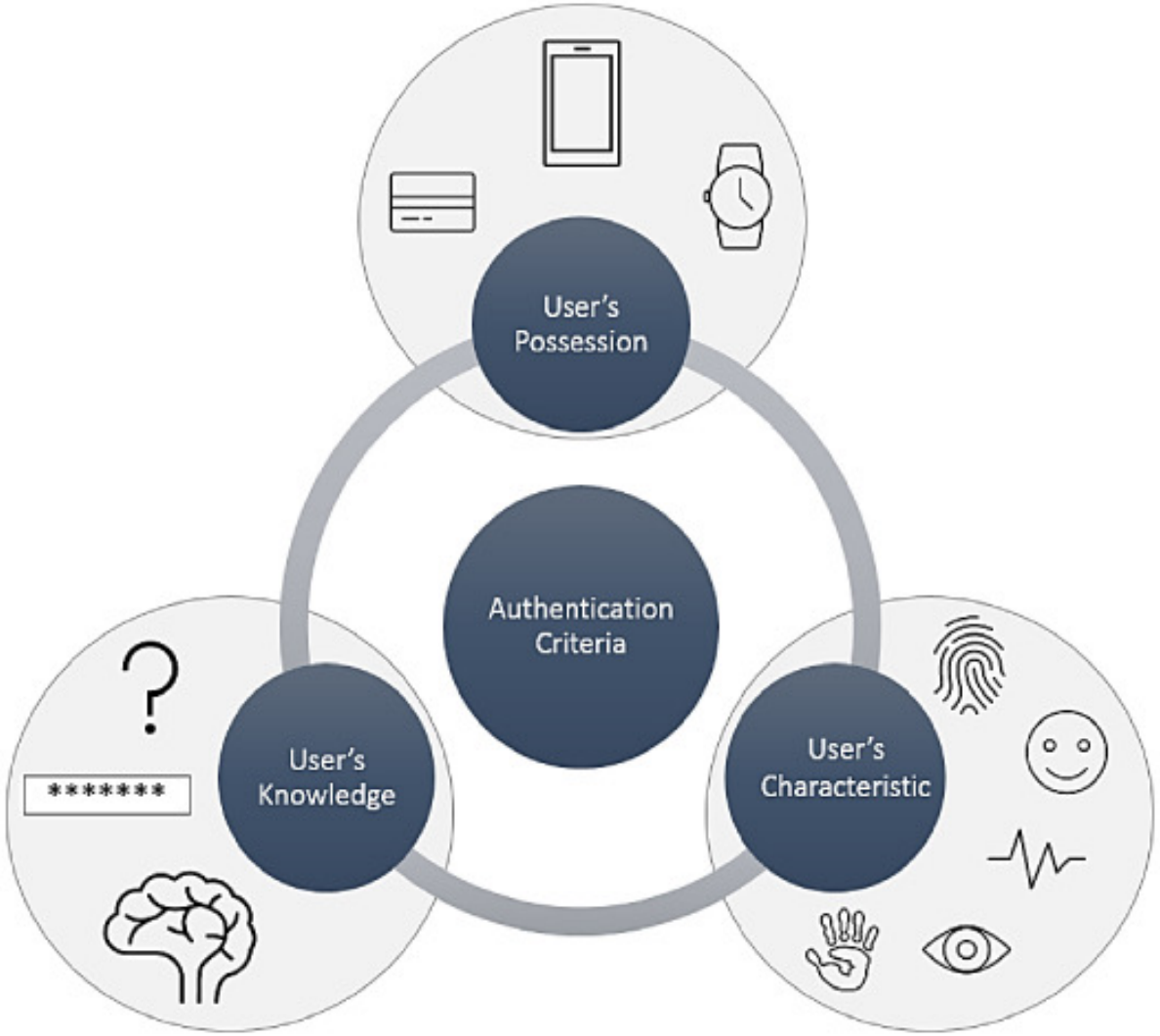
Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology*.

1. MULTI-FACTOR AUTHENTICATION: WHY AND HOW?

ARCADIAN-IoT

- A 2FA (two factor authentication) increases security by combining:

- If a password is compromised, a second factor ensures the security of the service/data.

