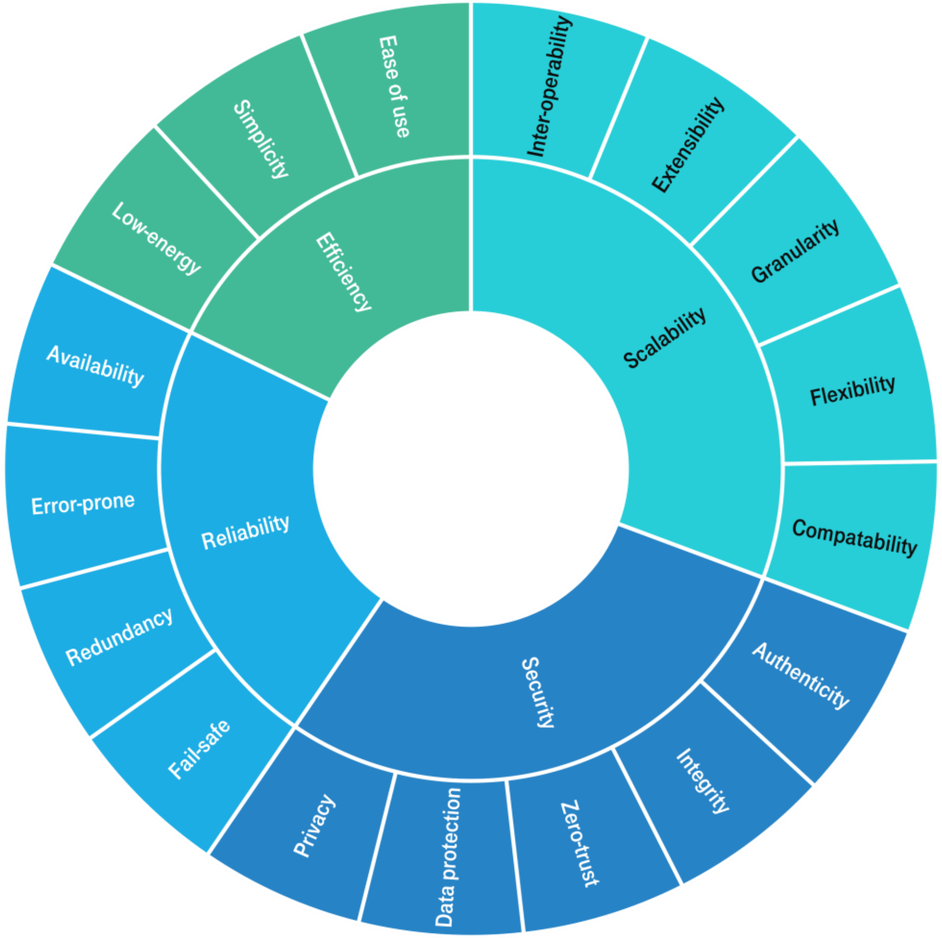
THE NEED FOR NEW AUTHENTICATION METHODS FOR IOT

Dirk v. Hugo, Behcet Sarikaya

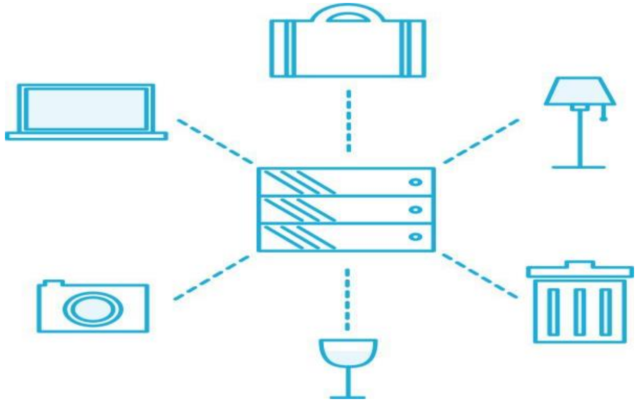
IETF 114 July 2022

Next Generation Type of Communication

- Characterized by diverse applications connecting in a heterogeneous environment in terms of network technologies and devices
- ultra massive (um)IoT may become chance and challenge - basic requirements in dimensions/assessment criteria:
  - Efficiency
  - Reliability
  - Scalability
  - Security
    - Opening risk of DDoS attacks etc.
    - Strong access admission control



Authentication for NG connected things



- Authentication of high-end (platinum) vs. simple cheap (iron) devices: elaborated/refined '5G-like' vs. affordable and convenient
- Authentication models based on human intervention (like 802.1X) not fitting for low-cost IoT in this type of next-gen communication era
- 'Hardware based authentication': sensing of video/audio or shape/gestures from a device or touch of a person etc. uses out-of-band (OOB) channel – i.e., 2-factor authentication (2FA)

