Using DLT for IoT security

Iordanis Papoutsoglou (Research Associate)
Motivations for security

- Inspired by ENISA’s threat taxonomy for IoT devices.

- **Access control policies** as a good practice to enforce authorization on resources.

- Consider resource capabilities and future application.
- XACML is used for **ABAC** based on Hyperledger Fabric.
- Decision-making is **decentralised**, as XACML components deployed on blockchain (PDP, PAP, PEP).
- Decisions are stored for future audits.
XACML and Decentralisation for IoT devices

**XACML:**
- a flexible and distributed approach for policies,
- dynamic access control and fine-grained delegation with ABAC,
- alleviate maintenance and overhead.

**DLT:**
- data immutability,
- single point of failures avoidance,
- Performance,
- Consistency,
- Room for growth
Contribution and novelty

The architecture is based on permissioned network and does not rely on public blockchain (no cryptocurrency).

The decision (inputs, evaluation) is made on-chain.

General applicability for imposing policies.

Demo based on ASSIST’s port pilot.
Thank you!

Find more: https://assist-iot.eu