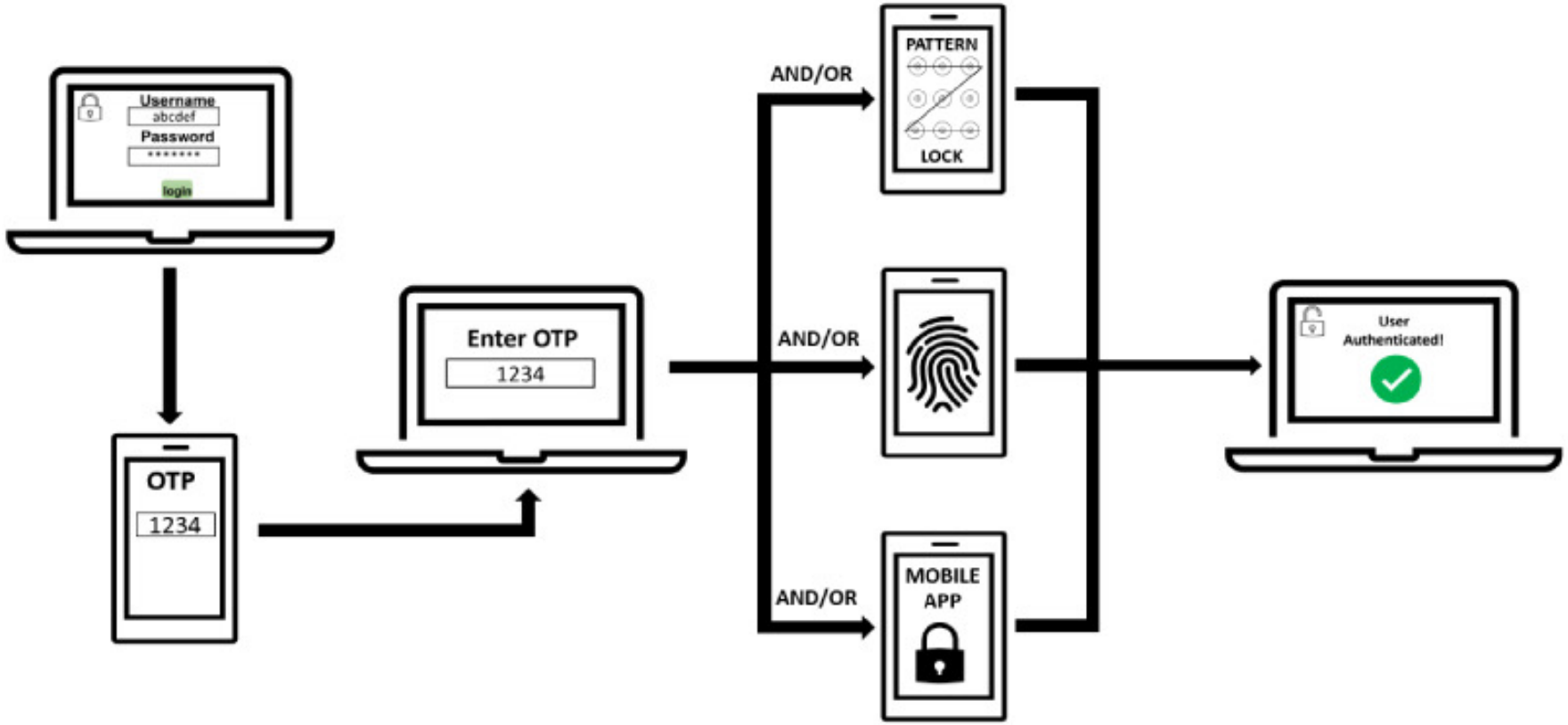


Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology*.

1. MULTI-FACTOR AUTHENTICATION: WHY AND HOW?

ARCADIAN-IoT

- A MFA creates more levels of authentication to maximize security. E.g.:



Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology*.