Source: https://www.3gpp.org/ and https://www.ietf.org/topics/iot/

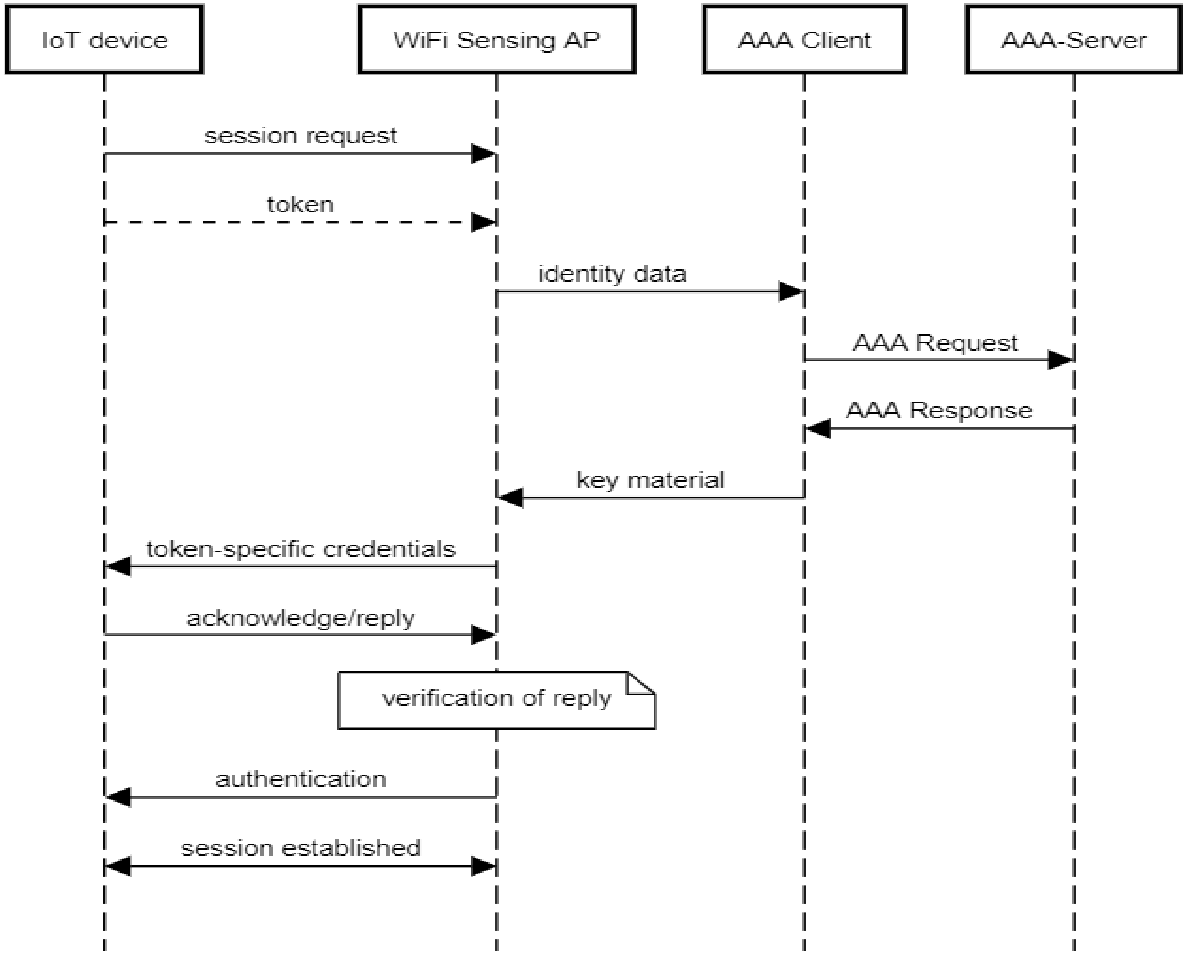
Security Challenges for “dumb” IoT devices

- User and device are separated and not physically connected.
- Unique identity for user applying to all own/personalized devices is given.
- Authentication has to work mutually.
- Simple (“dumb”) devices characterized by:
  - No pre-established relation with intended server or user,
  - No pre-provisioned device identifier or authentication credentials,
  - Input or output interface may be capable of only one-directional OOB communication
- While additional interface for (LED/audio/…) OOB channel may be cost factor, radio sensing via same radio tx/rx antenna signal analysis may simplify devices
- Both IEEE 802.11bf Wi-Fi sensing and 3GPP (5G/6G RAN sensing study) outcome could enable hardware based authentication

Proposed 2FA message exchange

draft-hsothers-iotsens-ps open issues:

- Detailed parameter specification in MSC (e.g., capability, type of sensing, generalized description of token to be expected)
- Standard IoT device ID in terms of (geospatial) (re-)naming
- Extension of AP to (L2) mesh / multicast communication
- Possible extension to RFC9140 on Nimble out-of-band (NOOB) authentication for EAP



Next Steps

- Presented motivation and status of our draft “The Need for New Authentication Methods for Internet of Things” discussing the problem statement and potential IETF work:
  - https://www.ietf.org/archive/id/draft-hsothers-iotsens-ps-02.txt
- Improved it much since Rev-00
- Solicit review and comments by WG
- Aiming at IoTOps WG adoption

- Thank you! - Further questions?
  - Contact: Sarikaya@ieee.org & Dirk.von-Hugo@telekom.de