2. ARCADIAN-IoT MULTI-FACTOR AUTHENTICATION

2. ARCADIAN-IoT MULTI-FACTOR AUTHENTICATION

ARCADIAN-IoT

Objectives

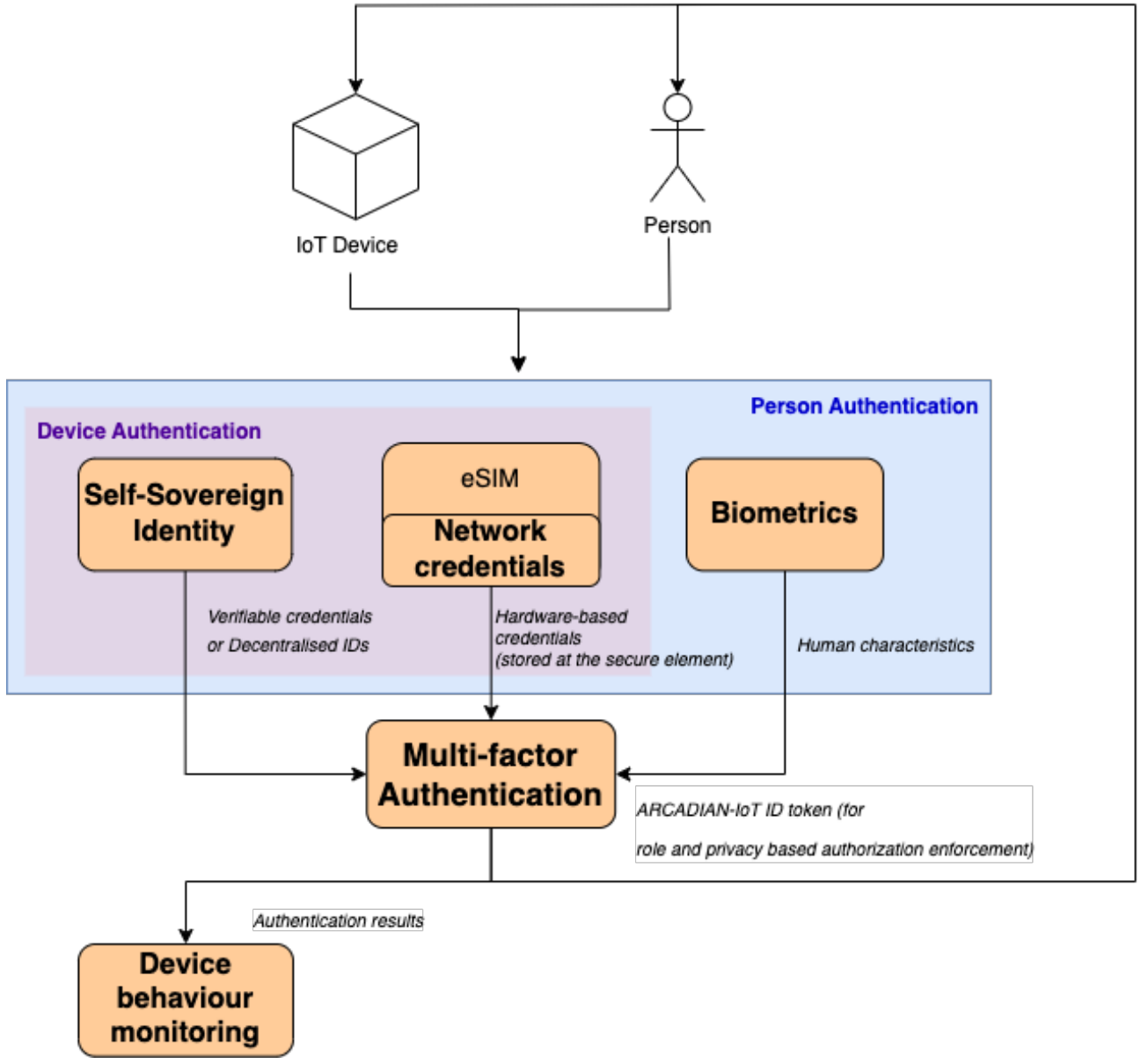
- Enable security and trust in the management of objects' identification
  - Enable 2 different identification factors for devices

- Enable distributed security and trust in management of persons' identification
  - Enable **3 multiple simultaneous identification approaches for persons**
  - Enable a mediated mutual authentication between persons and IoT devices

2. ARCADIAN-IoT MULTI-FACTOR AUTHENTICATION

High-level architecture

- **Objects identification** rely on 2 factors: a decentralized approach and a hardware-based approach.
- **Persons identification** rely on 3 factors: a decentralized approach, a hardware-based approach and biometrics.
- **ARCADIAN-IoT ID token** (built according to best practices*) is provided to the client (person / IoT) after a successful authentication
  - Components like **Self-Aware Data Privacy** enforce role and privacy-based authorization
- Authentication results (successful or not) are provided to **ARCADIAN-IoT Behaviour Monitoring**, allowing to detect threats (like brute force attacks)

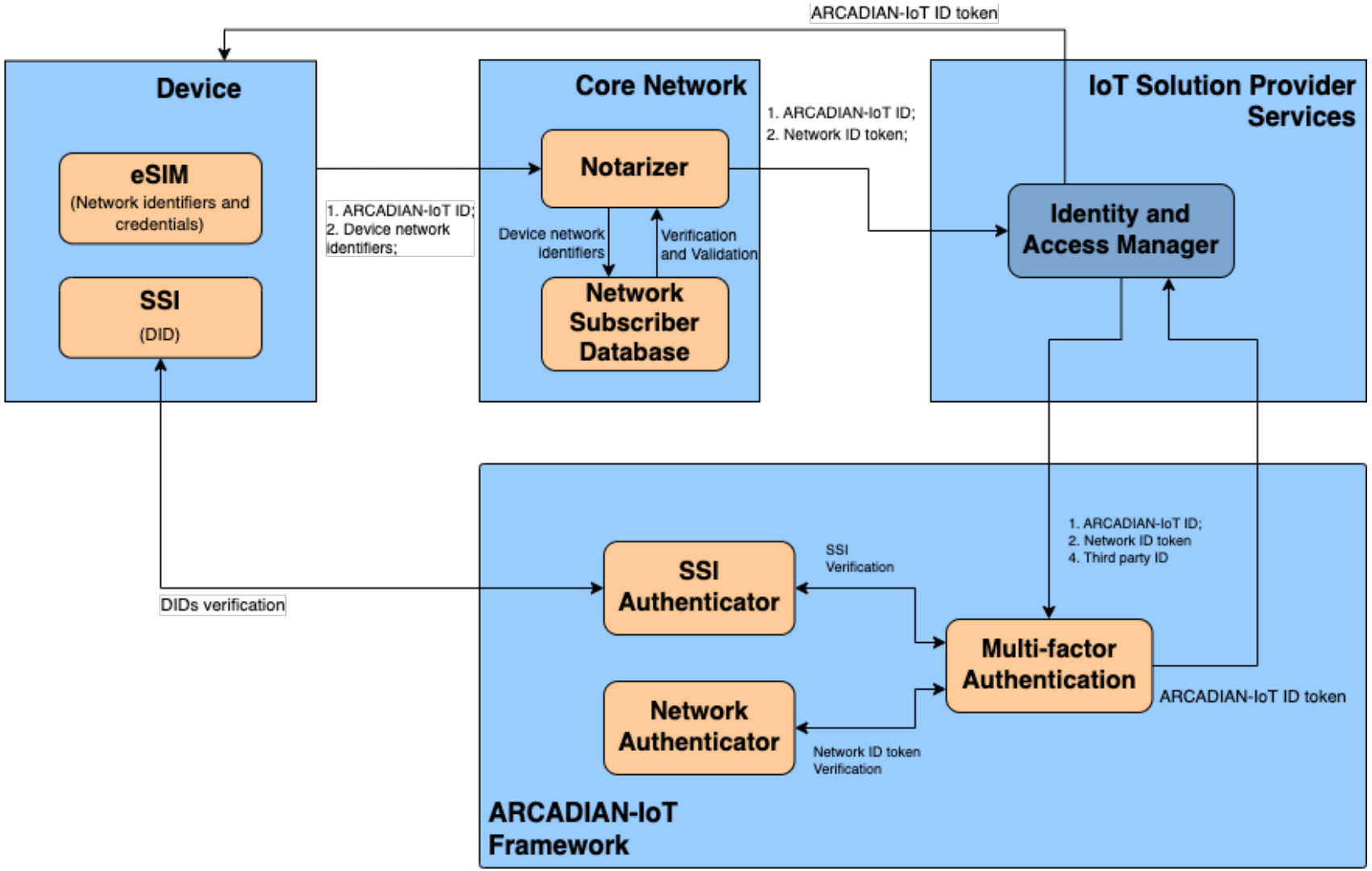


*https://auth0.com/docs/secure/tokens/id-tokens

2. ARCADIAN-IoT MULTI-FACTOR AUTHENTICATION

Enable 2 different identification factors for devices

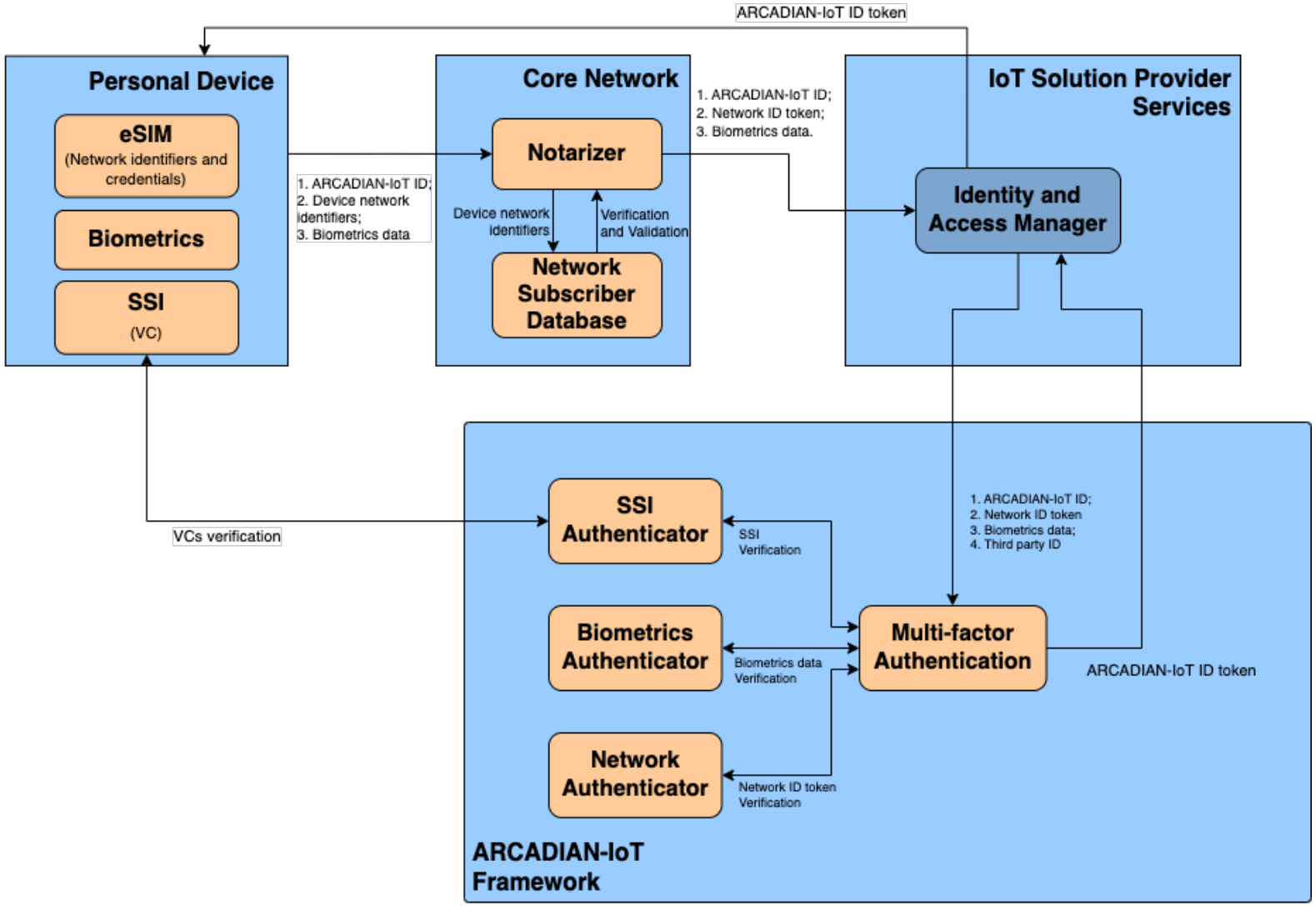
- **Device comms protocols: HTTP; MQTT** (secure comms to the core network)
- **ARCADIAN-IoT ID token**: JWT or CWT



2. ARCADIAN-IoT MULTI-FACTOR AUTHENTICATION

Enable 3 multiple simultaneous identification approaches for persons

- **Device comms protocols: HTTP; MQTT** (secure comms to the core network)
- **ARCADIAN-IoT ID token**: JWT or CWT



2. ARCADIAN-IoT MULTI-FACTOR AUTHENTICATION

ARCADIAN-IoT

Enable a mediated mutual authentication between persons and IoT devices

Demonstration in a person authentication using biometrics captured by a drone

Pre-requisites for the **person identification with the IoT device**:

1. Both the person and the IoT device have already **authenticated individually successfully**
2. It is the **person that is requesting the service** that will trigger its identification by the IoT device
3. For the identification to start, both the IoT device and the person need to be in the same **location** at the same **time**. Otherwise the process don't even start.

2. ARCADIAN-IoT MULTI-FACTOR AUTHENTICATION

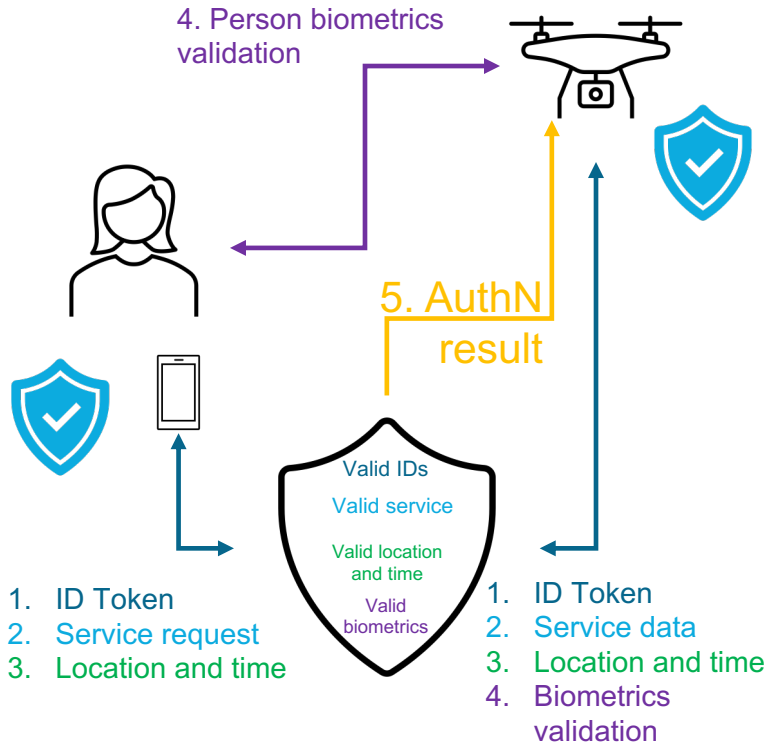
Enable a mediated mutual authentication between persons and IoT devices

Approach storyline:

The mediator (e.g. the solution provider) validates:

1. the requesting **person ARCADIAN-IoT ID token**, and the **IoT device ARCADIAN-IoT ID token**,
2. **the service data** (validates if that IoT device was selected to serve that person)
3. and current **time** and **location** of both

4. and biometrics captured by the IoT device matches the person biometrics



2. ARCADIAN-IoT MULTI-FACTOR AUTHENTICATION

ARCADIAN-IoT

TLDR: Why to adopt ARCADIAN-IoT MFA

1. **Resistant to password-related vulnerabilities like:**
   - Brute force attacks
   - Phishing
   - Credential stuffing (use of credentials captured in a data breach
2. It is a **beyond state of the art authentication solution** that maximizes security by joining:
   - Hardware based identification factor – physical hardening (for devices and persons)
   - Decentralized identifiers / Verifiable credentials – avoid single-trust entites (for devices and persons)
   - Beyond state of the art biometrics (for persons)
3. Integrates with other cybersecurity technologies like **behaviour monitoring and reputation system** for an efficient protection with reduced human intervention.

Q&A

João Casal (Head of R&D – joao.casal@1global.com)

Want to join my team in the sunny Lisbon working on innovative SIM, ProgNet and CyberSec tech? Talk with me! ☺